



Manual hybird 120 Gigaset Edition

Copyright© Version 1.0, 2013 Gigaset Communications GmbH

Legal Notice

This publication is subject to change. Gigaset GmbH offers no warranty whatsoever for information contained in this manual. Gigaset GmbH is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Copyright © Gigaset GmbH All rights to the data included, in particular the right to copy and propagate, are reserved by Gigaset GmbH.

Table of Contents

Chapter 1	Assistants	1
Chapter 2	System Management	2
2.1	Status	2
2.2	Global Settings	4
2.2.1	System	4
2.2.2	Passwords	10
2.2.3	Date and Time	12
2.2.4	Timer	16
2.2.5	System Licences	19
2.3	Access Codes	19
2.3.1	Alternative Access Codes	20
2.4	Interface Mode / Bridge Groups	21
2.4.1	Interfaces	23
2.5	Administrative Access	24
2.5.1	Access	24
2.5.2	SSH	25
2.5.3	SNMP	28
2.6	Remote Authentication	29
2.6.1	RADIUS	29
2.6.2	TACACS+	34
2.6.3	Options	37
2.7	Configuration Access	37
2.7.1	Access Profiles	38
2.7.2	Users	40
2.8	Certificates	41
2.8.1	Certificate List	42

2.8.2	CRLs	49
2.8.3	Certificate Servers	50
Chapter 3	Physical Interfaces	51
3.1	Ethernet Ports	51
3.1.1	Port Configuration	52
3.2	ISDN Ports	53
3.2.1	ISDN External	54
3.2.2	ISDN Internal	55
3.3	Analogue Ports.	57
3.3.1	Analogue External (FXO)	57
3.3.2	Analogue Internal (FXS)	59
Chapter 4	VoIP	61
4.1	Settings	61
4.1.1	SIP Provider	61
4.1.2	Locations	69
4.1.3	Codec Profiles	71
4.1.4	Options	74
Chapter 5	Numbering	76
5.1	Trunk Settings	76
5.1.1	Trunks	76
5.1.2	Trunk Numbers.	78
5.1.3	Trunk Groups	81
5.1.4	X.31	82
5.2	User Settings	83
5.2.1	Users	83
5.2.2	Class of Services	90
5.2.3	Parallel Ringing	104

5.3	Groups & Teams	105
5.3.1	Teams	105
5.4	Call Distribution	112
5.4.1	Incoming Distribution	112
5.4.2	Misdial Routing.	115
Chapter 6	Terminals	116
6.1	Gigaset Phones	116
6.1.1	Gigaset Phones	116
6.1.2	Gigaset DECT	119
6.2	Other phones	123
6.2.1	VoIP	123
6.2.2	ISDN	126
6.2.3	analog	127
6.2.4	CAPI	130
6.3	Overview	131
6.3.1	Overview	131
Chapter 7	Call Routing.	132
7.1	Outgoing Services	132
7.1.1	Direct Call	132
7.1.2	Call Forwarding	133
7.1.3	Dial Control	135
7.1.4	Priority Numbers	136
7.2	Automatic Route Selection	137
7.2.1	General	137
7.2.2	Interfaces / Provider.	138
7.2.3	Zones & Routing	139

Chapter 8	Applications	141
8.1	Calendar	141
8.1.1	Calendar	141
8.1.2	Public Holiday	144
8.2	Rerouting	145
8.2.1	Rerouting Functions.	145
8.2.2	Rerouting Applications	149
8.3	Voice Applications	150
8.3.1	Wave Files.	151
8.4	System Phonebook	152
8.4.1	Entries	153
8.4.2	Import / Export	154
8.4.3	General	156
8.5	Call Data Records	156
8.5.1	Outgoing	156
8.5.2	Incoming	157
8.5.3	General	158
8.6	Mini Call Center	159
8.6.1	Status	160
8.6.2	Lines	160
8.6.3	Agents	163
8.6.4	General	164
8.7	Doorcom Units	164
8.7.1	Doorcom Units	165
8.7.2	Doorcom Signalling	166
8.8	Alarm Calls	169
8.8.1	Alarm Calls	169
8.9	Voice Mail System	172

8.9.1	Voice Mail Boxes	172
8.9.2	Status	176
8.9.3	General	177
Chapter 9	LAN	179
9.1	IP Configuration	179
9.1.1	Interfaces	179
9.2	VLAN	183
9.2.1	VLANs	183
9.2.2	Port Configuration	184
9.2.3	Administration	185
Chapter 10	Networking	186
10.1	Routes	186
10.1.1	IPv4 Route Configuration	186
10.1.2	IPv4 Routing Table	191
10.1.3	Options	192
10.2	NAT.	193
10.2.1	NAT Interfaces	193
10.2.2	NAT Configuration	194
10.3	QoS	200
10.3.1	QoS Filter	200
10.3.2	QoS Classification	203
10.3.3	QoS Interfaces/Policies	206
10.4	Access Rules	213
10.4.1	Access Filter	214
10.4.2	Rule Chains	217
10.4.3	Interface Assignment	219
10.5	Drop In	220
10.5.1	Drop In Groups.	220

Chapter 11	Multicast	223
11.1	General	224
11.1.1	General	225
11.2	IGMP	225
11.2.1	IGMP	225
11.2.2	Options	227
11.3	Forwarding	228
11.3.1	Forwarding	228
Chapter 12	WAN	230
12.1	Internet + Dialup	230
12.1.1	PPPoE	232
12.1.2	PPTP	237
12.1.3	ISDN	241
12.1.4	IP Pools	248
12.2	Real Time Jitter Control	249
12.2.1	Controlled Interfaces	249
Chapter 13	VPN	251
13.1	IPSec	251
13.1.1	IPSec Peers	252
13.1.2	Phase-1 Profiles	266
13.1.3	Phase-2 Profiles	273
13.1.4	XAUTH Profiles	277
13.1.5	IP Pools	278
13.1.6	Options	279
13.2	L2TP	282
13.2.1	Tunnel Profiles	283

13.2.2	Users	286
13.2.3	Options	290
13.3	PPTP	291
13.3.1	PPTP Tunnels	291
13.3.2	Options	297
13.3.3	IP Pools	298
13.4	GRE	299
13.4.1	GRE Tunnels	299
Chapter 14	Firewall	302
14.1	Policies	303
14.1.1	Filter Rules	303
14.1.2	QoS	306
14.1.3	Options	307
14.2	Interfaces	309
14.2.1	Groups	309
14.3	Addresses	309
14.3.1	Address List	309
14.3.2	Groups	310
14.4	Services	311
14.4.1	Service List	311
14.4.2	Groups	313
Chapter 15	Local Services	314
15.1	DNS	314
15.1.1	Global Settings	316
15.1.2	DNS Servers	318
15.1.3	Static Hosts	319
15.1.4	Domain Forwarding	320
15.1.5	Cache	322

15.1.6	Statistics	322
15.2	HTTPS	323
15.2.1	HTTPS Server	323
15.3	DynDNS Client	324
15.3.1	DynDNS Update	324
15.3.2	DynDNS Provider	326
15.4	DHCP Server	327
15.4.1	IP Pool Configuration	327
15.4.2	DHCP Configuration	328
15.4.3	IP/MAC Binding	331
15.4.4	DHCP Relay Settings	332
15.5	CAPI Server	333
15.5.1	User	333
15.5.2	Options	334
15.6	Scheduling	335
15.6.1	Trigger	335
15.6.2	Actions	340
15.6.3	Options	350
15.7	Surveillance	350
15.7.1	Hosts	351
15.7.2	Interfaces	353
15.7.3	Ping Generator	354
15.8	UPnP	355
15.8.1	Interfaces	355
15.8.2	General	356
15.9	HotSpot Gateway	357
15.9.1	HotSpot Gateway	358
15.9.2	Options	362
15.10	Wake-On-LAN	362
15.10.1	Wake-On-LAN Filter	362

15.10.2	WOL Rules	365
15.10.3	Interface Assignment	367
Chapter 16	Maintenance	368
16.1	Diagnostics	368
16.1.1	Ping Test	368
16.1.2	DNS Test	368
16.1.3	Traceroute Test	368
16.2	Software & Configuration	369
16.2.1	Options	369
16.3	Phone Update	374
16.3.1	Gigaset Phones	375
16.3.2	Firmware Files	376
16.3.3	Settings	377
16.4	Reboot	378
16.4.1	System Reboot	378
Chapter 17	External Reporting	379
17.1	Syslog	379
17.1.1	Syslog Servers	379
17.2	IP Accounting	381
17.2.1	Interfaces	381
17.2.2	Options	382
17.3	Alert Service	383
17.3.1	Alert Recipient	383
17.3.2	Alert Settings	384
17.4	SNMP	386
17.4.1	SNMP Trap Options	386
17.4.2	SNMP Trap Hosts	387

Chapter 18	Monitoring	388
18.1	Status Information	388
18.1.1	Users	388
18.1.2	Teams	389
18.2	Internal Log	390
18.2.1	System Messages	390
18.3	IPSec	390
18.3.1	IPSec Tunnels	391
18.3.2	IPSec Statistics.	392
18.4	Interfaces	393
18.4.1	Statistics	393
18.5	HotSpot Gateway	395
18.5.1	HotSpot Gateway	395
18.6	QoS	395
18.6.1	QoS	395
	Index	397

Chapter 1 Assistants

The **Assistants** menu offers step-by-step instructions for the following basic configuration tasks:

- **First steps**
- **Internet Access**
- **VPN**
- **PBX**

Choose the corresponding task from the navigation bar and follow the instructions and explanations on the separate pages of the Assistant.

Chapter 2 System Management

The **System Management** menu contains general system information and settings.

You see a system status overview. Global system parameters such as the system name, date/time, passwords and licences are managed and the access and authentication methods are configured.

2.1 Status

If you log into the **GUI**, your device's status page is displayed, which shows the most important system information.

You see an overview of the following data:

- System status
- Your device's activities: Resource utilisation, active sessions and tunnels
- Status and basic configuration of the LAN, WAN, ISDN, and ADSL interfaces
- Information on plugged add-on modules (if any)

You can customise the update interval of the status page by entering the desired period in seconds as **Automatic Refresh Interval** and clicking on the **Apply** button.



Caution

Under **Automatic Refresh Interval** do not enter a value of less than 5 seconds, otherwise the refresh interval of the screen will be too short to make further changes!

The menu **System Management->Status** consists of the following fields:

Fields in the System Information menu

Field	Value
Uptime	Displays the time past since the device was rebooted.
System Date	Displays the current system date and system time.
Serial Number	Displays the device serial number.
BOSS Version	Displays the currently loaded version of the system software.
Back-up of configura-	Indicates whether a backup configuration is available on the

Field	Value
tion on SD card	SD card or not.
Last configuration stored	Displays day, date and time of the last saved configuration (boot configuration in flash).
Night Mode Status	Indicates whether your device is in the normal mode (<i>Off</i>) or in night mode (<i>On</i>).

Fields in the Resource Information menu

Field	Value
CPU Usage	Displays the CPU usage as a percentage.
Memory Usage	Displays the usage of the working memory in MByte in relation to the available total working memory in MByte. The usage is also displayed in brackets as a percentage.
Memory Card	Shows the status of any optional external memory card that has been inserted, and the size of the memory in GBytes or MBytes.
Active Sessions (SIF, RTP, etc...)	Displays the total of all SIF, TDRC, and IP load balancing sessions.
Active IPsec Tunnels	Displays the number of currently active IPsec tunnels in relation to the number of configured IPsec tunnels.

Fields in the Modules menu

Feld	Wert
DSP Module	Shows the type of plugged DSP module if any. An acquired fax licence, if any, can be displayed.

Fields in the Physical Interfaces menu

Field	Value
Interface - Connection Information - Link	<p>The physical interfaces are listed here and their most important settings are shown. The system also displays whether the interface is connected or active.</p> <p>Interface specifics for Ethernet interfaces:</p> <ul style="list-style-type: none"> • IP address • Netmask • Not configured

Field	Value
	Interface specifics for ISDN interfaces: <ul style="list-style-type: none"> • Configured • Not configured Interface specifics for xDSL interfaces: <ul style="list-style-type: none"> • Downstream/Upstream Line Speed

Fields in the WAN Interfaces menu

Field	Value
Description - Connection Information - Link	All the WAN interfaces are listed here and their most important settings are shown. The system also displays whether the interface is active.

2.2 Global Settings

The basic system parameters are managed in the **Global Settings** menu.

2.2.1 System

The **System Management->Global Settings->System** menu is used for entering your system's basic data.

The **System Management->Global Settings->System** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Value
System Name	Enter the system name of your device. This is also used as the PPP host name. A character string of up to 255 characters is possible. The device type is entered as the default value.
Location	Enter the location of your device.
Contact	Enter the relevant contact person. Here you can enter the e-

Field	Value
	<p>mail address of the system administrator, for example.</p> <p>A character string of up to 255 characters is possible.</p>
Maximum Number of Syslog Entries	<p>Enter the maximum number of syslog messages that are stored internally in the device.</p> <p>Possible values are <i>0</i> to <i>1000</i>.</p> <p>The default value is <i>50</i>. You can display the stored messages in Monitoring->Internal Log.</p>
Maximum Message Level of Syslog Entries	<p>Select the priority of system messages above which a log should be created.</p> <p>System messages are only recorded internally if they have a higher or identical priority to that indicated, i.e. all messages generated are recorded at syslog level <i>Debug</i>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Emergency</i>: Only messages with emergency priority are recorded. • <i>Alert</i>: Messages with emergency and alert priority are recorded. • <i>Critical</i>: Messages with emergency, alert and critical priority are recorded. • <i>Error</i>: Messages with emergency, alert, critical and error priority are recorded. • <i>Warning</i>: Messages with emergency, alert, critical, error and warning priority are recorded. • <i>Notice</i>: Messages with emergency, alert, critical, error, warning and notice priority are recorded. • <i>Information</i> (default value): Messages with emergency, alert, critical, error, warning, notice and information priority are recorded. • <i>Debug</i>: All messages are recorded.
Maximum Number of Accounting Log Entries	<p>Enter the maximum number of login process entries that are stored internally in the device.</p>

Field	Value
	<p>Possible values are <i>0</i> to <i>1000</i>.</p> <p>The default value is <i>20</i>.</p>

Transfer to busy subscriber

You can define in the configuration whether a call can be transferred to a busy subscriber or, if it is off, that the caller will hear the engaged tone so that the call is terminated. Otherwise the caller is held and hears the ringing tone or the on-hold music. If the destination subscriber hangs up, the held subscriber hears the ringing tone. The destination subscriber is called and can take the held call.

Fields in the menu System Settings

Field	Value
Transfer Signalling	<p>Specify how the call is to be transferred to an internal extension.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>With the ringing tone</i> (the default value): Caller hears the ringing tone while being transferred. • <i>With music on hold (MoH)</i>: The caller hears the system's on-hold music while being transferred.
Transfer to busy extension	<p>Set whether a caller may be transferred to a busy subscriber.</p> <p>The function is activated with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Rerouting to Number	<p>Set the destination to which incoming calls should be diverted to, e. g. in the case of a misdial.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None - Busy Tone</i>: The caller hears the engaged tone by default and cannot be redirected to a destination. • <i><Extension number></i>: By default, the incoming call is routed to the number selected. <p>The default value is the preset internal number <i>40</i> (<i>Team global</i>).</p>

Field	Value
Interconnect external calls	<p>When brokering with two external subscribers, select whether they are to be connected after you hang up.</p> <p>The function is activated with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

Country settings

Your business is an international company with subsidiaries in several countries. Despite the differences in network implementation in the different countries, you want to use the same system in each subsidiary. By setting the respective country variants, the system can be adjusted to the particular features of the network in the required country.

As the system requirements vary from country to country, the functionality of certain features needs to be customised. The basic settings for different country variants are stored in the system.

Fields in the menu Country Settings

Field	Value
Country Profile	<p>Select the country in which you want to use the system.</p> <p>Note: This does not change the language of the text in the system menu of system telephones.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Deutschland</i> (default value) • <i>Nederland</i> • <i>Great Britain</i> • <i>België</i> • <i>Italia</i> • <i>Danmark</i> • <i>España</i> • <i>Sverige</i> • <i>Norge</i> • <i>France</i> • <i>Portugal</i> • <i>Österreich</i>

Field	Value
	<ul style="list-style-type: none"> • <i>Schweiz</i> • <i>Česko</i> • <i>Slovenija</i> • <i>Polska</i> • <i>Magyarország</i> • <i>Ellada</i>
Display Language	<p>Select the language you require for the system menu.</p> <p>The system provides the system telephones with a special menu - the system menu - with typical system functions. The displays in the system menu may be in a variety of languages. These language displays do not depend on the settings in the individual system telephones.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Deutsch</i> (default value) • <i>English</i> • <i>Italian</i>
International Prefix / Country Code	<p>Enter the country code.</p> <p>You need this entry if, e. g., you wish to automatically generate an international number under SIP Provider. You dial, as usual, the national prefix e. g. 05151 909999 and the system then automatically dials +495151 909999. If you fail to enter the country code, you may misdial, as the system will then dial +5151 909999. Without the entry Generate international phone number and International Prefix / Country Code, the full number plus the country code always has to be dialled in the case of SIP providers.</p> <p>Note: Not every SIP provider supports this setting.</p>
National Prefix / City Code	<p>Enter the national prefix and the area code for the location where your system is installed. With a point-to-point ISDN access, this area code is essential, because otherwise e. g. no automatic external callback is possible.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Charge Settings

Field	Value
Charge Rate Factor	Enter the factor for the connection costs. The default value is <i>0.00</i> .
Currency	Here, enter the name of the currency, e. g. <i>EUR</i> , (max. three characters). This entry is just a name which is not involved in any calculation of the tariff unit factor. Special characters are not permitted.
Charge Information (S0 / Upn Extension)	Select the transmission method for charge information on the internal S0 bus. Possible values: <ul style="list-style-type: none"> • <i>Keypad</i>: Depending on country and provider, the charging information is transmitted so as to allow direct display by the terminal. • <i>Functional</i>: The charge information is transmitted in binary, coded form, and the terminal first needs to decode it (EURO ISDN). • <i>Both</i> (default value): Both protocols are recognised.

Fields in the menu Day Mode

Field	Value
Global Rerouting	Select the call variant in day modus that shall apply to the overall system if no specific redirect has been set up. The default value is <i>Variant 1</i> .

Night operation

You can switch the system to night operation and thus enable particular call variants for the team signalling, the door intercom signalling and the rejection functions.

An advanced switching of the call variants is possible via a code or the calendar that has been configured for night operation. You configure a calendar for night operation in the **Applications->Calendar->Calendar->New** menu.

Fields in the menu Night Mode

Field	Value
Team Signalling	Select the call variants for team signalling in night operation.

Field	Value
Doorcom Signalling	Select the door intercom variants for door intercom signalling in night operation.
Rerouting of Incoming Distribution	Select the call variants for reject to message in night operation.
Extension Rerouting	Select the call variants for reject to direct dial-in in night operation.
Global Rerouting	Select the call variants for general rejection in night operation.
Alarm Input	Select the call variants for alarm in night operation.

2.2.2 Passwords

Setting the passwords is another basic system setting.



Note

All bintec elmeg devices are delivered with the same username and password and the same PINs. As long as the passwords or PINs remain unchanged, they are not protected against unauthorised use.

When you log onto your device for the first time, you are prompted to change the password. You need to change the system administrator password in order to be able to configure your device.

Make sure you change all passwords and PIN's to prevent unauthorised access to the device

The **System Management->Global Settings->Passwords** menu consists of the following fields:

Fields in the System Password menu

Field	Value
System Admin Password	Enter the password for the user name <code>admin</code> . This password is also used with SNMPv3 for authentication (MD5) and encryption (DES).
Confirm Admin Password	Confirm the password by entering it again.

Field	Value
word	

PIN1 and PIN2

You can use various protection functions to prevent misuse of your system. Your system settings protect you by means of a 4-digit PIN1 (pin number). Access from outside (remote access) is protected by a 6-character PIN2.

PIN1 is a 4-digit pin number that allows you to protect system settings from unauthorised access. PIN2 is a 6-digit pin number that prevents unauthorised external subscribers from being able to use your system. These functions can only be used after entering a 6-digit PIN2.

Various settings are protected by the system's PIN1. In the basic setting, the PIN1 is set to *none*.

The following performance features are protected using PIN2:

- Remote access for Follow me, room monitoring

Fields in the Configuration via Phone (4-Digit Numeric PIN) menu

Field	Value
PIN1	Enter PIN1. With the 4-digit PIN1 (PIN number) you protect your system settings through configuration via telephone.

Fields in the Remote Access to Phone (6-Digit Numeric PIN) menu

Field	Value
Remote Access (e.g. Follow me, Room Monitoring)	Select whether a remote access of your system is to be permitted. The function is activated with <i>Enabled</i> . The function is disabled by default.
PIN2	Only if Remote Access (e.g. Follow me, Room Monitoring) is enabled. Enter the PIN2 . The default value is <i>000000</i> .

Field	Value
	Through the 6-digit PIN2 you protect from external access (remote access).

Fields in the SNMP Communities menu

Field	Value
SNMP Read Community	Enter the password for the user name <code>read</code> .
SNMP Write Community	Enter the password for the user name <code>write</code> .

Field in the Global Password Options menu

Field	Value
Show passwords and keys in clear text	<p>Define whether the passwords are to be displayed in clear text (plain text).</p> <p>The function is enabled with <code>Show</code></p> <p>The function is disabled by default.</p> <p>If you activate the function, all passwords and keys in all menus are displayed and can be edited in plain text.</p> <p>One exception is IPSec keys. They can only be entered in plain text. After pressing OK or calling the menu again, they are displayed as asterisks.</p>

2.2.3 Date and Time

You need the system time for tasks such as correct time-stamps for system messages, or accounting.

You have the following options for determining the system time (local time):

ISDN/Manual

The system time can be updated via ISDN, i.e. with every existing external connection the date and time are taken from the ISDN. The date and time can also be entered manually, e. g. if time and date are not sent in the ISDN or no time server is provided. The time remains for approx. 3 hours after the system's power supply is switched off.

The clock switches from summer to winter time (and back) automatically. This is independent of the exchange time or the ntp server time. Summer time starts on the last Sunday in March by switching from 2 a.m. to 3 a.m. The calendar-related or schedule-related switches that are scheduled for the missing hour are then carried out. Winter time starts on the last Sunday in October by switching from 3 a.m. to 2 a.m. The calendar-related or schedule-related switches that are scheduled for the additional hour are then carried out.

Time server

You can obtain the system time automatically, e.g. using various time servers. To ensure that the device uses the desired current time, you should configure one or more time servers.



Note

If a method for automatically deriving the time is defined on the device, the values obtained in this way automatically have higher priority. A manually entered system time is therefore overwritten.

The menu **System Management**->**Global Settings**->**Date and Time** consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Time Zone	Select the time zone in which your device is installed. You can select Universal Time Coordinated (UTC) plus or minus the deviation in hours or a predefined location, e. g. <i>Europe/Berlin</i> .
Current Local Time	The current date and current system time are shown here. The entry cannot be changed.

Fields in the Manual Time Settings menu

Field	Description
Set Date	Enter a new date. Format: <ul style="list-style-type: none"> • Day: dd

Field	Description
	<ul style="list-style-type: none"> • Month: mm • Year: yyyy
Set Time	<p>Enter a new time.</p> <p>Format:</p> <ul style="list-style-type: none"> • Hour: hh • Minute: mm

Fields in the Automatic Time Settings (Time Protocol) menu

Field	Description
ISDN Timeserver	<p>Determine whether the system time is to be updated via ISDN.</p> <p>If a time server is configured, the time is only determined over ISDN until a successful update is received from this time server. Updating over ISDN is deactivated for the period in which the time is determined by means of a time server.</p> <p>The function is activated with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
First Timeserver	<p>Enter the primary time server, by using either a domain name or an IP address.</p> <p>In addition, select the protocol for the time server request.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (default value): This server uses the simple network time protocol via UDP port 123. • <i>Time Service / UDP</i>: This server uses the Time service with UDP port 37. • <i>Time Service / TCP</i>: This server uses the Time service with TCP port 37. • <i>None</i>: This time server is not currently used for the time request. <p>Ex works, the <i>ntp1.sda.t-online.de</i> server is entered here.</p>

Field	Description
Second Timeserver	<p>Enter the secondary time server, by using either a domain name or an IP address.</p> <p>In addition, select the protocol for the time server request.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (default value): This server uses the simple network time protocol via UDP port 123. • <i>Time Service / UDP</i>: This server uses the Time service with UDP port 37. • <i>Time Service / TCP</i>: This server uses the Time service with TCP port 37. • <i>None</i>: This time server is not currently used for the time request. <p>Ex works, the <i>ntp1.sul.t-online.de</i> server is entered here.</p>
Third Timeserver	<p>Enter the third time server, by using either a domain name or an IP address.</p> <p>In addition, select the protocol for the time server request.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (default value): This server uses the simple network time protocol via UDP port 123. • <i>Time Service / UDP</i>: This server uses the Time service with UDP port 37. • <i>Time Service / TCP</i>: This server uses the Time service with TCP port 37. • <i>None</i>: This time server is not currently used for the time request.
Time Update Interval	<p>Enter the time interval in minutes at which the time is automatically updated.</p> <p>The default value is <i>1440</i>.</p>
Time Update Policy	<p>Enter the time period after which the system attempts to contact the time server again following a failed time update.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Normal</i> (default value): The system attempts to contact the time server after 1, 2, 4, 8, and 16 minutes. • <i>Aggressive</i>: For ten minutes, the system attempts to contact the time server after 1, 2, 4, 8 seconds and then every 10 seconds. • <i>Endless</i>: For an unlimited period, the system attempts to contact the time server after 1, 2, 4, 8 seconds and then every 10 seconds. <p>If certificates are used to encrypt data traffic in a VPN, it is extremely important that the correct time is set on the device. To ensure this is the case, for Time Update Policy, select the value <i>Endless</i>.</p>
Internal Time Server	<p>Select whether the internal timeserver is to be used.</p> <p>The function is activated by selecting <i>Enabled</i>. Time requests from a client will be answered with the current system time. This is given as GMT, without offset.</p> <p>The function is enabled by default. Clients' time requests are answered in the LAN.</p>

2.2.4 Timer

In the **Timer** menu you can configure the times at which particular system features are to be switched on by default.

The menu **System Management->Global Settings->Timer** consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Call Forwarding (CFNR)	<p>Enter the time after which a Call Forwarding (CFNR) will be executed.</p> <p>Possible values are 1 to 99.</p> <p>The default value is 15.</p>

Field	Description
Direct Call	<p>Enter the time after which the configured number will be dialled when the receiver is lifted.</p> <p>You wish to set up a telephone for which the connection to a specific number is established without entering the number (e.g. emergency telephone). You are not at home. However, there is someone at home who needs to be able to reach you quickly and easily by telephone if necessary (e. g. children or grandparents). If you have set up the "Direct Call" function for one or more telephones, the receiver of the corresponding telephone only needs to be lifted. After a time period without further entries set in configuration, the system automatically dials the configured direct call number.</p> <p>If you do not dial within the specified period from picking up the receiver, automatic dialling is initiated.</p> <p>Possible values are <i>1</i> to <i>30</i>.</p> <p>The default value is <i>5</i>.</p>
External Door Connections	<p>If an external telephone requests a door intercom call, here you can set the time after which this call is forcefully terminated.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>infinite</i> • <i>60 seconds</i> • <i>120 seconds</i> • <i>180 seconds</i> (default value) • <i>240 seconds</i> • <i>300 seconds</i>

Fields in the Advanced Settings menu

Field	Value
Explicit Call Transfer	<p>Enter the time after which the initiating subscriber is to be called back or hear call waiting if the required subscriber could not be reached.</p> <p>You have passed a caller to another subscriber by brokering or transfer. This subscriber cannot be reached or is engaged. But you wish to prevent the subscriber terminating the call or being</p>

Field	Value
	<p>diverted by the system after a time. You achieve this using an automatic callback to your telephone. In the case of calls which are transferred with no message (special call transfer, UbA), a callback or call waiting (if there is already a new call) is made to the initiating subscriber after the time entered here.</p> <p>Possible values are <i>10 to 179</i>.</p> <p>The default value is <i>30</i>.</p>
<p>Transfer to busy extension</p>	<p>Enter the time after which a subscriber in the waiting loop is re-connected with the switchboard.</p> <p>The switchboard wishes to pass a call to a particular employee. However, this person is currently on the phone. The call can then be switched to the subscriber's waiting loop. If the call is not taken in the time entered here, the switchboard is called again.</p> <p>Possible values are <i>10 to 600</i>.</p> <p>The default value is <i>30</i>.</p>
<p>System Parked Enquiry</p>	<p>Enter the time after which an open hold for enquiry is terminated and the subscriber called back or given a call waiting.</p> <p>You are making a call and want to transfer it to a colleague. Unfortunately, you do not know where this colleague is. System Parking (Open Enquiry) holds the caller in the system's queue. You can now make an announcement from your telephone to notify your colleague that the call is waiting. Using a code for the open hold for enquiry, the colleague can take the call on any telephone.</p> <p>If a call waiting in the queue is not taken by a subscriber within the time entered here, the initiating subscriber is called back or given a call waiting.</p> <p>Possible values are <i>10 to 600</i>.</p> <p>The default value is <i>30</i>.</p>

2.2.5 System Licences

This chapter shows the software licenses enabled ex works.


The options for editing, new entries and restore are not usually required.

Possible values for Status

Licence	Meaning
OK	Subsystem is activated.
Not OK	Subsystem is not activated.
Not supported	You have entered a licence for a subsystem your system does not support.

The **System Licence ID** is also displayed above the list.

2.2.5.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to enter more licences.

The menu **System Management->Global Settings->System Licences->New** consists of the following fields:

Fields in the Basic Settings menu

Field	Value
Licence Serial Number	Enter the licence serial number you received when you bought the licence.
Licence Key	Enter the licence key you received by e-mail.

2.3 Access Codes

In your day-to-day work you have employed codes to use particular features and you wish to use them again with your new system. However, other codes are set for these features in the basic setting. No problem - you can change the codes for different features. So you can use your usual codes for these features in the future.

2.3.1 Alternative Access Codes

You use the **Alternative Access Codes** menu to configure the system's access number plan.

The access number can be set individually for some performance features in the system configuration. The access number preset in the system is supplemented with a call number from the system's internal number plan. For performance features **Open inquiry** and **Bundles**, several access codes can be assigned. The performance feature with modified access number is operated as described for the corresponding performance feature. You can use the modified access number (internal number) or the access number described in the user guide (excluding dialling code).

The **System Management->Access Codes->Alternative Access Codes** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Line Access Digit	Select the exchange code. Possible values: <ul style="list-style-type: none"> • <i>None</i> • 0 (default value) • 6 • 7 • 8 • 9
Pick-up Group	Enter the new code for performance feature Pick-up (group) .
Pick-up (Extension)	Enter the new code for performance feature Pick-up (internal subscriber) .
Assign project codes	Enter the new code for performance feature Assign project codes .
Speed Dial	Enter the new code for performance feature Speed Dial .
Trunk Group Selection	Create the new access numbers for the Trunk Group Selection feature.

Field	Description
	To do this, first click Add to create a bundle selection, select the bundle and enter the access number you require for the bundle.
System Parking (Open Enquiry)	<p>Create the new access numbers for the System Parking (Open Enquiry) feature.</p> <p>To do this, first click Add to create a queue in which the caller is to be held, and enter the access number you require for the queue. You can create a maximum of 10 entries.</p>

2.4 Interface Mode / Bridge Groups

In this menu, you define the operation mode for your device's interfaces.

Routing versus bridging

Bridging connects networks of the same type. In contrast to routing, bridges operate at layer 2 of the OSI model (data link layer), are independent of higher-level protocols and transmit data packets using MAC addresses. Data transmission is transparent, which means the information contained in the data packets is not interpreted.

With routing, different networks are connected at layer 3 (network layer) of the OSI model and information is routed from one network to the other.

Conventions for port/interface names

If your device has a radio port, it receives the interface name *WLAN*. If there are several radio modules, the names of wireless ports in the user interface of your device are made up of the following parts:

- (a) *WLAN*
- (b) Number of the physical port (1 or 2)

Example: *WLAN1* The name of the Ethernet port is made up of the following parts:

- (a) *ETH*
- (b) Number of the port

Example: *ETH1*

The name of the interface connected to an Ethernet port is made up of the following parts:

- (a) Abbreviation for interface type, whereby *en* stands for internet.
- (b) Number of the Ethernet port
- (c) Number of the interface

Example: *en1-0* (first interface on the first Ethernet port)

The name of the bridge group is made up of the following parts:

- (a) Abbreviation for interface type, whereby *br* stands for bridge group.
- (b) Number of the bridge group

Example: *br0* (first bridge group)

The name of the wireless network (VSS) is made up of the following parts:

Abbreviation for interface type, whereby *vss* stands for wireless network.

- (a) Number of the wireless module
- (b) Number of the interface

Example: *vss1-0* (first wireless network on the first wireless module)

The name of the WDS link or bridge link is made up of the following parts:

- (a) Abbreviation for interface type
- (b) Number of the wireless module on which the WDS link or bridge link is configured
- (c) Number of the WDS link or bridge link

Example: *wds1-0* (first WDS link or bridge link on the first wireless module)

The name of the client link is made up of the following parts:

- (a) Abbreviation for interface type
- (b) Number of the wireless module on which the client link is configured
- (c) Number of the client link

Example: *sta1-0* (first client link on the first wireless module)

The name of the virtual interface connected to an Ethernet port is made up of the following parts:

- (a) Abbreviation for interface type
- (b) Number of the Ethernet port
- (c) Number of the interface connected to the Ethernet port

(d) Number of the virtual interface

Example: *en1-0-1* (first virtual interface based on the first interface on the first Ethernet port)

2.4.1 Interfaces

You define separately whether each interface is to operate in routing or bridging mode.

If you want to set bridging mode, you can either use existing bridge groups or create a new bridge group.

The default setting for all existing interfaces is routing mode. When selecting the option *New Bridge Group* for **Mode / Bridge Group**, a bridge group, i.e. *br0, br1* etc. is automatically created and the interface is run in bridging mode.

The **System Management->Interface Mode / Bridge Groups->Interfaces** menu consists of the following fields:

Fields in the Interfaces menu

Field	Description
Interface Description	Displays the name of the interface.
Mode / Bridge Group	Select whether you want to run the interface in <i>Routing Mode</i> or whether you want to assign the interface to an existing (<i>br0, br1</i> etc.) or new bridge group (<i>New Bridge Group</i>). When selecting <i>New Bridge Group</i> , a new bridge group is automatically created after you click the OK button.
Configuration Interface	Select the interface via which the configuration is to be carried out. Possible values: <ul style="list-style-type: none"> • <i>Select one</i> (default value): Ex works setting The right configuration interface must be selected from the other options. • <i>Ignore</i>: No interface is defined as configuration interface. • <i><Interface name></i>: Select the interface to be used for configuration. If this interface is in a bridge group, it is assigned the group's IP address when it is taken out of the group.

2.4.1.1 Add

Choose the **Add** button to edit the mode of PPP interfaces.

The **System Management->Interface Mode / Bridge Groups->Interfaces->Add** menu consists of the following fields:

Fields in the Interfaces menu

Field	Description
Interface	Select the interface whose status should be changed.

2.5 Administrative Access

In this menu, you can configure the administrative access to the device.


2.5.1 Access

In the **System Management->Administrative Access->Access** menu, a list of all IP-capable interfaces is displayed.

For an Ethernet interface you can select the access parameters *Telnet, SSH, HTTP, HT-TPS, Ping, SNMP* and for the ISDN interfaces *ISDN Login*.

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Restore Default Settings	Only when you make changes to the administrative access configuration are relevant access rules set up and activated. You can restore the default settings with the  icon.

2.5.1.1 Add

Select the **Add** button to configure administrative access for additional interfaces.

The **System Management->Administrative Access->Access->Add** menu consists of the following fields:

Fields in the menu Access

Field	Description
Interface	Select the interface for which administrative access is to be configured.

2.5.2 SSH

Your devices offers encrypted access to the shell. You can enable or disable this access in the **System Management->Administrative Access->SSH Enabled** menu (standard value). You can also access the options for configuring the SSH login.

You need an SSH client application, e.g. PuTTY, to be able to reach the SSH Daemon.

If you wish to use SSH Login together with the PuTTY client, you may need to comply with some special configuration requirements, for which we have prepared FAQs. You will find these in the Service/Support section at www.gigasetpro.com.

To be able to reach the shell of your device via an SSH client, make sure the settings for the SSH Daemon and SSH client are the same.



Note

If configuration of an SSH connection is not possible, restart the device to initialise the SSH Daemon correctly.

The **System Management->Administrative Access->SSH** menu consists of the following fields:

Fields in the menu SSH (Secure Shell) Parameters

Field	Value
SSH service active	Select whether the SSH Daemon is to be enabled for the interface. The function is activated by selecting <i>Enabled</i> . The function is enabled by default.
SSH Port	Here you can enter the port via which the SSH connection is to be established. The default value is <i>22</i> .

Field	Value
Maximum number of concurrent connections	<p>Enter the maximum number of simultaneously active SSH connections.</p> <p>The default value is <i>1</i>.</p>

Fields in the menu Authentication and Encryption Parameters

Field	Value
Encryption Algorithms	<p>Select the algorithms that are to be used to encrypt the SSH connection.</p> <p>Possible options:</p> <ul style="list-style-type: none"> • <i>3DES</i> • <i>Blowfish</i> • <i>AES-128</i> • <i>AES-256</i> <p>By default <i>3DES</i>, <i>Blowfish</i> and <i>AES-128</i> are enabled.</p>
Hashing Algorithms	<p>Select the algorithms that are to be available for message authentication of the SSH connection.</p> <p>Possible options:</p> <ul style="list-style-type: none"> • <i>MD5</i> • <i>SHA-1</i> • <i>RipeMD 160</i> <p>By default <i>MD5</i>, <i>SHA-1</i> and <i>RipeMD 160</i> are enabled.</p>

Fields in the menu Key Status

Field	Value
RSA Key Status	<p>Shows the status of the RSA key.</p> <p>If an RSA key has not been generated yet, <i>Not generated</i> is displayed in red and a link, <i>Generate</i>, is provided. If you select the link, the generation process is triggered and the view is updated. The <i>Generating</i> status is displayed in green. When generation has been completed successfully, the status changes from <i>Generating</i> to <i>Generated</i>. If an error occurs during the generation, <i>Not generated</i> and the <i>Generate</i></p>

Field	Value
	<p>link are displayed again. You can then repeat generation.</p> <p>If the <i>Unknown</i> status is displayed, generation of a key is not possible, for example because there is not enough space in the FlashROM.</p>
DSA Key Status	<p>Shows the status of the DSA key.</p> <p>If no DSA key has yet been generated, <i>Not generated</i> is displayed in red and a link, <i>Generate</i>, is provided. If you select the link, the generation process is triggered and the view is updated. The <i>Generating</i> status is displayed in green. When generation has been completed successfully, the status changes from <i>Generating</i> to <i>Generated</i>. If an error occurs during the generation, <i>Not generated</i> and the <i>Generate</i> link are displayed again. You can then repeat generation.</p> <p>If the <i>Unknown</i> status is displayed, generation of a key is not possible, for example because there is not enough space in the FlashROM.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the menu **Advanced Settings**

Field	Value
Login Grace Time	<p>Enter the time (in seconds) that is available for establishing the connection. If a client cannot be successfully authenticated during this time, the connection is terminated.</p> <p>The default value is <i>600</i> seconds.</p>
Compression	<p>Select whether data compression should be used.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
TCP Keepalives	<p>Select whether the device is to send keepalive packets.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Logging Level	<p>Select the syslog level for the syslog messages generated by</p>

Field	Value
	<p>the SSH Daemon.</p> <p>Possible settings:</p> <ul style="list-style-type: none"> • <i>Information</i> (default value): Fatal and simple errors of the SSH Daemon and information messages are recorded. • <i>Fatal</i>: Only fatal errors of the SSH Daemon are recorded. • <i>Error</i>: Fatal and simple errors of the SSH Daemon are recorded. • <i>Debug</i>: All messages are recorded.

2.5.3 SNMP

SNMP (Simple Network Management Protocol) is a network protocol used to monitor and control network elements (e.g. routers, servers, switches, printers, computers etc.) from a central station. SNMP controls communication between the monitored devices and monitoring station. The protocol describes the structure of the data packets that can be transmitted, as well as the communication process.

The data objects queried via SNMP are structured in tables and variables and defined in the MIB (Management Information Base). This contains all the configuration and status variables of the device.

SNMP can be used to perform the following network management tasks:

- Surveillance of network components
- Remote controlling and configuration of network components
- Error detection and notification

You use this menu to configure the use of SNMP.

The menu **System Management->Administrative Access->SNMP** consists of the following fields:

Fields in the Basic Settings menu

Field	Value
SNMP Version	<p>Select the SNMP version your device is to use to listen for external SNMP access.</p> <p>Possible values:</p>

Field	Value
	<ul style="list-style-type: none"> • <i>v1</i>: SNMP Version 1 • <i>v2c</i>: Community-Based SNMP Version 2 • <i>v3</i>: SNMP Version 3 <p>By default, <i>v1</i>, <i>v2c</i> and <i>v3</i> are enabled.</p> <p>If no option is selected, the function is deactivated.</p>
SNMP Listen UDP Port	<p>Shows the UDP port (<i>161</i>) at which the device receives SNMP requests.</p> <p>The value cannot be changed.</p>

**Tip**

If your SNMP Manager supports SNMPv3, you should, if possible, use this version as older versions transfer all data unencrypted.

2.6 Remote Authentication

This menu contains the settings for user authentication.

2.6.1 RADIUS

RADIUS (Remote Authentication Dial In User Service) is a service that enables authentication and configuration information to be exchanged between your device and a RADIUS server. The RADIUS server administrates a database with information about user authentication and configuration and for statistical recording of connection data.

RADIUS can be used for:

- Authentication
- Accounting
- Exchange of configuration data

For an incoming connection, your device sends a request with user name and password to the RADIUS server, which then searches its database. If the user is found and can be authenticated, the RADIUS server sends corresponding confirmation to your device. This confirmation also contains parameters (called RADIUS attributes), which your device uses as WAN connection parameters.

If the RADIUS server is used for accounting, your device sends an accounting message at the start of the connection and a message at the end of the connection. These start and end messages also contain statistical information about the connection (IP address, user name, throughput, costs).

RADIUS packets


The following types of packets are sent between the RADIUS server and your device (client):

Packet types

Field	Value
ACCESS_REQUEST	Client -> Server If an access request is received by your device, a request is sent to the RADIUS server if no corresponding connection partner has been found on your device.
ACCESS_ACCEPT	Server -> Client If the RADIUS server has authenticated the information contained in the ACCESS_REQUEST, it sends an ACCESS_ACCEPT to your device together with the parameters used for setting up the connection.
ACCESS_REJECT	Server -> Client If the information contained in the ACCESS_REQUEST does not correspond to the information in the user database of the RADIUS server, it sends an ACCESS_REJECT to reject the connection.
ACCOUNTING_START	Client -> Server If a RADIUS server is used for accounting, your device sends an accounting message to the RADIUS server at the start of each connection.
ACCOUNTING_STOP	Client -> Server If a RADIUS server is used for accounting, your device sends an accounting message to the RADIUS server at the end of each connection.

A list of all entered RADIUS servers is displayed in the **System Management->Remote Authentication->RADIUS** menu.

2.6.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to add RADIUS servers.

The **System Management->Remote Authentication->RADIUS->New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Value
Authentication Type	<p>Select what the RADIUS server is to be used for.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>PPP Authentication</i> (default value only for PPP connections): The RADIUS server is used for controlling access to a network. • <i>Accounting</i> (for PPP connections only): The RADIUS server is used for recording statistical call data. • <i>Login Authentication</i>: The RADIUS server is used for controlling access to the SNMP shell of your device. • <i>IPSec Authentication</i>: The RADIUS server is used for sending configuration data for IPSec peers to your device. • <i>XAUTH</i>: The RADIUS server is used for authenticating IPSec peers via XAuth.
Vendor Mode	<p>Only for Authentication Type = <i>Accounting</i></p> <p>In hotspot applications, select the mode define by the provider.</p> <p>In standard applications, leave the value set to <i>Default</i>.</p> <p>Possible values for hotspot applications:</p> <ul style="list-style-type: none"> • <i>France Telecom</i>: For France Telecom hotspot applications. • <i>bintec HotSpot Server</i>: For hotspot applications.
Server IP Address	<p>Enter the IP address of the RADIUS server.</p>

Field	Value
RADIUS Secret	Enter the shared password used for communication between the RADIUS server and your device.
Default User Password	Some Radius servers require a user password for each RADIUS request. Enter the password that your device sends as the default user password in the prompt for the dialout routes on the RADIUS server.
Priority	<p>If a number of RADIUS server entries were created, the server with the highest priority is used first. If this server does not answer, the server with the next-highest priority is used.</p> <p>Possible values from 0 (highest priority) to 7 (lowest priority).</p> <p>The default value is 0.</p> <p>See also Policy in the Advanced Settings.</p>
Entry active	<p>Select whether the RADIUS server configured in this entry is to be used.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Group Description	<p>Define a new RADIUS group description or assign the new RADIUS entry to a predefined group. The configured RADIUS servers for a group are queried according to Priority and the Policy.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>New</i> (default value): Enter a new group description in the text field. • <i>Default Group 0</i>: Select this entry for special applications, such as Hotspot Server configuration. • <i><Group Name></i>: Select a predefined group from the list.

The **Advanced Settings** menu consists of the following fields:

Fields in the Advanced Settings menu

Field	Value
Policy	Select how your device is to react if a negative response to a

Field	Value
	<p>request is received.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Authoritative</i> (default value): A negative response to a request is accepted. • <i>Non-authoritative</i>: A negative response to a request is not accepted. A request is sent to the next RADIUS server until your device receives a response from a server configured as authoritative.
UDP Port	<p>Enter the UDP port to be used for RADIUS data.</p> <p>RFC 2138 defines the default ports 1812 for authentication (1645 in older RFCs) and 1813 for accounting (1646 in older RFCs). You can obtain the port to be used from the documentation for your RADIUS server.</p> <p>The default value is <i>1812</i>.</p>
Server Timeout	<p>Enter the maximum wait time between ACCESS_REQUEST and response in milliseconds.</p> <p>After timeout, the request is repeated according to Retries or the next configured RADIUS server is requested.</p> <p>Possible values are whole numbers between <i>50</i> and <i>50000</i>.</p> <p>The default value is <i>1000</i> (1 second).</p>
Alive Check	<p>Here you can activate a check of the accessibility of a RADIUS server in Status <i>Down</i> .</p> <p>An Alive Check is carried out regularly (every 20 seconds) by sending an ACCESS_REQUEST to the IP address of the RADIUS server. If the server is reachable, Status is set to <i>alive</i> again. If the RADIUS server is only reachable over a switched line (dialup connection), this can cause additional costs if the server is <i>down</i> for a long time.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Retries	<p>Enter the number of retries for cases when there is no re-</p>

Field	Value
	<p>response to a request. If an response has still not been received after these attempts, the Status is set to <i>down</i>. In Alive Check = Enabled your device attempts to reach the server every 20 seconds. If the server responds, Status is set back to <i>alive</i> .</p> <p>Possible values are whole numbers between 0 and 10.</p> <p>The default value is 1. To prevent Status being set to <i>down</i>, set this value to 0.</p>
RADIUS Dialout	<p>Only for Authentication Type = PPP Authentication and <i>IPSec Authentication</i>.</p> <p>Select whether your device receives requests from RADIUS server dialout routes. This enables temporary interfaces to be configured automatically and your device can initiate outgoing connections that are not configured permanently.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>If the function is active, you can enter the following options:</p> <ul style="list-style-type: none"> • <i>Reload Interval</i>: Enter the time period in seconds between update intervals. <p>The default entry here is 0 i.e. an automatic reload is not carried out.</p>

2.6.2 TACACS+

TACACS+ permits access control for your device, network access servers (NAS) and other network components via one or more central servers.

Like RADIUS, TACACS+ is an AAA protocol and offers authentication, authorisation and accounting services (TACACS+ Accounting is currently not supported by bintec elmeg devices).


The following TACACS+ functions are available on your device:

- Authentication for login shell
- Command authorisation on the shell (e.g. telnet, show)

TACACS+ uses TCP port 49 and establishes a secure and encrypted connection.

A list of all entered TACACS+ servers is displayed in the **System Management->Remote Authentication->TACACS+** menu.

2.6.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to add TACACS+ servers.

The **System Management->Remote Authentication->TACACS+ ->New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Authentication Type	Displays which TACACS+ function is to be used. The value cannot be changed. Possible values: <ul style="list-style-type: none"> • <i>Login Authentication</i>: Here, you can define whether the current TACACS+ server is to be used for login authentication to your device.
Server IP Address	Enter the IP address of the TACACS+ server that is to be requested for login authentication.
TACACS+ Secret	Enter the password to be used to authenticate and, if applicable, encrypt data exchange between the TACACS+ server and the network access server (your device). The maximum length of the entry is 32 characters.
Priority	Assign a priority to the current TACACS+ server. The server with the lowest value is the one used first for TACACS+ login authentication. If no response is given or access is denied (only if Policy = <i>Non-authoritative</i>), the entry with the next-highest priority is used. The available values are 0 to 9, the default value is 0.
Entry active	Select whether this server is to be used for login authentication. The function is activated by selecting <i>Enabled</i> . The function is enabled by default.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Policy	<p>Select the interpretation of the TACACS+ response.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Non-authoritative</i> (default value): The TACACS+ servers are queried in order of their priority (see Priority) until a positive response is received or a negative response has been received from an authoritative server. • <i>Authoritative</i>: A negative response to a request is accepted, i.e. a request is not sent to another TACACS+ server. <p>The device's internal user administration is not turned off by TACACS+. It is checked after all TACACS+ servers have been queried.</p>
TCP Port	<p>Shows the default TCP port (49) used for the TACACS+ protocol. The value cannot be changed.</p>
Timeout	<p>Enter time in seconds for which the NAS is to wait for a response from TACACS+.</p> <p>If a response is not received during the wait time, the next configured TACACS+ server is queried (only if Policy = <i>Non-authoritative</i>) and the status of the current server is set to <i>Blocked</i>.</p> <p>The possible values are 1 to 60, the default value is 3.</p>
Block Time	<p>Enter the time in seconds for which the status of the current server shall remain blocked.</p> <p>When the block has ended, the server is set to the status specified in the Entry active field.</p> <p>The possible values are 0 to 3600, the default value is 60. The value 0 means that the server is never set to <i>Blocked</i> status and thus no other servers are queried.</p>
Encryption	<p>Select whether data exchange between the TACACS+ server and the NAS is to be encrypted with MD5.</p>

Field	Description
	<p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p> <p>If the function is not enabled, the packets and all related information are transferred unencrypted. Unencrypted transfer is not recommended as a default setting and should only be used for debugging.</p>

2.6.3 Options

This setting possible here causes your device to carry out authentication negotiation for incoming calls, if it cannot identify the calling party number (e.g. because the remote terminal does not signal the calling party number). If the data (password, partner PPP ID) obtained by executing the authentication protocol is the same as the data of a listed remote terminal or RADIUS user, your device accepts the incoming call.

The menu **System Management->Remote Authentication->Options** consists of the following fields:

Fields in the Global RADIUS Options menu


Field	Description
Authentication for PPP Dialin	<p>By default, the following authentication sequence is used for incoming calls with RADIUS: First CLID, then PPP and then PPP with RADIUS.</p> <p>Options:</p> <ul style="list-style-type: none"> • <i>Inband</i>: Only inband RADIUS requests (PAP,CHAP, MS-CHAP V1 & V2) (i.e. PPP requests without CLID) are sent to the RADIUS server defined in Server IP Address. • <i>Outband (CLID)</i> : Only outband RADIUS requests (i.e. requests for calling line identification = CLID) are sent to the RADIUS server. <p><i>Inband</i> is enabled by default.</p>



2.7 Configuration Access

In the **Configuration Access** menu you can configure user profiles.


To do so, you create access profiles and users and assign each user at least one access profile. An access profile makes available that part of the GUI that a user requires for their tasks. Parts of the GUI that are not required are blocked.

2.7.1 Access Profiles

The menu **System Management->Configuration Access->Access Profiles** displays a list of all the access profiles that have been configured. You can delete existing entries with the icon .

By default, more than one access profile has already been created for the devices **hybird 120**. You can reset these to the default settings using the icon  and the icon .

2.7.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create additional access profiles.


To create an access profile you can use all the entries in the navigation bar of the GUI plus **Save configuration** and **Switch to SNMP Browser**. You can create a maximum of 29 access profiles.


The menu **System Management->Configuration Access->Access Profiles->New** consists of the following fields:

Fields in the menu Basic Settings





Field	Description
Description	Enter a unique name for the access profile.
Level No.	The system automatically assigns a sequential number to the access profile. This cannot be edited.



Fields in the menu Buttons

Field	Description
Save configuration	<p>If you activate the button Save configuration the user is permitted to save configurations.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>Note that the passwords in the saved file can be viewed in clear text.</p> </div>


Field	Description
	<p>Enable or disable Save configuration.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Switch to SNMP Browser	<p>If you activate the button Switch to SNMP Browser, the user can switch to the SNMP browser view, access the parameters and modify all the settings displayed there.</p> <p> Caution</p> <p>Note that the permission for Switch to SNMP Browser means that the user can access the entire MIB, because no individual access profile can be created in this view. The user can save the changed MIB with the permission for Save configuration.</p> <p>With the permission for Switch to SNMP Browser you remove the configured GUI restrictions at the MIB level once more.</p> <p>Enable or disable Switch to SNMP Browser.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>


Fields in the menu Navigation Entries



Field	Description
Menus	<p>You see all the menus from the GUI's navigation bar. Menus that contain at least one sub-menu are flagged by  and . The icon  indicates pages.</p> <p>When you create a new access profile, no elements are assigned yet, i.e. all the available menus, sub-menus and pages are flagged with the icon .</p> <p>Each element in the navigation bar can have three values. Click the icon in the row you want to display these three val-</p>

Field	Description
	<p>ues.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Deny</i>: The menu and all its lower-level menus are blocked. • <i>Allow</i>: The menu is released. Lower-level menus may need to be specifically released. • <i>Allow all</i>: The menu and all its lower-level menus are released. <p>You can select <i>Allow</i> and <i>Allow all</i> in the corresponding row to assign elements to the current access profile.</p> <p>Elements that are assigned to the current access profile are flagged with the icon .</p> <p> indicates a menu that is blocked, but which has at least one released sub-menu.</p>


2.7.2 Users

The menu **System Management->Configuration Access->Users** displays a list of all the users that have been configured. You can delete existing entries with the icon .

You can click the button  to display the details of the configured user. You can see which fields and menus are assigned to the user.

The icon  means that **Read-only** is permitted. If a row is flagged with the icon the information is released for reading and writing. The icon  indicates blocked entries.

2.7.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to enter additional users.

The menu **System Management->Configuration Access->Users->New** consists of the following fields:

Fields in the menu Basic Settings

Field	Description
User	Enter a unique name for the user.

Field	Description
Password	Enter a password for the user.
User must change password	<p>The administrator can use the option User must change password to specify that the user must select their own password the first time they log in. To do this, the option Save configuration needs to be enabled in the menu Access Profiles. If this option is not enabled, a warning message displays.</p> <p>Enable or disable User must change password.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Access Level	<p>Use Add to assign at least one access profile to the user. Selecting Read-only specifies that the user can view the parameters of the access profile, but not change them. Selecting Read-only is only possible if the option Switch to SNMP Browser in the menu Access Profiles is not enabled.</p> <p>If the option Switch to SNMP Browser is enabled, a warning message displays because the user can switch to the SNMP browser view, access the parameters and make any changes they like. The option Read-only is not available in the SNMP browser view.</p> <p>If intersecting access profiles are assigned to a user, read and write have a higher priority than Read-only. Buttons cannot be set to the setting Read-only.</p>

2.8 Certificates

An asymmetric cryptosystem is used to encrypt data to be transported in a network, to generate or check digital signatures and the authenticate users. A key pair consisting of a public key and a private key is used to encrypt and decrypt the data.

For encryption the sender requires the public key of the recipient. The recipient decrypts the data using his private key. To ensure that the public key is the real key of the recipient and is not a forgery, a so-called digital certificate is required.

This confirms the authenticity and the owner of a public key. It is similar to an official passport in that it confirms that the holder of the passport has certain characteristics, such as gender and age, and that the signature on the passport is authentic. As there is more than one certificate issuer, e.g. the passport office for a passport, and as such certificates can

be issued by several different issuers and in varying qualities, the trustworthiness of the issuer is extremely important. The quality of a certificate is regulated by the German Signature Act or respective EU Directives.

Certification authorities that issue so-called qualified certificates are organised in a hierarchy with the Federal Network Agency as the higher certifying authority. The structure and content of a certificate are stipulated by the standard used. X.509 is the most important and the most commonly used standard for digital certificates. Qualified certificates are personal and extremely trustworthy.

Digital certificates are part of a so-called Public Key Infrastructure (PKI). PKI refers to a system that can issue, distribute and check digital certificates.


Certificates are issued for a specific period, usually one year, i.e. they have a limited validity period.

Your device is designed to use certificates for VPN connections and for voice connections over Voice over IP.

2.8.1 Certificate List

A list of all existing certificates is displayed in the **System Management->Certificates->Certificate List** menu.

2.8.1.1 Edit

Click the  icon to display the content of the selected object (key, certificate, or request).

The certificates and keys themselves cannot be changed, but a few external attributes can be changed, depending on the type of the selected entry.

The **System Management->Certificates->Certificate List->** menu consists of the following fields:

Fields in the Edit parameters menu

Field	Description
Description	Shows the name of the certificate, key, or request.
Certificate is CA Certificate	Mark the certificate as a certificate from a trustworthy certification authority (CA). Certificates issued by this CA are accepted during authentication.

Field	Description
	<p>The function is enabled with <i>True</i>.</p> <p>The function is disabled by default.</p>
Certificate Revocation List (CRL) Checking	<p>Only for Certificate is CA Certificate = <i>True</i></p> <p>Define the extent to which certificate revocation lists (CRLs) are to be included in the validation of certificates issued by the owner of this certificate.</p> <p>Possible settings:</p> <ul style="list-style-type: none"> • <i>Disabled</i>: No CRLs check. • <i>Always</i>: CRLs are always checked. • <i>Only if a CRL Distribution Point is present</i> (default value): A check is only carried out if a CRL Distribution Point entry is included in the certificate. This can be determined under "View Details" in the certificate content. • <i>Use settings from superior certificate</i>: The settings of the higher level certificate are used, if one exists. If it does not, the same procedure is used as that described under "Only if a CRL Distribution Point is present".
Force certificate to be trusted	<p>Define that this certificate is to be accepted as the user certificate without further checks during authentication.</p> <p>The function is enabled with <i>True</i>.</p> <p>The function is disabled by default.</p>



Caution

It is extremely important for VPN security that the integrity of all certificates manually marked as trustworthy (certification authority and user certificates) is ensured. The displayed "fingerprints" can be used to check this integrity: Compare the displayed values with the fingerprints specified by the issuer of the certificate (e.g. on the Internet). It is sufficient to check one of the two values.

2.8.1.2 Certificate Request

Registration authority certificates in SCEP

If SCEP (Simple Certificate Enrollment Protocol) is used, your device also supports separate registration authority certificates.

Registration authority certificates are used by some Certificate Authorities (CAs) to handle certain tasks (signature and encryption) during SCEP communication with separate keys, and to delegate the operation to separate registration authorities, if applicable.


When a certificate is downloaded automatically, i.e. if **CA Certificate** = `-- Download` `--` is selected, all the certificates needed for the operation are loaded automatically.

If all the necessary certificates are already available in the system, these can also be selected manually.

Select the **Certificate Request** button to request or import more certificates.

The menu **System Management->Certificates->Certificate List->Certificate Request** consists of the following fields:

Fields in the Certificate Request menu

Field	Description
Certificate Request Description	Enter a unique description for the certificate.
Mode	<p>Select the way in which you want to request the certificate.</p> <p>Possible settings:</p> <ul style="list-style-type: none"> • <i>Manual</i> (default value): Your device generates a PKCS#10 for the key. This file can then be uploaded directly in the browser or copied in the  menu using the View details field. This file must be provided to the CA and the received certificate must then be imported manually to your device. • <i>SCEP</i>: The key is requested from a CA using the Simple Certificate Enrolment Protocol.
Generate Private Key	<p>Only for Mode = <i>Manual</i></p> <p>Select an algorithm for key creation.</p> <p><i>RSA</i> (default value) and <i>DSA</i> are available.</p>

Field	Description
	<p>Also select the length of the key to be created.</p> <p>Possible values: <i>512, 768, 1024, 1536, 2048, 4096</i>.</p> <p>Please note that a key with a length of 512 bits could be rated as unsecure, whereas a key of 4096 bits not only needs a lot of time to create, but also occupies a major share of the resources during IPsec processing. A value of 768 or more is, however, recommended and the default value is 1024 bits.</p>
SCEP URL	<p>Only for Mode = <i>SCEP</i></p> <p>Enter the URL of the SCEP server, e.g. <code>http://scep.bintec-elmeg.com:8080/scep/scep.dll</code></p> <p>Your CA administrator can provide you with the necessary data.</p>
CA Certificate	<p>Only for Mode = <i>SCEP</i></p> <p>Select the CA certificate.</p> <ul style="list-style-type: none"> In <code>-- Download --</code>: In CA Name, enter the name of the CA certificate of the certification authority (CA) from which you wish to request your certificate, e.g. <i>cawindows</i>. Your CA administrator can provide you with the necessary data. <p>If no CA certificates are available, the device will first download the CA certificate of the relevant CA. It then continues with the enrolment process, provided no more important parameters are missing. In this case, it returns to the Generate Certificate Request menu.</p> <p>If the CA certificate does not contain a CRL distribution point (Certificate Revocation List, CRL), and a certificate server is not configured on the device, the validity of certificates from this CA is not checked.</p> <ul style="list-style-type: none"> <name of an existing certificate>: If all the necessary certificates are already available in the system, you select these manually.
RA Sign Certificate	<p>Only for Mode = <i>SCEP</i></p> <p>Only for CA Certificate not = <code>-- Download --</code></p>

Field	Description
	<p>Select a certificate for signing SCEP communication.</p> <p>The default value is <code>-- Use CA Certificate --</code>, i.e. the CA certificate is used.</p>
RA Encrypt Certificate	<p>Only for Mode = <i>SCEP</i></p> <p>Only if RA Sign Certificate not = <code>-- Use CA Certificate --</code></p> <p>If you use one of your own certificates to sign communication with the RA, you can select another one here to encrypt communication.</p> <p>The default value is <code>-- Use RA Sign Certificate --</code>, i.e. the same certificate is used as for signing.</p>
Password	<p>Only for Mode = <i>SCEP</i></p> <p>You may need a password from the certification authority to obtain certificates for your keys. Enter the password you received from the certification authority here.</p>

Fields in the Subject Name menu

Field	Description
Custom	<p>Select whether you want to enter the name components of the subject name individually as specified by the CA or want to enter a special subject name.</p> <p>If <i>Enabled</i> is selected, a subject name can be given in Summary with attributes not offered in the list. Example: "CN=VPNServer, DC=mydomain, DC=com, c=DE".</p> <p>If the field is not selected, enter the name components in Common Name, E-mail, Organizational Unit, Organization, Locality, State/Province and Country.</p> <p>The function is disabled by default.</p>
Summary	<p>Only for Custom = enabled.</p> <p>Enter a subject name with attributes not offered in the list.</p> <p>Example: "CN=VPNServer, DC=mydomain, DC=com, c=DE".</p>

Field	Description
Common Name	Only for Custom = disabled. Enter the name according to CA.
E-mail	Only for Custom = disabled. Enter the e-mail address according to CA.
Organizational Unit	Only for Custom = disabled. Enter the organisational unit according to CA.
Organization	Only for Custom = disabled. Enter the organisation according to CA.
Locality	Only for Custom = disabled. Enter the location according to CA.
State/Province	Only for Custom = disabled. Enter the state/province according to CA.
Country	Only for Custom = disabled. Enter the country according to CA.

The menu **Advanced Settings** consists of the following fields:

Fields in the Subject Alternative Names menu

Field	Description
#1, #2, #3	For each entry, define the type of name and enter additional subject names. Possible values: <ul style="list-style-type: none"> • <i>None</i> (default value): No additional name is entered. • <i>IP</i>: An IP address is entered. • <i>DNS</i>: A DNS name is entered. • <i>E-mail</i>: An e-mail address is entered. • <i>URI</i>: A uniform resource identifier is entered.

Field	Description
	<ul style="list-style-type: none"> • <i>DN</i>: A distinguished name (DN) name is entered. • <i>RID</i>: A registered identity (RID) is entered.

Fields in the Options menu

Field	Description
Autosave Mode	<p>Select whether your device automatically stores the various steps of the enrolment internally. This is an advantage if enrolment cannot be concluded immediately. If the status has not been saved, the incomplete registration cannot be completed. As soon as the enrolment is completed and the certificate has been downloaded from the CA server, it is automatically saved in the device configuration.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

2.8.1.3 Import

Choose the **Import** button to import certificates.

The menu **System Management->Certificates->Certificate List->Import** consists of the following fields:

Fields in the Import menu

Field	Description
External Filename	Enter the file path and name of the certificate to be imported, or use Browse... to select it from the file browser.
Local Certificate Description	Enter a unique description for the certificate.
File Encoding	<p>Select the type of coding so that your device can decode the certificate.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Auto</i> (default value): Activates automatic code recognition. If downloading the certificate in auto mode fails, try with a certain type of encoding.

Field	Description
	<ul style="list-style-type: none"> • <i>Base64</i> • <i>Binary</i>
Password	<p>You may need a password to obtain certificates for your keys.</p> <p>Enter the password here.</p>

2.8.2 CRLs

In the **System Management->Certificates->CRLs** menu, a list of all CRLs (Certification Revocation List) is displayed.

If a key is no longer to be used, e.g. because it has fallen into the wrong hands or has been lost, the corresponding certificate is declared invalid. The certification authority revokes the certificate and publishes it on a certificate blacklist, so-called CRL. Certificate users should always check against these lists to ensure that the certificate used is currently valid. This check can be automated via a browser.

The Simple Certificate Enrollment Protocol (SCEP) supports the issue and revocation of certificates in networks.

2.8.2.1 Import

Choose the **Import** button to import CRLs.

The **System Management->Certificates->CRLs->Import** menu consists of the following fields:

Fields in the CRL Import menu

Field	Description
External Filename	Enter the file path and name of the CRL to be imported, or use Browse... to select it from the file browser.
Local Certificate Description	Enter a unique description for the CRL.
File Encoding	<p>Select the type of encoding, so that your device can decode the CRL.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Auto</i> (default value): Activates automatic code recognition. If

Field	Description
	<p>downloading the CRL in auto mode fails, try with a certain type of encoding.</p> <ul style="list-style-type: none"> • <i>Base64</i> • <i>Binary</i>
Password	Enter the password required for the import.

2.8.3 Certificate Servers

A list of certificate servers is displayed in the **System Management->Certificates->Certificate Servers** menu.

A certification authority (certification service provider, Certificate Authority, CA) issues your certificates to clients applying for a certificate via a certificate server. The certificate server also issues the private key and provides certificate revocation lists (CRL) that are accessed by the device via LDAP or HTTP in order to verify certificates.

2.8.3.1 New

Choose the **New** button to set up a certificate server.

The **System Management->Certificates->Certificate Servers->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a unique description for the certificate server.
LDAP URL Path	Enter the LDAP URL or the HTTP URL of the server.

Chapter 3 Physical Interfaces

3.1 Ethernet Ports

An Ethernet interface is a physical interface for connection to the local network or external networks.

The Ethernet ports **ETH1** to **ETH4** are assigned to a single logical Ethernet interface in ex works state. The logical Ethernet interface `en1-0` is assigned and is preconfigured with the **IP Address** `192.168.0.250` and **Netmask** `255.255.255.0`.

The logical Ethernet interface `en1-4` is assigned to the **ETH5** port and is not preconfigured.



Note

To ensure your system can be reached, when splitting ports make sure that Ethernet interface `en1-0` with the preconfigured IP address and netmask is assigned to a port that can be reached via Ethernet. If in doubt, carry out the configuration using a serial connection via the **Serial 1** interface.

ETH1 - ETH4

The interfaces can be used separately. They are logically separated from each other, each separated port is assigned the desired logical Ethernet interface in the **Ethernet Interface Selection** field of the **Port Configuration** menu. For each assigned Ethernet interface, another interface is displayed in the list in the **LAN->IP Configuration** menu, and the interface can be configured completely independently.

ETH5

By default, the logical Ethernet interface `en1-4` is assigned to the **ETH5** port. The configuration options are the same as those for the ports **ETH1 - ETH4**.

VLANs for Routing Interfaces

Configure VLANs to separate individual network segments from each other, for example (e.g. individual departments of a company) or to reserve bandwidth for individual VLANs

when managed switches are used with the QoS function.

3.1.1 Port Configuration

Port Separation

Your device makes it possible to run the switch ports as one interface or to logically separate these from each other and to configure them as independent Ethernet interfaces.

During configuration, please note the following: The splitting of the switch ports into several Ethernet interfaces merely logically separates these from each other. The available total bandwidth of max. 1000 mbps full duplex for all resulting interfaces remains the same. For example, if you split all the switch ports from each other, each of the resulting interfaces only uses a part of the total bandwidth. If you group together several switch ports into one interface, the full bandwidth of max. 1000 mbps full duplex is available for all the ports together.

The menu **Physical Interfaces->Ethernet Ports->Port Configuration** consists of the following fields:

Fields in the Switch Configuration menu

Field	Description
Switch Port	Shows the respective switch port. The numbering corresponds to the numbering of the Ethernet ports on the back of the device.
Ethernet Interface Selection	Assign a logical Ethernet interface to the switch port. You can select from five interfaces, <i>en1-0</i> to <i>en1-2</i> . In the basic setting, switch port 1-4 has the <i>en1-0</i> interface assigned to it.
Configured Speed / Mode	Select the mode in which the interface is to run. Possible values: <ul style="list-style-type: none"> • <i>Full Autonegotiation</i> (default value) • <i>Auto 1000 mbps only</i> • <i>Auto 100 mbps only</i> • <i>Auto 10 mbps only</i> • <i>Auto 100 mbps / Full Duplex</i>

Field	Description
	<ul style="list-style-type: none"> • <i>Auto 100 mbps / Half Duplex</i> • <i>Auto 10 mbps / Full Duplex</i> • <i>Auto 10 mbps / Half Duplex</i> • <i>Fixed 1000 mbps / Full Duplex</i> • <i>Fixed 100 mbps / Full Duplex</i> • <i>Fixed 100 mbps / Half Duplex</i> • <i>Fixed 10 mbps / Full Duplex</i> • <i>Fixed 10 mbps / Half Duplex</i> • None: The interface is created but remains inactive.
Current Speed / Mode	<p>Shows the actual mode and actual speed of the admin interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>1000 mbps / Full Duplex</i> • <i>100 mbps / Full Duplex</i> • <i>100 mbps / Half Duplex</i> • <i>10 mbps / Full Duplex</i> • <i>10 mbps / Half Duplex</i> • <i>Down</i>
Flow Control	<p>Select whether a flow control should be conducted on the corresponding interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Disabled</i> (default value): No flow control is performed. • <i>Enabled</i>. Flow will be controlled. • <i>Auto</i>: Flow will be controlled automatically.

3.2 ISDN Ports

The system's ISDN connections can be configured as either internal or external ISDN connections. The external ISDN connections are used for connection to the network operator's ISDN network. The internal ISDN connections are provided for connecting various ISDN terminals (system telephones, ISDN telephones, ...).

3.2.1 ISDN External


You configure your system's external ISDN connections in the **Physical Interfaces->ISDN Ports->ISDN External** menu.

The access configuration for an external ISDN can be set up for point-to-multipoint (P-MP) and point-to-point (P-P).

The following variants are possible when connecting to more than one ISDN connection:

- All external ISDN connections are only point-to-multipoint connections (P-MP).
- All external ISDN connections are only point-to-point connections (P-P).
- The external ISDN connections are point-to-multipoint connections (P-MP) and point-to-point connections (P-P).

3.2.1.1 Working with

Choose the  button to edit an entry.

The menu **Physical Interfaces->ISDN Ports->ISDN External->** consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a user-defined description of the ISDN interface. The default value is <i>ISDN External</i> .
Name	Shows the name of the ISDN interface. Possible values: <ul style="list-style-type: none"> • <i>S/U</i>: 4 wire (S) • <i>/</i>: Displays the port on the module to which the ISDN connection is connected. Example: <i>S/U 1</i> = The interface is in Port 1 and is used as an S connector.
Access Type	Select whether the ISDN interface will be operated as a point-to-multipoint connection or as a point-to-point connection. Possible values:

Field	Description
	<ul style="list-style-type: none"> • <i>ISDN P-P</i> (default value) • <i>ISDN P-MP</i>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Permanent Layer 2 Activation	<p>This function (also known as permanent monitoring) constantly monitors the functionality and transmission quality of an external ISDN connection. For this purpose, the system is in permanent contact with your network operator's exchange. If the exchange does not keep the ISDN layer 2 permanently enabled, the system can initiate the repeated establishment of layer 2.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
ISDN Synchronisation	<p>When an external device (e. g. GSM gateway) is connected to an external point-to-point ISDN access in the system, the external device's signal can disturb the synchronisation in the ISDN signal. Only if such a disturbance occurs should you switch off the layer 1 synchronisation.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

3.2.2 ISDN Internal

You configure your system's internal ISDN interfaces in the **Physical Interfaces->ISDN Ports->ISDN Internal** menu.

Internal ISDN connections are always point-to-multipoint connections.


When connecting terminals to an internal ISDN connection, please note that not every ISDN terminal sold by retailers is able to use the features provided by the system via your key interface.

The **Physical Interfaces->ISDN Ports->ISDN Internal** menu consists of the following fields:

Fields in the ISDN Internal menu

Field	Description
Name	Shows the name of the ISDN interface. Possible values: <ul style="list-style-type: none"> • <i>S/U</i>: 4 wire (S) • <i>/</i>: Displays the port on the module to which the ISDN connection is connected. Example: <i>S/U 2</i> = The interface is in Port 2 and is used as an S connector.
Usage	Shows the function of the ISDN interface. Possible values: <ul style="list-style-type: none"> • <i>Upn</i>: Interface for CAPI terminals. • <i>Upn</i>: Interface for UPN terminals. • <i>S0</i>: Interface for ISDN S0 connection.
Default MSN	Shows whether a standard MSN is assigned for an internal S0 bus. You can use a standard MSN to access unconfigured S0 terminals. As a standard MSN, you can dial the internal numbers configured in the Numbering->User Settings->Users menu and assigned to a terminal in the Terminals menu.
Status	Displays the status of the interface.

3.2.2.1 Edit

Choose the  button to edit an entry.

The menu **Physical Interfaces->ISDN Ports->ISDN Internal->** consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Default MSN	<p>Dial the number you want. You can dial any number that you have configured in the Numbering->User Settings->Users->Numbers menu.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Not configured</i> • <i><Subscriber Number></i>



3.3 Analogue Ports

3.3.1 Analogue External (FXO)


The **Analogue External (FXO)** menu displays all of your system's available analogue external connections.

The **Physical Interfaces->Analogue Ports->Analogue External (FXO)** menu consists of the following fields:

Values in the Analogue External (FXO) list

Field	Description
Name	<p>Shows the name of the analogue interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>FXO</i>: Name for the analogue connection.
Description	Shows the user-defined description of the analogue interface.
Dialling Method	<p>Displays the dialling method used.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Tone Dialling (DTMF)</i> (default value) • <i>Pulse Dialling (PD)</i>
Status	Displays the status of the interface.
Action	Change the status of the interface by pressing the  button or  button in the Action column.

3.3.1.1 Edit

Choose the  button to edit an entry.

The menu **Physical Interfaces->Analogue Ports->Analogue External (FXO)->** consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a user-defined description of the analogue interface.
Name	Shows the name of the analogue interface. Possible values: <ul style="list-style-type: none"> • <i>FXO</i>: Name for the analogue connection.
Dialling Method	Select which dialling method should be used. Possible values: <ul style="list-style-type: none"> • <i>Tone Dialling (DTMF)</i> (default value) • <i>Pulse Dialling (PD)</i>
CLIP	Select whether the CLIP feature is to be used, i. e. whether the caller's number should be displayed to the person called. Possible values: <ul style="list-style-type: none"> • <i>OFF</i> (default value): The caller's number is not displayed to the person called. • <i>FSK</i>: The data is sent as DTMF.
Receive charges	Select whether your device is to receive charge information from the network. For this purpose, you can define the charge impulse at 12 kHz or 16 kHz. Possible values: <ul style="list-style-type: none"> • <i>OFF</i> (default value) Charge information is not received. • <i>12 kHz</i> • <i>16 kHz</i>

Fields in the Advanced Settings menu

Field	Description
Busy Tone Detection	<p>Select whether Busy Tone Detection should be used.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Dial Tone Detection	<p>Select whether Dial Tone Detection should be used.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p> <p>If the Dial Tone Detection is enabled and the external dial tone has been recognised, your hybird 120 immediately starts to dial.</p>
Dial Tone Pause	<p>Only for Dial Tone Detection disabled.</p> <p>Enter the value you want which the system is to wait for, as a maximum, when dialling a telephone number, before it begins dialling.</p> <p>You can switch on the Dial Tone Pause if the hybird 120 fails to recognise the external dial tone or if no dial tone is being sent. You must decide the duration of the Dial Tone Pause.</p> <p>Possible values are whole number values between 1 second and 5 seconds.</p>
End-of-Selection Signal	<p>Enter the time that the system is to wait, after dialling a number, before it considers the telephone number to be complete and makes the connection. The default value is 5 seconds.</p>

3.3.2 Analogue Internal (FXS)

The **Analogue Internal (FXS)** menu displays all of your system's available analogue internal connections.

The menu **Physical Interfaces->Analogue Ports->Analogue Internal (FXS)** consists of the following fields:

Values in the Analogue Internal (FXS) list

Field	Description
Name	<p>Shows the name of the analogue interface.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>FXS</i>: Name for the analogue connection.
Usage	<p>Shows the function of the analogue interface.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Telephone</i>• <i>Doorcom Units</i>• <i>Multi Function Device/Telefax</i>• <i>Modem</i>• <i>Answering Machine</i>• <i>Emergency Phone</i> <p>The function of the analogue terminal is configured in the Terminals->Other phones->analog menu.</p>
Status	<p>Displays the status of the interface.</p>

Chapter 4 VoIP

Voice over IP (VoIP) uses the IP protocol for voice and video transmission.

The main difference compared with conventional telephony is that the voice information is not transmitted over a switched connection in a telephone network, but divided into data packets by the Internet protocol and these packets are then passed to the destination over undefined paths in a network. This technology uses the existing network infrastructure for voice transmission and shares this with other communication services.

4.1 Settings



You set up your VoIP connections in the **VoIP->Settings** menu.


You can telephone over the internet using all internally connected telephones. The number of connections depends on various parameters:

- The availability of the system's free channels.
- The available bandwidth of the DSL connection.
- The configured, available SIP providers.
- The SIP-out licenses that have been entered.


4.1.1 SIP Provider

You configure the SIP provider you want in the **VoIP->Settings->SIP Provider** menu.

You change the status of the SIP provider by pressing the  button or the  button in the **Action** column.

After about one minute, registration with the provider has taken place and the status is automatically set to  (active).

4.1.1.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

The menu **VoIP->Settings->SIP Provider->New** consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	You can enter a name for the SIP provider. A 20 digit alpha-numeric sequence is possible.
Provider Status	Select whether this VoIP provider entry is enabled (<i>Enabled</i> , default value) or not (<i>disabled</i>).
Access Configuration	Select which type of VoIP phonenumbers you wish to configure. Possible values: <ul style="list-style-type: none"> • <i>Single Number(s)</i> (default value): Enter the individual DSL phonenumbers. • <i>Direct Dial-In</i>: Enter a basic number in conjunction with an extension number block.
Authentication ID	Enter your provider's authentication ID. A 64 digit alpha-numeric sequence is possible.
Password	At this point, you can assign a password. A 32 digit alpha-numeric sequence is possible.
User Name	Enter the user name you received from your VoIP provider. A 64 digit alpha-numeric sequence is possible.
Domain	Enter a new domain name or a new IP address for the SIP proxy server. If you do not make an entry, the entry in the Registrar field is used. Note: Enter a name or IP address only if this is explicitly specified by the provider.

Fields in the Outgoing Signalisation Settings menu

Field	Description
Outgoing Signalisation	Select the signal you want for outgoing calls. Possible values: <ul style="list-style-type: none"> • <i>Standard</i> (default value) • <i>Global CLIP no Screening Number</i>

Field	Description
	<ul style="list-style-type: none"> • <i>Individual CLIP no Screening Number</i> • <i>Fixed Out DDI (Only for Access Type = Direct Dial-In)</i>
Global CLIP no Screening Number	<p>Only for Outgoing Signalisation <i>Global CLIP no Screening Number</i></p> <p>Enter the number that is to be displayed to the person called with any outward connection.</p> <p>This number is not checked.</p>
Signal remote caller number	<p>Only for Outgoing Signalisation = <i>Global CLIP no Screening Number</i> and <i>Individual CLIP no Screening Number</i></p> <p>You can display the number of an external subscriber if it is signalled.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Signal fixed out number	<p>Only for Outgoing Signalisation = <i>Fixed Out DDI</i></p> <p>Enter the number that is to be displayed to the person called with any outward connection.</p>

Fields in the Registrar menu

Field	Description
Registrar	Enter the DNS name or IP address of the SIP server. A 26 digit alpha-numeric sequence is possible.
Registrar Port	Enter the number of the port to be used for the connection to the server. The default value is <i>5060</i> . A 5 digit sequence is possible.
Transport Protocol	<p>Select the transport protocol for the connection.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>UDP</i> (default value) • <i>TCP</i>

Fields in the STUN menu

Field	Description
STUN server	<p>Enter the name or the IP address of the STUN server.</p> <p>STUN = Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)</p> <p>A STUN server is required to allow VoIP devices access to the internet behind an active NAT. This determines the current public IP address for the connection, which is used for precise remote addressing.</p> <p>Maximum number of characters: 32.</p>
Port STUN server	<p>Enter the number of the port to be used for the connection to the STUN server.</p> <p>The default value is <i>3478</i>. A 5 digit sequence is possible.</p>

Fields in the Timer menu

Field	Description
Registration Timer	<p>Enter the time in seconds within which the SIP client must re-register to prevent the connection from disconnecting automatically.</p> <p>The default value is <i>60</i>.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Proxy	Enter the DNS name or IP address of the SIP server. A 26 digit alpha-numeric sequence is possible.
Proxy Port	Enter the number of the port to be used for the connection to the proxy. The default value is <i>5060</i> . A 5 digit sequence is possible.
Transport Protocol	<p>Select the transport protocol for the connection.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none"> • <i>UDP</i> (default value) • <i>TCP</i>

Fields in the Further Settings menu

Field	Description
From Domain	Enter the SIP provider's "From Domain". It is used after the @ as sender data in the SIP header of the SIP data packages.
Number of allowed simultaneous Calls	<p>Select the maximum number of calls that shall be simultaneously possible Please also note the settings for bandwidth management here.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>International</i> (default value): An unlimited number of simultaneous calls is possible. • 1 • 2 • 3 • 4 • 5 • 10
Location	<p>Select the location of the SIP server. Locations are defined in the VoIP->Settings->Locations menu.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Any Location</i> (default value): The server is not operated at any defined location. • <Location Name>
Codec Profiles	<p>Select the codec profile for this SIP server. Codec profiles are defined in the VoIP->Settings->Codec Profiles menu.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>System Default</i> (default value): The server is operated with a codec profile predefined in the system. • <Codec profile name>

Field	Description
Dial End Monitoring Time	Select the time (after dialling the last digit of a call number) after which the system begins external dialling.
Call Hold inside the PBX system	Select whether a telephone call in the system can be switched to hold without losing the connection (inquiry calls/brokering). If this function is not enabled, the call is held at the SIP provider, if he supports this performance feature. The function is activated by selecting <i>Enabled</i> . The function is enabled by default.
Call Forwarding extern (SIP 302)	Select whether calls are to be redirected externally with the SIP provider. The call is forwarded using SIP status code 302. The function is activated by selecting <i>Enabled</i> . The function is disabled by default.
Generate international phone number	If you have enabled this function and entered <i>43</i> (for Austria) under Global Settings Country Profile , the 0043 before a number dialled with area code is generated automatically. The function is activated by selecting <i>Enabled</i> . The function is disabled by default.
Generate national subscriber number	If you have enabled this function and entered the National Prefix / City Code (e.g. for Abfaltersbach <i>4846</i>) under Global Settings , the 4846 before a number dialled with area code is generated automatically. The function is activated by selecting <i>Enabled</i> . The function is disabled by default.
Deactivate number suppression	If you enable this function, the number is always sent, independently of whether you have switched Suppress outgoing CLIP (CLIR) on or off for an extension. The function is activated by selecting <i>Enabled</i> . The function is disabled by default.
SIP Header Field for	Select the position of the user name (user ID) in the SIP head-

Field	Description
User Name	<p>er for outgoing calls.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>P-Preferred</i>: The so-called "p-preferred-identity" field is added to the SIP header and contains the User Name. • <i>P-Asserted</i>: The so-called "p-asserted-identity" field is added to the SIP header and contains the User Name. • <i>None</i>: The User Name is not transmitted.
SIP Header Field(s) for Caller Address	<p>Select the position of the sender ID (e.g. subscriber number) in the SIP header for outgoing calls. (For incoming calls, the subscriber number is taken automatically from the SIP header.)</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Display</i>: The sender ID is placed in the "Display" field of the SIP header. • <i>User Name</i>: The sender ID is transferred to the "User" field of the SIP header. • <i>P-Preferred</i>: The so-called "p-preferred-identity" field is added to the SIP header to transmit the sender ID there. • <i>P-Asserted</i>: The so-called "p-asserted-identity" field is added to the SIP header to transmit the sender ID there.
Substitution of International Prefix with "+"	<p>Select whether the prefix (e.g. 00) should be replaced by + for international numbers.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
PBX coupling	<p>Select whether another PABX can log into your system. In this way, several PABX systems can be linked.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Delete SIP bindings after Restart	<p>If after registering with a provider a reset of the system should occur, for example, or a power failure, depending on the provider, another registration may prove impossible. Enabling these performance features allows re-registration after restart.</p>

Field	Description
	<p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Upstreaming Device with NAT	<p>If you enable this function, you can use a gateway with NAT and still make VoIP calls. Without this function, it may not be possible to call you with VoIP if you use a gateway with NAT.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Early media support	<p>Select whether you'll allow exchange of voice and audio data before a receiver accepts a call.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Provider without Registration	<p>Select whether registration and authentication with a provider can be eliminated. In this case, the relevant data can be sent to a specific IP address already known to the correspondent. An example of this method is Microsoft Exchange SIP.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>If this function is not enabled, an authentication is performed by default. For this, every SIP client (user) sends its current position to a registrar server. This information on the user and his current address is saved by the registrar on a server queried by other proxies to locate the user.</p>
T.38 FAX support	<p>Select whether faxes shall be transmitted with T.38.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p> <p>If the function is disabled, faxes are transmitted with G.711.</p>
Substitution of Incoming Number Prefix	<p>For incoming calls, if the call number should be forwarded in the system in modified form: in the first input field enter the sequence of the incoming number to be replaced by the number</p>

Field	Description
	sequence entered in the second input field.

4.1.2 Locations



In the **VoIP->Settings->Locations** menu you configure the locations of the VoIP subscribers who have been configured on your system, and define the bandwidth management for the VoIP traffic.

Individual locations can be set up for using the bandwidth management. A location is identified from its fixed IP address or DynDNS address or from the interface to which the device is connected. The available VoIP bandwidth (up- and downstream) can then be set up for each location.

Fields in the Registration behavior for VoIP subscribers without assigned location menu

Field	Description
Default Behavior	<p>Specify how the system is to proceed when registering VoIP subscribers for whom no location has been defined.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Registration for Private Networks Only</i> (default value): The VoIP subscriber is only registered if located within the private network. • <i>Forbidden</i>: The VoIP subscriber is never registered. • <i>Unrestricted Registration</i>: The VoIP subscriber is always registered.

4.1.2.1 Edit or New

Choose the  icon to edit existing entries. Select the **New**  button to create new entries.

The menu **VoIP->Settings->Locations->New** consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter the description of the entry.
Parent Location	You can cascade the SIP locations as you wish. Define here which SIP location that has been defined constitutes the high-

Field	Description
	level node for the SIP location to be configured here.
Type	<p>Select whether the location is to be defined through IP addresses/DNS names or interfaces.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Addresses</i> (default value): The SIP location is defined via IP addresses or DNS names. • <i>Interfaces</i>: The SIP location is defined via the available interfaces.
Addresses	<p>Only for Type = <i>Addresses</i></p> <p>Enter the IP addresses of the devices at the SIP locations.</p> <p>Click Add to configure new addresses.</p> <p>Enter the IP address or DNS name that you want under IP Address/DNS Name.</p> <p>Also enter the required Netmask.</p>
Interfaces	<p>Only for Type = <i>Interfaces</i></p> <p>Indicate the interfaces to which the devices of a SIP location are connected.</p> <p>Click Add to select a new interface.</p> <p>Under Interface, select the interface you want.</p>
Upstream Bandwidth Limitation	<p>Determine whether the upstream bandwidth is to be restricted.</p> <p>The bandwidth is reduced with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Maximum Upstream Bandwidth	<p>Enter the maximum data rate in the send direction in kBits per second.</p>
Downstream Bandwidth Limitation	<p>Determine whether the downstream bandwidth is to be restricted.</p> <p>The bandwidth is reduced with <i>Enabled</i>.</p>

Field	Description
	The function is disabled by default.
Maximum Downstream Bandwidth	Enter the maximum data rate in the receive direction in kBits per second.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu


Field	Description
DSCP Settings for rtp Traffic	<p>Select the Type of Service (TOS) for RTP data.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>DSCP Binary Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). • <i>DSCP Decimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • <i>DSCP Hexadecimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111. • <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63. • <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.

4.1.3 Codec Profiles

In the **VoIP->Settings->Codec Profiles** , you can define the various codec profiles to control voice quality and set up specific provider-dependent default settings.

When setting up the codec, remember that a good voice quality requires a corresponding bandwidth so that the number of simultaneous calls will be restricted. The remote terminal also has to support the relevant codec choice.

4.1.3.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

The menu **VoIP->Settings->Codec Profiles->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter a description for the entry.
Codec Proposal Sequence	<p>Choose the order in which the codecs are offered for use by the system. If the first codec cannot be used, the second is tried and so on.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Default</i> (default value): the codec in the first position in the menu will be used if possible. • <i>Quality</i>: The codecs are sorted by quality. The codec with the best quality is used if possible. • <i>Low Bandwidth</i>: The codecs are sorted by required bandwidth. If possible, the codec with the lowest bandwidth requirement is used. • <i>High Bandwidth</i>: The codecs are sorted by required bandwidth. If possible, the codec with the highest bandwidth requirement is used.
G.711 uLaw	<p>Only for Codec Proposal Sequence not <i>default</i></p> <p>ISDN codec with US characteristic</p> <p>G.711 uLaw passes audio signals in the range of 300-3500 Hz and samples them at the rate of 8,000 samples per second. At 64 kbit/s bit rate the mean opinion score (MOS) is 4,4. This audio codec uses μlaw quantization.</p>
G.711 aLaw	<p>Only for Codec Proposal Sequence not <i>default</i></p> <p>ISDN codec with EU characteristic</p> <p>G.711 aLaw passes audio signals in the range of 300-3400 Hz and samples them at the rate of 8,000 samples per second. At 64 kbit/s bit rate the mean opinion score (MOS) is 4,4. This au-</p>

Field	Description
	dio codec uses alaw quantization.
G.722	<p>Only for Codec Proposal Sequence not <i>default</i></p> <p>G.722 passes audio signals in the range of 50-7000 Hz and samples them at the rate of 16,000 samples per second. At 64 kbit/s bit rate the mean opinion score (MOS) is 4,5.</p>
G.729	<p>Only for Codec Proposal Sequence not <i>default</i></p> <p>G.729 passes audio signals in the range of 300-2400 Hz and samples them at the rate of 8,000 samples per second. At 8 kbit/s bit rate the mean opinion score (MOS) is 3,9.</p>
G.726 (16 kbit/s)	<p>Only for Codec Proposal Sequence not <i>default</i></p> <p>G.726 (16 kbit/s) passes audio signals in the range of 200-3400 Hz and samples them at the rate of 8,000 samples per second. At 16 kbit/s bit rate the mean opinion score (MOS) is 3,7.</p>
G.726 (24 kbit/s)	<p>Only for Codec Proposal Sequence not <i>default</i></p> <p>G.726 (24 kbit/s) passes audio signals in the range of 200-3400 Hz and samples them at the rate of 8,000 samples per second. At 24 kbit/s bit rate the mean opinion score (MOS) is 3,8.</p>
G.726 (32 kbit/s)	<p>Only for Codec Proposal Sequence not <i>default</i></p> <p>G.726 (32 kbit/s) passes audio signals in the range of 200-3400 Hz and samples them at the rate of 8,000 samples per second. At 32 kbit/s bit rate the mean opinion score (MOS) is 3,9.</p>
G.726 (40 kbit/s)	<p>Only for Codec Proposal Sequence not <i>default</i></p> <p>G.726 (40 kbit/s) passes audio signals in the range of 200-3400 Hz and samples them at the rate of 8,000 samples per second. At 40 kbit/s bit rate the mean opinion score (MOS) is 4,2.</p>
DTMF	Only for Codec Proposal Sequence not <i>default</i>

Field	Description
	<p>Select whether the DTMF Outband codec is to be used. First the system attempts to use RFC 2833. If the remote terminal does not use this standard, SIP Info is used.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
G.726 Codec settings	<p>Only for Codec Proposal Sequence not <i>default</i></p> <p>Select the coding method for the G.726 codec.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>I.366</i> • <i>RFC3551 / X.420</i>

4.1.4 Options

In the **VoIP->Settings->Options** menu, you'll find general VoIP settings.

The **VoIP->Settings->Options** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
RTP Port	<p>Enter the port via which the RTP data is to be transported.</p> <p>The default value is <i>10000</i>.</p>
Client Registration Timer	<p>Here, enter a default value for the time in seconds within which the SIP clients must re-register to prevent the connection from disconnecting automatically.</p> <p>The default value is <i>60</i>.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
DSCP Settings for sip Traffic	Select the Type of Service (TOS) for SIP data.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none">• <i>DSCP Binary Value</i> (default value): Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). The default value is <i>101110</i>.• <i>DSCP Decimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format).• <i>DSCP Hexadecimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format).• <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. <i>00111111</i>.• <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. <i>63</i>.• <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. <i>3F</i>.

Chapter 5 Numbering

5.1 Trunk Settings

Your system is a telecommunication installation for external connection to the Euro ISDN (DSS1) and the Internet:

ISDN connections (S0): Depending on module extension, the system features external ISDN connections configured for connection to the network operator's ISDN connection. Depending on module extension, several ISDN connections can either be set as an internal or external ISDN connection.




Note

If you assign a name to the connections in these settings, it will not be used in the subsequent configuration. It merely serves as description for the connection.

5.1.1 Trunks

You configure your system's external connections in the **Numbering->Trunk Settings->Trunks** menu.

5.1.1.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create new connections.

The **Numbering->Trunk Settings->Trunks->New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	You can enter a name for the connection you selected.
Access Type	Shows the configured connection type. Possible values: <ul style="list-style-type: none"> • <i>Point-to-multipoint connection</i> (default value)

Field	Description
	<ul style="list-style-type: none"> • <i>ISDN P-P</i> • <i>FXO</i>
Port	<p>Only for Access Type = <i>ISDN P-MP</i></p> <p>Select the description for the port via which this external connection is connected.</p>
Ports	<p>Only for Access Type = <i>ISDN P-P</i> or <i>FXO</i></p> <p>Select the description for the port via which this external connection is connected.</p> <p>All free external ISDN interfaces are available.</p> <p>Use the Add button to select other ports, in order, e. g., to configure a party line.</p>

Fields in the Outgoing Signalisation Settings menu

Field	Description
Outgoing Signalisation	<p>Select the signal you want for outgoing calls.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Standard</i> (default value) • <i>Global CLIP no Screening Number</i> • <i>Individual CLIP no Screening Number</i> • <i>Fixed Out DDI</i>
Global CLIP no Screening Number	<p>Only for Outgoing Signalisation = <i>Global CLIP no Screening Number</i></p> <p>Here, you can enter a number to be displayed with the called party for all outbound external calls.</p> <p>This number is not checked.</p>
Signal remote caller number	<p>Only for Outgoing Signalisation = <i>Global CLIP no Screening Number</i> and <i>Individual CLIP no Screening Number</i></p> <p>You can display the number of an external subscriber if it is signalled.</p>

Field	Description
	<p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Signal fixed out number	<p>Only for Outgoing Signalisation = <i>Fixed Out DDI</i></p> <p>You can display a fixed number for all outbound "external" calls, e.g. your head office number.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Type of Number	<p>Select the number type for outgoing calls.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>System Setting</i>: The standard system setting (country setting) is used. • <i>Unknown</i>: Select this setting if the number type "unknown" is to be signalled. • <i>Subscriber</i>: This is an extension number. • <i>National</i>: This is a national number (area code + extension number).
Call Hold inside the PBX system	<p>Select whether a telephone call is to be put on hold in the system without losing the connection.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

5.1.2 Trunk Numbers

In the menu **Numbering->Trunk Settings->Trunk Numbers** you assign the external numbers and the name indicated in a system telephone display to the external connections you've defined.

An external connection can be configured as a point-to-multipoint or point-to-point connection; in the process, the connection description is defined. The intended port name is then assigned to this connection. The port name (**Description**) can be defined under **Physical Interfaces->ISDN Ports->ISDN External** for the module connection.

External numbers at the point-to-point connection

For a point-to-point connection, you receive a PBX number together with a 1-, 2-, 3- or 4-character extension number range. This extension number range comprises the direct dial-in numbers for the PBX connection. If you've requested several point-to-point connections, the number of extensions can be expanded, or you receive another PBX number with your own extension number range.


With a point-to-point connection, external calls are signalled to the subscriber whose assigned internal number corresponds to the dialled extension number. You configure the internal numbers to be reached directly via direct dial-in of the extension numbers as **Internal Number** in the menu **Numbering->User Settings->User->Add->Trunk Numbers->Internal Numbers**.

Example: You have a point-to-point connection with the PBX number *1234* and extension numbers from *0* to *30*. A call under *1234-22* is normally signalled at the internal subscriber with call number *22*. However, if you enter extension number *22* in this list, you can define that calls under *1234-22* are signalled at the internal subscriber by call number *321*.

External subscriber numbers at point-to-multipoint connection

For a point-to-multipoint connection, you can request up to 10 numbers (MSN, multiple subscriber number) per ISDN connection. These MSNs are the external subscriber numbers for your ISDN connections. Definition of the internal number occurs under **Numbering->User Settings->User->Add->Trunk Numbers**.

5.1.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create new numbers.

The **Numbering->Trunk Settings->Trunk Numbers->New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Trunk	Select the connection defined in Numbering->Trunk Settings->Trunks for which to perform the number configuration.
Type of Number	Select the call number type to be defined according to connection type.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Single Number (MSN)</i>: Only for point-to-multipoint connections. • <i>P-P Base Number</i>: Only for point-to-point connections. • <i>P-P DDI Exception</i>: Only for point-to-point connections. • <i>P-P Additional MSN</i>: Only for point-to-point connections.
Displayed Name	<p>In general, you enter the name to be displayed for this number in the called system telephone's display.</p> <p>Für Type of Number = <i>P-P Base Number</i> this field displays the name of the connection.</p>
Single Number (MSN)	<p>Here, enter the MSN for a point-to-multipoint connection.</p>
P-P Base Number	<p>Here, enter the number for the point-to-point connection (without direct dial number).</p>
P-P DDI Exception	<p>Here, enter the direct dial exception for a point-to-point connection.</p> <p>Note: Only enter the extension according to your extension number range that should be routed to differing internal subscriber numbers. Direct dial at the point-to-point connection always proceeds to the subscriber whose number was dialled along as extension. E. g. the internal subscriber has the number <i>16</i>. If this subscriber is called from outside on <i>1234567-16</i>, the call is signalled at his telephone. However, if with direct dial <i>16</i> a subscriber with the number <i>888</i> is to be called, enter <i>888</i> as the exception number. In Incoming Distribution you then assign the exception number to the subscriber with the number <i>16</i>. You can subsequently perform additional settings in Incoming Distribution.</p>
P-P Additional MSN	<p>Here, enter an additional MSN for a point-to-point connection.</p> <p>With some providers, it's possible to also transmit a point-to-multipoint number on a point-to-point connection in parallel to the direct dial number; e.g. a fax number pre-existing setup of a point-to-point connection, or the old point-to-multipoint number.</p>

5.1.3 Trunk Groups


In the **Numbering->Trunk Settings->Trunk Groups** menu, you can group the various external connections and individually provide these to the users.

You wish to assign specific external connections to internal subscribers for outgoing connections. You can join these external connections together to create bundles and supply these to extensions for outgoing calls. In this way, all extensions start external dialling with the same dialling code, but can only establish a connection using the bundle released for the extension in question.

The external connections of your system can be grouped into bundles. You can configure up to 99 bundles (01 - 99). The code number for bundle assignment can be modified (menu **Alternative Access Codes**).

When initiating an external call through the bundle code number, the bundle cleared for the subscriber is used in connection setup.

5.1.3.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create a new bundle.

The **Numbering->Trunk Settings->Trunk Group->New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the entry.
Sequence of Trunk Lines in Group	<p>Select the desired external connections for a bundle. The order when dialling to the outside matches the sequence of external connections in this list.</p> <p>You wish to assign specific external connections for outgoing connections to the internal subscribers of your system. You can group external connections into bundles and provide these to subscribers for the outgoing dialling. In this way, all subscribers initiate the external dialling with same bundle access code, but can only set up a connection over the bundles for which they have been cleared.</p>

5.1.4 X.31

Packet-switched data transmission (X.31)

To improve customer service, you wish to allow cashless payment methods such as debit or credit card, or record purchase data for a customer card. For this purpose, you connect a data device to your system, which transmits data for customers and credit cards to a central location.

You can connect a data device which operates according to the X.31 transmission standard (data transmission over the D channel) to the system's internal ISDN connections. These are, for example, checkout terminals, cashpoints or customer card terminals.


For use of these performance features, your network operator provides you TEI's (Terminal Endpoint Identifier), which you assign to individual connections when configuring your system. An additional addressing of these terminals occurs via these TEI's.



Note

You can only use this performance feature if performance feature **X.31** has been requested from the network operator, and you operate a corresponding terminal on this connection. For information on operation, please see the user's guide for your terminals.

5.1.4.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to set up new X.31 applications.

The **Numbering->Trunk Settings->X.31->New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Select Interface	Select the external interface over which you access the network operator providing you performance feature X.31.
Terminal Endpoint Identifier (TEI)	Here, select the TEI value (TEI, Terminal Endpoint Identifier) which you have received from your network operator. An additional addressing of these terminals occurs via the TEI's. Possible values are 00 to 63. The default value is 00.

Field	Description
Internal Assignment	Select the internal ISDN interface to which your data device, which operates according to the X.31 transmission standard (data transmission over the D channel), is connected.

5.2 User Settings


In this menu, you configure and administer your system's users. The users are organised into authorisation classes to which the desired external lines are assigned, and which may use performance features according to request. The user assigned to an authorisation class receives an internal number and specific authorisations. A default authorisation class (Default CoS) is preset ex-works, to which new users are automatically assigned.

After it's been defined in User Settings which functions and authorisations a user, or several users, have access to, authorisation of user settings is assigned to a terminal in menu **Terminals**. In this way, it's possible to create settings for several terminals via an authorisation class, e. g. a user setting *Boss*, a user setting *Department Head* and a user setting *Clerk*. Now, all that's left to do is assign the corresponding terminals to one of these **Class of Service**.

5.2.1 Users

In the **Numbering->User Settings->Users** you configure the users of your system, their class, and assign them internal and external numbers.

You see an overview of the users that have been created. The entries in the **Name** column are sorted alphabetically. Click the column title of any other column to sort entries in ascending or descending order

Choose the  icon to edit existing entries. Select the **New** button in order to create new users.

5.2.1.1 Basic Settings

Enter basic user information in the **Numbering->User Settings->Users->Basic Settings** menu.

The **Numbering->User Settings->Users->Basic Settings** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Name	<p>Enter the name of the user.</p> <p>This name is displayed in the phone book if you have entered a number and cleared it for the phone book under Mobile Number Home Number. The name is displayed with the codes (M) for mobile communication, and (H) for home number in the system telephone display.</p>
Description	Enter additional user information.

Fields in the External Numbers menu

Field	Description
Mobile Number	Enter a number under which the user can be reached via mobile phone. Also select whether this number is to be shown in the system telephone display so that it can be dialled on the system telephone from the system phone book (Access from system phone option).
Home Number	Enter a number under which the user can be reached privately. Also select whether this number is to be shown in the system telephone display so that it can be dialled on the system telephone from the system phone book (Access from system phone option).
E-mail Address	Enter the e-mail address for the user.

Fields in the Class of Service menu

Field	Description
Standard	<p>Select the authorisation class = CoS (Class of Service). Definition of the authorisation class and creation of new authorisation classes occurs under Numbering->User Settings->Class of Services. Only selection occurs in this setting.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Default CoS</i> (default value) • <i>Not allowed</i>: No class of service • <i><Authorisation class></i>
Optional	Select an optional authorisation class. This CoS is required for

Field	Description
	<p>the calendar settings. Definition of the authorisation class and creation of new authorisation classes occurs under Numbering->User Settings->Class of Services. Only selection occurs in this setting.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Default CoS</i> (default value) • <i>Not allowed</i>: No class of service • <i><Authorisation class></i>
Night	<p>Select the authorisation class for night operation. This CoS is required for the calendar settings. Definition of the authorisation class and creation of new authorisation classes occurs under Numbering->User Settings->Class of Services. Only selection occurs in this setting.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Default CoS</i> (default value) • <i>Not allowed</i>: No class of service • <i><Authorisation class></i>

Fields in the Further Options menu

Field	Description
Busy on busy	<p>Select whether the performance feature "Busy on Busy" shall be enabled for this user.</p> <p>If a subscriber for whom multiple telephone numbers have been configured makes a call, you can decide whether additional calls for this user shall be signalled. If "Busy on Busy" is set for this user, other callers get an Engaged signal if the user is calling on one of her numbers.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

5.2.1.2 Numbers

In the menu **Numbering->User Settings->Users->Numbers** internal numbers which are later assigned to the terminals can be entered. Depending on the type, one or more numbers can be assigned per terminal.

The **Numbering->User Settings->Users->Numbers** menu consists of the following fields:

Fields in the Internal Numbers menu.

Field	Description
Internal Numbers	<p>Enter the internal numbers for the user and the description to be shown in the system telephone display (Displayed Description). In addition, select whether this internal number shall be displayed in the System Phonebook, and whether the LED next to the corresponding function key (Busy Lamp Field) should light up.</p> <p>The functions are activated by default.</p> <p>Add new Internal Numbers with Add.</p>

5.2.1.3 Outgoing Signalisation


In the **Numbering->User Settings->Users->Outgoing Signalisation** menu, select the outgoing numbers for the user.

For an outgoing call, if the remote subscriber should not see the number assigned to your own connection, one of the existing numbers can be selected here for display. If no number is defined, the system transmits no number to the provider.

Fields in the list Outgoing Signalisation


Field	Description
Internal Number	Displays the internal numbers configured for the user.
Displayed Description	Displays, for each internal number, the description configured for the system telephone display.
Outgoing Signalisation	<p>Select the signal you want for outgoing calls.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none"> • <i>Default, own DDI Signalling</i>: The user's own extension is used as the Outgoing Signalisation. This option is available when there is a point-to-point configuration or a SIP provider with direct dialling. • <i>Standard</i>: No Outgoing Signalisation is sent. In this case, the switchboard uses the port's main number. • <i><Fixed phone number></i>: For a FXO port, the phone number configured is already assigned as the Outgoing Signalisation and is displayed. • <i><Phone number></i>: When more than one number has been configured, you can select a number that you wish to use as the Outgoing Signalisation.

Select the  icon to specify for each internal number (indicated in the table by **Internal Number** and **Displayed Description**) which number shall be displayed for outgoing calls. Here, for each configured external connection, select one of the numbers configured for this purpose.

If more than one external connection has been configured, you can specify the procedure for outgoing calls. When an external line is engaged, the order of the entries determines the sequence in which the other lines assigned will be used to dial.

The configured **Outgoing Signalisation** can be hidden for each outgoing line; to do so, put a tick under **Hide Number** in the relevant row.

If you wish to move an entry in the list displayed, select the  icon in the relevant row. A new window opens.

The selected entry is displayed under **External Connection**, here e. g. *ISDN_1*.

Proceed as follows to move the selected entry:

- (1) Under **Move**, select in the list the entry relative to which you wish to move the selected entry, here e. g. *1.SIP-Provider_1*.
- (2) Select whether you want to insert the entry *above* or *below* the selected entry in the list, here e. g. *above*.
- (3) Select **Copy**.
The entries display in the changed order.
- (4) If the list contains more than two entries, move other entries if you wish.

The sequence configured here overwrites the setting that is assigned by the permission

class. However, the assigned permission class continues to determine whether a user has access to a particular external connection.

5.2.1.4 Optional Rerouting

In the **Numbering->User Settings->Users->Optional Rerouting** menu, to each displayed subscriber internal number you can assign a **Redirect application** and a **Active Variant (Day)**.

Here, for example, you can define to which co-worker calls shall be forwarded when you're in a conference, or whether the head office is responsible for taking calls during lunch.

Fields in the Optional Rerouting menu

Field	Description
Internal Number	Displays the internal numbers configured for the user.
Displayed Description	Displays, for each internal number, the description configured for the system telephone display.
Rerouting Application	<p>Select from the dropdown list the desired redirect application that you wish to assign to the internal number. You may choose from the redirect applications that you've configured in the Applications->Rerouting->Rerouting Applications->New menu with Type of redirect application = Internal Subscriber .</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i> • <Redirect application>
Active Variant (Day)	<p>Select the redirect application variant to be currently enabled. If a variant switch is set up via the calendar, this setting will be switched back again at the appropriate time.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Variant</i> • <i>Variant 2</i> • <i>Variant 3</i> • <i>Variant 4</i>

5.2.1.5 Authorizations

In the menu **Numbering->User Settings->Users->Authorizations** you can allow this user to make certain settings himself via HTML configuration. For this, a user name and password must be entered in the user HTML configuration, and personal access authorised. Once logged out, you can view and modify the corresponding settings after entering this user name and password.

The **Numbering->User Settings->Users->Authorizations** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Password for IP Phone Registration	Enter the password with which a user IP telephone must log in to the system. The password can remain free if IP telephones log in but need not authenticate themselves.
PIN for Phone Access	Here you can change the PIN for the user's personal answering machine (voicemail box). The default value is <i>none</i> .

Fields in the User HTML Configuration menu

Field	Description
Personal Access	Select whether this user shall receive access authorisation to a personalised user interface (user access) where he can perform his own entries and settings. The function is activated by selecting <i>Enabled</i> . The function is disabled by default.
Login Name	Only for Personal Access enabled. Enter a user name for this user. This is required for login on the user interface.
Password	Only for Personal Access enabled. Enter a password for this user. This is required for login on the user interface.

Call Through

Call Through consists in dialin to the system via an external connection and the call put through from the system via another external connection.



Note


In the connection data records, one data record is created for the incoming connection and one for the outgoing connection.

Fields in the Further Options menu

Field	Description
Call Through	<p>Select whether Call Through should be authorised for this user.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>When you enable the function, you must select under Use routing and signalisation from number the internal number from which the authorised external lines and call options for Call Through shall be used.</p>

5.2.2 Class of Services

In the **Numbering->User Settings->Class of Services** (CoS) the functions and performance features for the user settings are defined. These authorisation classes can then be assigned to individual users (user groups) in the user settings.

Choose the  icon to edit existing entries. Choose the **New** button to create additional authorisation classes. The authorisation class *Default CoS* is configured by default.

5.2.2.1 Basic Settings

In the menu **Numbering->User Settings->Class of Services->Basic Settings**, the basic settings along with the name for the new authorisation class are defined. The authorisation class can be located via the name.

The **Numbering->User Settings->Class of Services->Basic Settings** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the entry.

Fields in the Line Access Authorization menu

Field	Description
Line Access Authorization	<p>Select line access authorisation for the authorisation class.</p> <p>Line access authorisation determines which calls (internal, external,...) are allowed. The system distinguishes several authorisation levels.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>International</i>: The telephones have unrestricted dialling authorisations and can initiate all connections. • <i>National</i>: The telephones can initiate all calls except international calls. If a number starts with the code for international dialling, the number cannot be dialled. • <i>Incoming</i>: The telephones can receive incoming external calls, but cannot initiate any external calls. Internal calls are possible. • <i>Region</i>: The telephones cannot make any national or international calls. For this dial permission, 10 exception numbers allowing national or international dialling can be configured. An exception number can consist of complete call numbers or sections thereof (e. g. the first numerals). • <i>Local</i>: The telephones can make local calls. National and international calls are not possible. • <i>Internal</i>: The telephones do not have authorisation for incoming or outgoing external calls. Only internal telephone calls are possible.
Automatic Outside Line	<p>This setting defines whether automatic outside line is set up for this authorisation class. With automatic outside line, users of this authorisation class hear the external dialling tone after picking up the receiver and can immediately dial outside. To make internal calls, press the star key after picking up the receiver.</p>
Trunk Line Selection	<p>Select the connections over which outgoing calls from these</p>

Field	Description
with Line Access Number	telephones shall be externally routed. The order of entries determines in which sequence, in case of an engaged external line, dialling shall occur over the other assigned lines
Allow manual trunk group selection	<p>Besides general exchange access, a telephone can also selectively use a bundle. Here an external connection is initiated with the corresponding code for the target assignment of the bundle and not by dialling the dialling code.</p> <p>To be able to perform a selective bundle assignment, the authorisation class must possess the appropriate authorisation. The authorisation can also include bundles that the authorisation class can otherwise not assign. If a telephone does not possess the authorisation for selective bundle assignment, or if the selected bundle is in use, the busy tone is heard after dialling the code. If Automatic outside line is set up for an authorisation class, users of this authorisation class must press the star key before selective bundle assignment, then initiate external dialling with the code for bundle assignment.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>Then select the bundles for which manual bundle assignment is to be allowed. You can configure bundles in the Numbering->Trunk Settings->Trunk Groups menu.</p>

Number display

If you call a subscriber, your number is displayed to him. The person you're calling thus sees that you are calling even before picking up the receiver. If you don't want the person you're calling to see your number before picking up the receiver, you can prevent display of your number to your called party.

If your called party has set up call forwarding, you won't know at which telephone you've reached him. In this case, you can display the number to which your called party has forwarded the call. However, the person you're calling also has the option of preventing display of this number.

Call number display allows display of the caller's number already at call signaling, even on analogue telephones. Thus, you know who wishes to speak to you even before you've accepted the call.

**Note**

Transmission of analogue CLIP data can be set up separately for every analogue connection. Please refer to the users' guides for your analogue terminals to determine whether these support the "CLIP" and "CLIP off Hook" performance features.

Not all described performance features are included in the ISDN standard connection. Please inquire of your network operator the extent to which individual performance features must be separately ordered for your ISDN connection.

The menu **Advanced Settings** consists of the following fields:

Fields in the Further Settings menu

Field	Description
Dial Control	<p>Select whether numbers entered in the Call Routing->Outgoing Services->Dial Control menu shall be allowed or denied also for this authorisation class.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Automatic Route Selection (ARS)	<p>Select whether the routing rules entered in the Call Routing->Automatic Route Selection menu shall also be applied to this authorisation class.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Show Outgoing Number (CLIP)	<p>Select whether the caller number shall be displayed to the called party.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Show Connected Number (COLP)	<p>Select whether the called party number shall be displayed to the caller.</p> <p>If, for example, the called party has set up call forwarding to a</p>

Field	Description
	<p>third subscriber, the caller can display the number of the call forwarding destination using this performance feature.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Additional Info for Ex-tern Call	<p>Select what should be displayed for an exchange call.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Trunk and Number Name</i>: The display shows the exchange connection and the assigned name alternatively. • <i>Trunk Name Only</i>: Only the name assigned to the exchange connection is displayed. • <i>Number Name Only</i> (default value): The display shows the name assigned to the external number only. • <i>None</i>: Display is blank.

5.2.2.2 Features

Additional functions are configured in the **Numbering->User Settings->Class of Services->Features** menu.

Call pickup

A call is signalled to a co-worker who is presently absent from his work station. You now have two options to respond to the caller. You could walk over to your colleague's telephone, or transfer your colleague's call to your phone. Assignment is done by the option **Pick-up Group** in the menu **Features**; the group is then assigned to a user. If the values are identical, a call pickup is possible. Call pickup is not possible for open inquiry.

System telephones can pick up calls via programmed function keys. You can set up line keys, connection keys and team keys on system telephones.

- Line key: An ISDN connection or a VoIP provider is set up under a connection key. The LED assigned to the line key indicates the connection status. The LED lights up if both B channels of a connection are in use, or when the maximum number of simultaneous connections over a VoIP provider is reached. If an external call is signalled on another internal telephone, you can pick it up by pressing this line key.
- Line key: A system user is set up under a connection key. The LED assigned to the connection key indicates the subscriber status (call, connection,...). If a call is signalled

for this internal subscriber, you can pick it up by pressing this connection key.

- **Team key:** A team key is a normal line key to which the internal number of a team is assigned. The LED assigned to the team key indicates the team status (call, connection,...). If a call is signalled for this team, you can pick it up by pressing the team key.

Call waiting

As far as possible, you want to accept calls from every customer, even while you're already on the phone. If another call is signalled to your phone by a call-waiting tone or display notification, you can decide with which of two customers you wish to speak.

If a currently engaged subscriber is called, she gets automatic call-waiting. Call-waiting is possible for internal and external calls. The call-waiting connection is signalled to the called party visually and/or acoustically, depending on the terminal.

The called party can:

- Decline the call-waiting connection and proceed with the current call. The caller is then signalled "engaged".
- Accept the call-waiting connection and hold the current connection.
- Accept the call-waiting connection after the current connection is ended.
- Ignore the call-waiting connection. Call-waiting automatically ends after 30 seconds and the caller hears a "busy" signal.

Analogue terminals

The call-waiting option can be individually configured for every subscriber. Allowing call waiting or not can be set via configuration or via a code number in operations.

Analogue terminals get the system call waiting tone. The number of the call-waiting party can be shown in the analogue telephone display if it features the corresponding performance feature (CLIP off Hook). CLIP off Hook is disabled for analogue terminals in the basic setting, but may be enabled via configuration.

Call waiting can only occur simultaneously in the system for a limited number of analogue connections. If call waiting is already operating with this maximum number of call-waiting tones on analogue connections, additional call-waiting callers will get the busy tone.

If you hear the call-waiting tone during a call, you can take that call and transfer the ongoing call. An operating procedure allows transfer of the ongoing call and acceptance of the call waiting. The following conditions apply here:

- Every dialled number is accepted by the system.
- After the operation procedure, the subscriber and the call-waiting subscriber are immediately connected to each other (no acknowledge tones).

- Transfer to one's own number is possible, then call waiting.
- Internal, external target subscribers as well as teams can be dialled.
- A return call occurs in case of invalid or engaged target number.
- If the subscriber is free, a return call is made according to the target subscriber's defined period.
- With transfer to a team number, there is no return call in case of an engaged or unreachable team
- With transfer to a team number only return call after time is supported.

ISDN terminals

Configuration and operation of call waiting occurs as described in the users' guides of the corresponding terminals. ISDN terminals use their own tones to signal call waiting.



Note

Call waiting is not possible:

- for conference calls
- for do not disturb (analogue terminals)
- for announcements
- for room monitoring
- for terminals, for which the Data Protection performance feature is set up (e. g. fax, modem)
- in analogue subscriber's dialling status (the receiver has been picked up, but there is no connection yet)
- for current call-waiting protection
- for dialling a team number. Then there is no call waiting for analogue team subscribers.

ISDN telephones can also transfer a call waiting to another subscriber via the "Call Deflection" performance feature. An active connection is ended by replacing the receiver, for example. The call waiting connection is then signalled and can be accepted, e. g. by picking up the receiver.

The **Numbering->User Settings->Class of Services->Features** menu consists of the following fields:

Fields in the Feature Authorization menu

Field	Description
Pick-up Group	Enter the number of the group in which calls may be picked up.
Call Waiting	<p>Select whether call waiting shall be allowed for this authorisation class.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Use global rerouting	<p>Select whether global redirect shall be allowed for this authorisation class.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>The redirect target must be in a class of service that does not allow global redirect.</p> </div>
Switch signalling variants manually	<p>Select whether manual switching of call options shall be allowed for this authorisation class.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Call Through	<p>Select whether Call Through shall be allowed for this authorisation class.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

Simplex operation

The simplex operation function allows you to set up a connection from a system telephone to another system telephone without this connection having to be actively accepted by the called system telephone (pick up receiver, switch on loudspeaker/hands-free). As soon as the system telephone has accepted the simplex operation connection, the connection is set up. The caller and the called system telephone hear an attention tone at the beginning of the simplex operation. Duration of the simplex operation is limited to two minutes. If the

receiver of a concerned telephone is picked up during this period, the call is translated into a normal connection.

System telephones can initiate a simplex operation call via the system telephone menu or a programmed function key. If the simplex operation is initiated via a function key, notifications appear in the system telephone display as with a normal connection and the simplex operation key LED is switched on. The simplex operation can be ended by renewed pressing of the function key or by pressing the loudspeaker key. The LED switches off again at conclusion of the simplex operation.

If a telephone or a system telephone is the destination of a simplex operation call, the caller's number is indicated in the display. The simplex operation call is signalled over the loudspeaker with an attention tone. Simplex operation can be terminated with the ESC key.

A function key can also be configured on a system telephone to deny or allow simplex operation calls.



Note

Simplex operation calls are automatically accepted by the called telephone by enabling the hands-free function, if:

- the telephone is not in use
- simplex operation is allowed and
- the "Do not disturb" function (Call Protection) is disabled.

If a simplex operation connection is not ended by both subscribers, the connection is automatically ended by the system after ca. 2 minutes.

Message

Do you wish to call your co-workers to a meeting or to a meal? You could call each of them individually, or simply use the announcement function. With just one call, you reach all the announcement-enabled telephones without subscribers having to pick up the receiver.



Caution

Although you can be heard with the announcement, you cannot hear any comments your colleagues or family members make.

The announcement function allows you to set up a connection to another telephone

without this connection having to be actively accepted by the latter (pick up receiver or switch on loudspeaker/hands-free). As soon as a telephone has accepted the announcement, the connection is active. The announcer and the called subscriber initially hear a positive acknowledge tone. Announcement duration is unlimited.

Announcements are possible to ISDN and analogue telephones if these support the announcement performance feature. Please refer to the user's guide for your telephones to determine whether the performance feature is supported.

Announcements can be allowed or denied to telephones via a code number.

System telephones

Announcement to and from system telephones is possible. System telephones can initiate an announcement via the system telephone menu or using a programmed function key. If the announcement is initiated via a function key, notifications appear in your telephone display as with a normal connection and the announcement key LED is switched on. The announcement can be ended by renewed pressing of the function key or by pressing the loudspeaker key. The LED switches off again at conclusion of the announcement.

If a system telephone is the destination for an announcement, the number of the announcer appears on the display. The announcement is signalled with a positive acknowledge tone over the loudspeaker. The announcement can be terminated with the ESC key.

A function key with associated LED can also be set up on a system telephone to deny or allow announcements.

Individual announcement

You can initiate the announcement in a selective manner by dialling an internal number. The announcement can be allowed or denied by the destination subscriber via an operating procedure. The announcement is signalled to the destination subscriber and the announcer with a positive acknowledge tone.

Team announcement

An announcement can also be made to a team by dialling a team number. The team subscribers hear the announcement simultaneously. The announcement is signalled to the destination subscribers and the announcers with a positive acknowledge tone. The announcement to a team is also possible from an inquiry. With a team announcement, it can take up to four seconds before the connection to the individual team subscribers is established. The announcement then proceeds to the team subscribers who have accepted the announcement within this period.

**Note**

Announcements are automatically accepted by the called telephone by enabling the loudspeaker function, if:

- the telephone is not in use
- the announcement is set up and
- the "Do not disturb" function is not active.

MWI (Message Waiting Indication)

You've got new messages in your mailbox, or new e-mails waiting at your Internet service provider. As you have no prior knowledge, you must constantly check whether you do actually have new messages. With the MWI performance feature, your system receives the information about new messages from the corresponding service provider. Now you merely need query your mailbox or e-mail POB if new messages really are present. You can also send a MWI from a voicebox connected to the system, or from a system telephone set up as a reception telephone.

This information can be displayed or signalled on terminals (analogue terminals, ISDN terminals and system telephones) that support this performance feature. MMW information from outside is conveyed transparently by the system. When an MMI is present, the Gigaset telephone displays an envelope symbol and a text generated in the telephone, along with the caller's phone number.

Analogue terminals

- Switching on the MMI can only occur with receiver replaced.
- If there's a message from a voicemail system, there's a short call. Depending on the terminal, a symbol, a text generated in the telephone as well as the caller's telephone number can be displayed. If MWI information is deleted, there is no signalling.
- For the terminal, CLIP must be set up and enabled in the configuration.
- Callback to the voice mail system or reception telephone is possible; the MMI information is deleted in the process.

ISDN terminals

- Switching on the MWI is possible at all times (also during the call).
- If there's a message from a voicemail system, there's a short call. Depending on the terminal, a symbol, a text generated in the telephone as well as the caller's telephone number can be displayed. If MWI information is deleted, there is no signalling.
- Callback to the voice mail system or reception telephone is possible; the MMI informa-

tion is deleted in the process.

System telephones

- Switching on the MWI is possible at all times (also during the call). The caller's number is entered in the caller list. Depending on the type of system telephone, e. g. external voicemail, Netbox Heute, the name and number of the caller are entered. In addition, the **Caller list** LED flashes.
- Callback to the voice mail system or reception telephone is possible; the MMI information is deleted in the process.

Hotel room telephone

- If a message from a voicemail system is present, a special dialling tone is heard after the receiver is picked up.

Reception telephone

- MWI information can be switched on and off from a reception telephone to a room telephone via a telephone procedure. If MWI information is switched to a room telephone, the reception telephone number is entered into the caller list and the special dialling tone is enabled.

Disabling the MWI announcement

- Manual disabling via reception telephone procedure.
- Call from reception telephone to room telephone. The MWI information is automatically deleted in call status.
- Callback from room telephone to reception telephone deletes the MWI information.



Note

This performance feature must be requested for your ISDN connection from the network operator. There, you will also be informed of available services. The information can only be displayed on the internal ISDN terminal if an external MSN has been assigned to the terminal in the configuration.

All MWI data are deleted after a system reset.

Net Direct (keypad)

Some time ago, you purchased the most advanced telephone of the time. Since then, however, a number of new performance features have appeared on the public network,

which cannot be used by simply pressing a key. You can use the keypad function to employ your network operator's current ISDN functions by entering a key sequence from your ISDN or analogue telephone.

The keypad function allows control of service or performance features in your operator's network by entering character and numerical sequences.



Note

You can only use the keypad performance feature if it is supported by your network operator and has been requested for your ISDN connection. If you have set up an automatic outside line for an internal subscriber, the keypad functions cannot be directly used. First disable the **Automatic Outside Line** or dial the star key, then the code for manual outside line (e. g. 0) followed by keypad dialling, beginning with the star or hash key.

Keypad functions can only operate from terminals that have been assigned an external multiple subscriber number (MSN) in configuration and possess a keypad authorisation.

Your network operator's performance features are always set up for the number (MSN) sent by your terminal.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Receive System Intercom Call	<p>Select whether simplex operation calls to the system telephone shall be allowed for this authorisation class.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Receive Announcement Calls	<p>Select whether this authorisation class may receive announcements.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Receive MWI Information	<p>Select whether this authorisation class may receive information about existing messages (MWI = Message Waiting Indication).</p>

Field	Description
	<p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Net Direct (Keypad)	<p>Select whether you wish to use your network operator's current ISDN functions also from older ISDN or analogue telephones by entering a key sequence.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

5.2.2.3 Applications

Additional applications are configured in the **Numbering->User Settings->Class of Services->Applications** menu.

The **Numbering->User Settings->Class of Services->Applications** menu consists of the following fields:

Fields in the Application Authorization menu


Field	Description
System Phonebook Authorization	<p>Select whether this authorisation class may use entries in the system phone book and, if so, to what extent.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Yes, according to line access authorization</i> (default value): System phone book entries may be used unless located beyond the configured line access authorisation. • <i>Yes, without restrictions</i>: System phone book entries may be used in unrestricted access. • <i>No</i>: System phone book entries may not be used.
Music on Hold	<p>Select whether and which MoH (Music on Hold) shall be used.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Off</i> (default value): A caller on hold shall hear no music-on-hold. • <i><MoH-Wave file></i>: A caller on hold should hear the selec-

Field	Description
	<p>ted Wave file as music-on-hold.</p> <ul style="list-style-type: none"> • <i>MOH Internal 1</i> • <i>MOH Internal 2</i> • <i>MoH Wave 1 to 8</i>
Doorcom Access	<p>Select whether this authorisation class may connect to the door intercom.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
TAPI	<p>Select whether this authorisation class may use the system's TAPI functionalities.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Save call data records	<p>Define whether the connection data of this authorisation class shall be saved.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Transmit charge information	<p>Select whether the transferred charge information shall be transmitted to terminals of this authorisation class.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

5.2.3 Parallel Ringing

In the **Numbering->User Settings->Parallel Ringing** you configure whether, in case of incoming calls to an internal number, there shall be parallel signalling to another external number.

5.2.3.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create other entries.

The **Numbering->User Settings->Parallel Ringing->New** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Internal Number	Select the internal number for which the parallel call performance feature is to be set up.
External Number	Under New Number enter the external telephone number to which a call should be signalled in parallel. If a mobile number and a call number are configured for personal use under Users->Basic Settings->External Numbers , these are displayed in Configured Home Number or Configured Mobile Number and can be selected.
Parallel Ringing	Select whether this parallel call entry is to be enabled. The function is activated by selecting <i>Enabled</i> . The function is disabled by default.

5.3 Groups & Teams


In this menu, you configure your system's teams.

5.3.1 Teams

In the **Numbering->Groups & Teams->Teams** menu, you configure your system's teams.

Teams are groups of people working together to realise an objective. In practice, this means that all people within a team can be reached under the same subscriber number for external and internal calls. In the PABX, each team of telephones/terminals can thus be assigned a specific subscriber number to guarantee accessibility to internal and external calls. Individual structures of companies can be mapped by teams. Thus departments such as Service, Sales or Development can be called from inside or outside in a selective manner via team numbers. Within a team, the call can, for example, be signalled simultaneously to all, or first to one telephone, then also to a second, etc. In one team, answering machines or voice systems can also be used.

Four team call options are assigned to each team. Switching between call options can occur manually or via one of the calendars.

Choose the  icon to edit existing entries. Select the **New** button to create a new team.

5.3.1.1 General

In the **Numbering->Groups & Teams->Teams->General** basic conditions in the team are configured. Among these are the team name and the internal team number.

For internal team calls, a team number and team name can be assigned to the team in the configuration. If a team number is dialled, the caller sees the team name until a team subscriber accepts the call. The name of the team subscriber is then displayed.

The **Numbering->Groups & Teams->Teams->General** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the team.
Internal Number	Enter the internal number of the team.

Fields in the Further Settings menu

Field	Description
Switch call signalling	<p>Define whether the call option configured for the team shall be enabled manually over the telephone, or via the calendar. For this, calendar and switching times must first have been configured. You can create up to four call variants for each team in the menu Numbering->Groups & Teams->Teams->New->Variant1-4 .</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>No calendar, only manually</i>: Manual switch is enabled. • <i><Calendar></i>: Select one of the configured calendars.
Active Variant (Day)	Select one of the call options to be currently enabled. If a switch is set up via the calendar, this setting will be switched back again in a timely manner.
Permit Call Forwarding	<p>Define whether call forwarding may occur for the team.</p> <p>The function is activated by selecting <i>Enabled</i>.</p>

Field	Description
	The function is disabled by default.
Call Forwarding to External Numbers	Define whether there shall be call forwarding within the system itself (Through PABX) or via an exchange (provider, Through Exchange Office). Please note that for call forwarding within the system two external connections are used.

The menu **Advanced Settings** consists of the following fields:

Fields in the Timer menu

Field	Description
Team Speed Timer	Here, enter the Team Speed Timer following which call forwarding after time shall be performed in the team. The default value is <i>15</i> seconds.
Simultaneous on no response	With linear and rotating team calls, there is the option for all team subscribers to be simultaneously called after a defined period. The default value is <i>60</i> seconds.
Wrap-up Timer	This setting is only enabled in Signalling <i>Even Distribution (Longest Free)</i> . For every subscriber who has ended a call, a Post processing time is configured, during which he receives no more calls. Calls received by the subscriber on his number rather than via the team and self-initiated calls are not included in the time calculation. The default value is <i>60</i> seconds; the range <i>0... 999</i> seconds.

5.3.1.2 Variant 1 - 4

In the **Numbering->Groups & Teams->Teams->Variant 1-4** you configure a team's four call variants. You can create up to four different call options for each team. For this, assign either an internal or external number to the call option, and define how an incoming call should be signalled within the team.

Internal numbers of a team

Under **Internal Assignment**, select the internal subscribers who are to belong to this

team. If you wish to temporarily exclude a team subscribers from call signalling (e. g. team subscriber is on holiday), you can **Logout** the subscriber. Team calls are not signalled to logged out subscribers. Every team subscriber can also control login and logout himself via a system code.

For internal team calls, a team number and team name can be assigned to the team in the configuration. If a team number is dialled, the caller sees the team name until a team subscriber accepts the call. The name of the team subscriber is then displayed. A call to a team can be simultaneous, linear, rotating, setting up or parallel after time. With linear and rotating team calls, there is the option for all team subscribers to be simultaneously called after a defined period (1 - 99).

The **Numbering->Groups & Teams->Teams->Variant** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Assignment	<p>You can assign several internal numbers to each team, or an external number to each. Define whether calls for a team shall be signalled to internal or external subscribers.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>External</i>: The entered external number is called. • <i>Internal</i> (default value): The subscribers assigned to the selected number are called according to the defined signalling.
Internal Assignment	<p>Only if Assignment = <i>Internal</i></p> <p>Select the internal team subscribers.</p> <p>With Add, you add more internal numbers.</p>
External Assignment	<p>Only if Assignment = <i>External</i></p> <p>Enter the number of the external subscriber.</p>
Route and Charge Assignment	<p>Only if Assignment = <i>External</i></p> <p>Charges for the call and assignment of an external connection occur via the selected internal subscriber.</p>

Automatic call acceptance in the team

You want a caller to be accepted already at call signalling and not to hear the ringing tone. That's no problem if you're using automatic call acceptance for team calls. In this case, the caller is automatically accepted by the system and hears an announcement or system music-on-hold. During this time, the call is signalled to the entered team subscribers. If a subscriber takes the call, the connection to the caller is established.

If a team is called, it can be defined in configuration that the call is automatically accepted, and that the caller hears an announcement or music. The target subscriber(s) are called during this time. After the receiver is picked up, the announcement or music is turned off and the subscribers are connected to each other.

Possible settings for automatic call acceptance:

- *Simultaneous*: All assigned terminals are called simultaneously. If a terminal is busy, call waiting can be used.
- *Linear*: All assigned terminals are called in the sequence of their entry in configuration. If a terminal is engaged, the next free terminal is called. The call is signalled ca. 15 seconds per subscriber. This period can be set between 1 and 99 seconds (per team) in the configuration. If subscribers are on the phone or logged out, there is not forwarding time for these.
- *Rotating*: This call is a special case of the linear call. After all terminals are called, call signalling begins again with the first entered terminal. The call is signaled until the caller replaces the receiver or the call is ended by the exchange (after ca. 2 minutes).
- *Adding*: The terminals are called in the order of their entry in the subscriber list. Every terminal that has already been called is called again, until all entered terminals are called.
- *Linear, Simultaneous on No Reply*: Rotating or linear is set for the team call. After defined times have run out, all team subscribers can be called in parallel (simultaneously). Example: A precondition is that the sum of forwarding times is larger than the time **parallel after time**. There are 4 subscribers to a team. The forwarding time for each subscriber is 10 seconds, 40 seconds in total. The time **parallel after time** is set to 38 seconds. Every subscriber will be called. If a subscriber logs out of the team or is engaged, forwarding time is only 30 seconds, after which the **parallel after time** call is no longer made.
- *Even Distribution (Longest Free)*: Even distribution corresponds to **SignallingRotating** and insures that all team subscribers receive the same number of calls. For every subscriber who has ended a call, a **Wrap-up Time** (0...999 seconds) is set up for the team/subscriber, during which she receives no more calls. Calls received by the subscriber on his number rather than via the team and self-initiated calls are not included in the even distribution calculation. Even distribution begins with the subscriber who hasn't received calls for the longest time, on restart with the first subscriber entered in the subscriber list. A subscriber who has logged out of the team (code number or function key) is no longer taken into account for the even distribution. After a system

power failure, the existing **Even distribution** calculation is deleted and the process begins again. If all team subscribers are in **Post processing time**, external calls are routed to the preset redirect destination; internal calls hear the busy tone. If the same time since the last call is calculated for several team subscribers, the sequence of entries in **Internal Assignment** applies.

Fields in the Options menu

Field	Description
Signalling	<p>You can call team subscribers with a broadcast call.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Simultaneous</i> (default value) • <i>Linear</i> • <i>Rotating</i> • <i>Adding</i> • <i>Linear, Simultaneous on No Reply</i> • <i>Rotating, Simultaneous on No Reply</i> • <i>Even Distribution (Longest Free)</i>
Busy on busy	<p>Select whether the performance feature "Busy on Busy" is to be enabled for this call option.</p> <p>If a team subscriber is currently engaged, you can decide whether additional calls for this team should be signalled. If "Busy on Busy" is set for a team, other callers are signalled as "engaged".</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Automatic Call Pick-up with	<p>Select whether an incoming call should be automatically accepted, and the caller hear the desired music-on-hold or announcement. Signalling of the call to the team proceeds. The caller bears the costs for the existing connection.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>Also select the desired music-on-hold or announcement.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none"> • <i><File_x></i> • <i>MOH Internal 1</i> • <i>MOH Internal 2</i> • <i>MoH Wave 1 to 8</i>

The menu **Advanced Settings** consists of the following fields:

Fields in the Rerouting Functions menu

Field	Description
Rerouting on no response	<p>Select whether and, if so, to which team an incoming call should be redirected on no reply.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i> • <i><Team></i> <p>Also enter the time after which the call should be redirected.</p>
Further Rerouting	<p>Select whether and, if so, to which redirect option an incoming call shall be switched.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Off</i>: No other redirect options are used. • <i>Immediately</i>: The incoming call is immediately rerouted to the redirect function selected in Immediately. • <i>On Busy</i>: The incoming call is rerouted to the redirect function selected in On Busy.
Immediately	<p>Only if Further Rerouting = <i>Immediately</i></p> <p>Select the redirect function for immediate redirect. Configure redirect functions in Applications->Rerouting->Rerouting Functions.</p>
On Busy	<p>Only if Further Rerouting = <i>On Busy</i></p> <p>Select the redirect function for redirect on engaged. Configure redirect functions in Applications->Rerouting->Rerouting Functions.</p>

Field	Description
Busy starting with	Only if Further Rerouting = <i>On Busy</i> Select from which number of subscribers the team is considered engaged.

5.3.1.3 Log on / Log off

In the **Numbering->Groups & Teams->Teams->Log on / Log off** individual team members are logged in or out.

The **Numbering->Groups & Teams->Teams->Log on / Log off** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Numbers	Indicates the internal number of assigned team members.
Status	Select whether the team member is logged into the team. The team member is logged in by selecting <i>Logged on</i> .

5.4 Call Distribution


In this menu, you configure internal forwarding of all incoming calls.

5.4.1 Incoming Distribution

In the **Numbering->Call Distribution->Incoming Distribution** menu, you configure the assignment of incoming calls to the desired internal numbers..

In Call Assignment, you assign the call numbers entered under **External Numbers**, e.g. to the teams or to an internal number.

5.4.1.1 Edit

Choose the  icon to edit existing entries.

The **Numbering->Call Distribution->Incoming Distribution->** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
<Name of Number-Entry>	Displays the number configured.
Trunk	Displays the external connection for which call assignment is configured.
Assignment	<p>Select the internal number or the desired function to which incoming calls shall be assigned via the line selected in Trunk.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Internal Number</i> (default value): The internal team number is selected for assignment to a team. • <i>Call Through</i> • <i>Redirect application</i> • <i>Phone Remote Access</i> • <i>ISDN Login</i> • <i>Service Login</i> • <i>Mini Call Center</i>

Fields in the Internal Number and Rerouting Settings menu

Field	Description
Internal Number	<p>Only for Assignment = <i>Internal Number</i></p> <p>Select the internal number to which incoming calls shall be assigned via the line selected in Trunk.</p>
Rerouting Application	<p>Only for Assignment = <i>redirect application</i></p> <p>Select the desired redirect application to be assigned to the number. You can configure redirect applications in the Applications->Rerouting->Rerouting Applications menu.</p>
Active Variant (Day)	<p>Only for redirect application = <<i>configured redirect application</i>></p> <p>Select the redirect application variant to be currently enabled. If a variant switch is set up via the calendar, this setting will be switched back again at the appropriate time.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Variant 1</i> • <i>Variant 2</i> • <i>Variant 3</i> • <i>Variant 4</i>

Fields in the Call Through Settings menu

Field	Description
Authorization	<p>Only for Assignment = <i>Call Through</i></p> <p>Define the authorisation for which the Call Through function shall be released.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Number screening</i>: Dialling release occurs after matching the entered number with the entry in the system phone book or with the user's call number entries (Mobile Number and Home Number). • <i>Number screening and PIN</i>: Dialling release occurs after matching the entered number with the entry in the system phone book or with the user's call number entries (Mobile Number and Home Number) AND PIN entry. • <i>PIN</i>: Dialling release occurs after PIN entry. • <i>Number screening or PIN</i>: Dialling release occurs after matching the entered number with the entry in the system phone book or with the user's call number entries (Mobile Number and Home Number) OR PIN entry.
PIN (6 Digit Numeric)	<p>Only for Authorization = <i>Number screening and PIN, PIN, Number screening or PIN</i></p> <p>The system checks the caller's authorisation for Call Through, then activates a simulated external dialling tone for the call. Authorisation is granted if the caller has entered the correct 6-digit PIN.</p>
Internal Number and Rerouting Settings	<p>Select the internal subscriber via which Call Through is to occur. One of the system's telephone numbers is defined in the configuration for Call Through. An external caller using this</p>


Field	Description
	telephone number first hears the system's attention tone.

5.4.2 Misdial Routing

In the menu **Numbering->Call Distribution->Misdial Routing** for every external connection, you define the subscriber or the team to which the call shall go in any of the following cases:

- an incoming call has a wrong or truncated number / extension
- all members of the called team or call center are logged off.
- all members of the called call center are in post-processing.

5.4.2.1 Edit

Choose the  icon to edit existing entries.

The **Numbering->Call Distribution->Misdial Routing->** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Trunk	Displays the external connection for which redirect for wrong dialling is configured.
Rerouting to Number	Select the type of rerouting: <ul style="list-style-type: none"> • <i>None</i>: No redirect here, the caller gets a busy tone. • <i>Global Settings</i>: Redirect occurs as entered in System Management->Global Settings->System->Rerouting to Number. • <i><Internal number of a user or team></i>: The call is redirected to this user or team.

Chapter 6 Terminals

6.1 Gigaset Phones


In this menu, you perform assignment of configured internal numbers to the terminals and set additional functions according to terminal type.


The system telephone end devices are listed alphabetically in the **Description** column. Click the column title of any other column to sort entries in ascending or descending order

6.1.1 Gigaset Phones


In the **Terminals->Gigaset Phones->Gigaset Phones** menu you assign the configured internal numbers to the connected devices.

Any devices that are connected are automatically detected and listed in the lower part of the overview.

Choose the  icon to edit existing entries. As soon as a **Description** is entered for the telephone and saved with **OK**, the entry for that device is moved to the upper part of the overview.

To continue with configuring, click the  symbol again.

Select the **New** button to manually set up a new IP end device.

Select the  button to go to the Gigaset telephone user interface administrator page. This is described in the telephone user guide!

6.1.1.1 General

In the menu **Terminals->Gigaset Phones->Gigaset Phones->General**, you make the basic settings for an IP telephone.

The **Terminals->Gigaset Phones->Gigaset Phones->General** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Description	To clearly identify the telephone in the system, enter a descrip-

Field	Description
	tion for the telephone.
Phone Type	<p>Displays the type of your IP telephone.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>DE310 IP PRO</i> • <i>DE410 IP PRO</i> • <i>DE700 IP PRO</i> • <i>DE900 IP PRO</i>
Location	<p>Select the location of the telephone. You define locations in the VoIP->Settings->Locations menu. Depending on the setting in this menu, default behaviour for registration of VoIP subscribers for which no location should be defined is displayed for selection.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Not defined (Unrestricted Registration)</i>: No location is defined. According to set default behaviour, the subscriber is nevertheless registered. • <i>Not defined (No Registration)</i>: No location is defined. According to set default behaviour, the subscriber is not registered. • <i>Not defined (Registration for Private Networks Only)</i>: No location is defined. According to set default behaviour, the subscriber is only registered if located in a private network. • <i><Location></i>: A defined location is selected. The subscriber is only registered if at this location.
MAC Address	Shows the MAC address of the telephone.

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Further Settings

Field	Description
No Hold and Retrieve	The performance features hold a call and retrieve a held call are not available on certain telephones.

Field	Description
	The function is activated by selecting <i>Enabled</i> . The function is disabled by default.


Fields in the menu **Codec Settings**

Field	Description
Codec Profile	Select the Codec profile to be used. Codec profiles are configured in the VoIP->Settings->Codec Profiles menu.

6.1.1.2 Numbers

In the menu **Terminals->Gigaset Phones->Gigaset Phones->Numbers** you assign an IP telephone up to twelve internal phone numbers using **Add**.

The available internal phone numbers are created under **Numbering->User Settings->Users->New**.

You can delete assigned numbers from the list with .

Values in the list **Number Settings**

Field	Description
Connections Nr.	Shows the serial number of the connection.
Internal Number	Displays the assigned internal number.
Displayed Description	Displays the description that will be displayed on the IP telephone's display.
User	Displays the user's name.

6.1.1.3 Settings

In the **Terminals->Gigaset Phones->Gigaset Phones->Settings** menu you can reset the telephone's administrator password.

The **Terminals->Gigaset Phones->Gigaset Phones->Settings** menu consists of the following fields:




Fields in the menu **System Phone**


Field	Description
Admin Password	<p>Select whether the administrator password should be reset.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>As soon as you select the OK button, the password is reset to the default setting.</p>

6.1.2 Gigaset DECT


The menu **Terminals->Gigaset Phones->Gigaset DECT** displays the base stations of the connected DECT single-cell and multi-cell systems.

Any base stations that are connected are automatically detected and listed in the lower part of the overview. (DHCP is required for this.)

Choose the  icon to edit existing entries. As soon as a **Description** is entered for a base station and copied with **OK**, the entry for that device is moved to the upper part of the overview. After a short time, the icons  and  are displayed for this device.


To be able to use automatic provisioning, click the  icon again and add the relevant phone numbers.

Select the **New** button to manually set up a new base station.


Select the button  to go to the base station's Web configurator. This is described in the user guide for the relevant DECT system!

Use the automatic provisioning to use the **elmeg hybrid** to transfer elementary telephony parameters to the DECT system. If you want to use the assistant **First Steps** to do this, you activate the value *elmeg IP1x/DECT* under **Assistants->First steps->Advanced Settings->Add** in the field **Transmit Provisioning Server for** . Instead of this, you can also set the fields **Option** = *URL (provisioning server)* and **Value** = *http://<IP address of the provisioning server>/eg_prov* under **Local Services->DHCP Server->DHCP Configuration->New->Advanced Settings** .

To register the mobile parts you first set the base station to login mode. Then you do the registering of the mobile parts on the mobile parts themselves. To configure the base station in any more detail, you need to use the DECT system's web configurator.

Select the button  to trigger an update of the device's provisioning. If the update is successful, the updated value displays in the **Last seen** column within 10 seconds.

**Note**

If you wish to test whether your base station is correctly configured and accessible, select the button  and check whether an updated value is displayed within 10 seconds in the **Last seen** column.

**Note**

If you wish to change the language currently used with a DECT single-cell system, the system has to be connected to the provisioning server of the **el-meg hybird**. You required an installed SD card. All the languages used need to be stored on the SD card. Single-cell systems load the language required from the SD card when necessary.

6.1.2.1 General

In the menu **Terminals->Gigaset Phones->Gigaset DECT** you make the basic settings for base stations.

The **Terminals->Gigaset Phones->Gigaset DECT->General** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Description	To clearly identify the base station in the system, enter a description for the telephone.
Phone Type	Displays the type of base station. Possible values: <ul style="list-style-type: none"> • <i>N510 IP PRO</i> • <i>N720 DM PRO</i>
Location	Select the location of the base station. You define locations in the VoIP->Settings->Locations menu. Depending on the setting in this menu, default behaviour for registration of VoIP subscribers for which no location should be defined is displayed for selection.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Not defined (Unrestricted Registration)</i>: No location is defined. According to set default behaviour, the subscriber is nevertheless registered. • <i>Not defined (No Registration)</i>: No location is defined. According to set default behaviour, the subscriber is not registered. • <i>Not defined (Registration for Private Networks Only)</i>: No location is defined. According to set default behaviour, the subscriber is only registered if located in a private network. • <i>Location</i>: A defined location is selected. The subscriber is only registered if at this location.
MAC Address	Shows the MAC address of the base station.
IP/MAC Binding	<p>Displays the IP address automatically assigned by DHCP.</p> <p>Here you have the option of permanently assigning the displayed IP address to the base station with the displayed MAC address.</p> <p>This option should be activated to enable quick re-login after a functional fault.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Further Settings

Field	Description
No Hold and Retrieve	<p>The performance features hold a call and retrieve a held call are not available on certain telephones.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

Fields in the menu Codec Settings

Field	Description
Codec Profile	Select the Codec profile to be used. Codec profiles are configured in the VoIP->Settings->Codec Profiles menu.

6.1.2.2 Numbers

In the menu **Terminals->Gigaset Phones->Gigaset DECT->Numbers** you assign **Internal Numbers** to the mobile parts. You can select from the numbers that you have created for this purpose under **Numbering->User Settings->Users**.

The system automatically assigns a serial number, the **Mobile Number**, to each mobile part so that you can identify the device. You can then use **Add** to assign a **Internal Number** to a mobile part from the list.

You can delete assigned numbers with .

Values in the list Numbers

Field	Description
Mobile Number	Displays the serial number of the mobile part. This number is permanently assigned to the mobile part so that it can be uniquely identified.
Internal Number	Displays the assigned internal number.
Displayed Description	Displays the description entered for the internal number. In standby mode this description is shown on the mobile part's display.
User	Displays the user's name.

6.1.2.3 Settings

In the **Terminals->Gigaset Phones->Gigaset DECT->Settings** menu you can reset the administrator password for the base station.

The **Terminals->Gigaset Phones->Gigaset DECT->Settings** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Admin Password	Select whether the administrator password should be reset. The function is activated by selecting <i>Enabled</i> .

Field	Description
	<p>The function is disabled by default.</p> <p>As soon as you select the OK button, the password is reset to the default setting.</p>

6.2 Other phones


In this menu, you perform assignment of configured internal numbers to the terminals and set additional functions according to terminal type.

Terminals of the corresponding category (VoIP, ISDN, or analog) are sorted alphabetically in the **Description** column. Click the column title of any other column to sort entries in ascending or descending order

6.2.1 VoIP

In the **Terminals->Other phones->VoIP** menu, you configure the connected VoIP terminals. For example, you perform assignment of a configured internal number.

6.2.1.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to add VoIP terminals.

The **Terminals->Other phones->VoIP->New** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Description	Enter a description for the IP telephone.
Location	<p>Select the location of the telephone. You define locations in the VoIP->Settings->Locations menu. Depending on the setting in this menu, default behaviour for registration of VoIP subscribers for which no location should be defined is displayed for selection.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <i>Not defined (Unrestricted Registration)</i>: No location is defined. According to set default behaviour, the subscriber is nevertheless registered.

Field	Description
	<ul style="list-style-type: none"> • <i>Not defined (No Registration)</i>: No location is defined. According to set default behaviour, the subscriber is not registered. • <i>Not defined (Registration for Private Networks Only)</i>: No location is defined. According to set default behaviour, the subscriber is only registered if located in a private network. • <i><Location></i>: A defined location is selected. The subscriber is only registered if at this location.

Fields in the menu **Number Settings**

Field	Description
Internal Numbers	<p>Select the internal number for this terminal You can define several internal numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>No free Extension Available</i>: All configured internal numbers are already in use. First configure another user with additional numbers. • <i><Internal Number></i>: Select one of the existing numbers of the configured users.

The menu **Advanced Settings** consists of the following fields:

Fields in the menu **SIP Client Settings**

Field	Description
SIP Client Mode	<p>Select whether a <i>dynamic</i> SIP client or a <i>static</i> SIP client is to be used.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Dynamic</i> (default value): Your device (e. g. a standard SIP telephone) runs a SIP registration to tell the system its (dynamic) IP address. • <i>Static</i>: The system accepts an incoming call from a (statically configured) SIP client without this client needing to have been registered beforehand, if the IP address of the client matches the IP address entered under SIP Client IP Address. This mode is used by, for example, the Microsoft Office Communications Server and other unified xommunica-

Field	Description
	tion servers.
SIP Client IP Address	Only for SIP Client Mode = <i>Static</i> . Enter the static local IP address of the SIP client.
Port Number	Only for SIP Client Mode = <i>Static</i> Enter the number of the port to be used for connection. A 5 digit sequence is possible. For example, port <i>5065</i> must be entered for connection to a Microsoft Exchange Communication Server.
Transport Protocol	Only for SIP Client Mode = <i>Static</i> Select the transport protocol for the connection. Possible values: <ul style="list-style-type: none"> • <i>UDP</i> (default value) • <i>TCP</i> For example, the <i>TCP</i> protocol must be entered for connection to a Microsoft Exchange Communication Server.

Fields in the menu **Codec Settings**

Field	Description
Codec Profile	Select the codec profile to be used if the connection is over a VoIP line. Codec profiles are configured in the VoIP -> Settings -> Codec Profiles menu.

Fields in the menu **Further Settings**


Field	Description
Multiple SIP Connections (Sub-Exchange)	Select whether multilinks shall be allowed from this terminals. Operation as subsystem: Only in case of connection of a subsystem to a system Here, with a disabled performance feature, only a connection via the subscriber SIP registration is possible. If a second call comes in, it is accepted and the existing call is held. With an enabled performance feature, several SIP connections are possible over the same login. If the perform-

Field	Description
	<p>ance feature is enabled for as system without subsystem, two simultaneous calls on the phone are not connected to each other after the receiver is replaced but released, for example. Here, the performance feature should not be set.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
No Hold and Retrieve	<p>The performance features "hold a call" and "retrieve a held call" are not available on certain telephones.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

6.2.2 ISDN

In the **Terminals->Other phones->ISDN** menu, you configure the connected ISDN terminals. For example, you perform assignment of a configured internal number.

6.2.2.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to add ISDN terminals.

The **Terminals->Other phones->ISDN->New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the ISDN telephone.
Interface	Select the interface to which the ISDN telephone shall be connected.

Fields in the Basic Phone Settings menu


Field	Description
Terminal Type	<p>Select the terminal type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Telephone</i> (default value)


Field	Description
	<ul style="list-style-type: none"> • <i>Answering Machine</i> • <i>Voice Mail</i> • <i>Emergency Phone</i>
Internal Numbers	<p>Select the internal number for this terminal You can define several internal numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>No free Extension Available</i>: All configured internal numbers are already in use. First configure another user with additional numbers. • <i><Internal Number></i>: Select one of the existing numbers of the configured users.

6.2.3 analog

In the **Terminals->Other phones->analog** menu, you configure the connected analogue terminals. For example, you perform assignment of a configured internal number.

6.2.3.1 Edit

Choose the  icon to edit existing entries.

Choose the  icon to copy existing entries. Copying an entry can prove useful if you wish to create an entry only distinguished by a few parameters from an existing entry. In this case, you copy the entry and modify the desired parameters.

The **Terminals->Other phones->analog->Edit** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the analogue telephone.
Interface	Select the interface to which the telephone shall be connected.

Fields in the Basic Phone Settings menu

Field	Description
Terminal Type	Select the terminal type.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Multi Function Device/Telefax</i> • <i>Telephone</i> • <i>Modem</i> • <i>Answering Machine</i> • <i>Emergency Phone</i>
Internal Number	<p>Select the internal number for this terminal.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>No free Extension Available</i>: The configured internal number is already in use. First configure another user with additional numbers. • <i><Internal Number></i>: Select one of the existing numbers of the configured users.

Fields in the Phone Settings menu

Field	Description
Call Waiting	<p>Select whether call waiting shall be allowed for this device.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Do not Disturb	<p>Select whether you wish to use the call protection (do not disturb) performance feature.</p> <p>With this performance feature, you can enable call signalling to your terminal. Analogue terminals use system code numbers for this.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Internal Calls not signaled</i> • <i>External Calls not signaled</i> • <i>No Calls signaled</i>

The menu **Advanced Settings** consists of the following fields:

Fields in the CLIP Settings menu

Field	Description
Show incoming Number (CLIP)	<p>Select whether the subscriber's number shall be transmitted.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Show Date and Time	<p>Only for Show incoming Number (CLIP) <i>Enabled</i></p> <p>Select whether the time and date should be taken from your hybird and displayed on the telephone.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Show incoming Name (CNIP)	<p>Only for Show incoming Number (CLIP) <i>Enabled</i></p> <p>Select whether the caller's number shall be displayed. The caller's number can be displayed if an entry exists in the system telephone book.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Show incoming waiting Number (CLIP off Hook)	<p>Only for Show incoming Number (CLIP) <i>Enabled</i></p> <p>Select whether the number of a caller waiting during an existing call shall be displayed.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

Fields in the Further Settings menu


Field	Description
Show new Messages (MWI)	<p>Only for Show incoming Number (CLIP) <i>Enabled</i></p> <p>Select whether new messages shall be signalled on a voice mail system.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

Field	Description
Transmit Charges Pulses	<p>Select whether the system shall generate charge pulses for the terminal from the ISDN network charge information. For this purpose, you can define the charge impulse at 12 kHz or 16 kHz.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>off</i>: Charge information from the ISDN network is not transmitted. • <i>12 kHz</i> • <i>16 kHz</i>
FXS Ringing Frequency	<p>Call signalling in analogue terminals occurs by configuring a call switching voltage at the called analogue connections. This call switching voltage is converted into a specific ring tone by the analogue terminal. In the system, for the analogue connections you can set a call switching voltage with a frequency of <i>25 Hz</i> or <i>50 Hz</i>.</p> <p>The default value is <i>50 Hz</i>.</p>
Flash Time for DTMF Dialling	<p>When operating analogue terminals with the multifrequency code dialling method, you can set the flashtime that the system detects as maximum flash length. If the terminal flash is longer than the defined period, "replaced receiver" is detected.</p> <p>Values from <i>100 ms</i> (standard value) to <i>1000 ms</i> are possible.</p>

6.2.4 CAPI

If your device supports CAPI, you configure the connected CAPI terminals in the menu **Terminals->Other phones->CAPI**. For example, you perform assignment of a configured internal number.

6.2.4.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to add CAPI terminals.

The **Terminals->Other phones->CAPI->New** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Description	Enter a description for the CAPI telephone.

Fields in the menu **Basic Phone Settings**

Field	Description
Internal Numbers	<p>Use Add to select the internal number for this terminal. You can define several internal numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>No free Extension Available</i>: All configured internal numbers are already in use. First configure another user with additional numbers. • <i><Internal Number></i>: Select one of the existing numbers of the configured users.

6.3 Overview

6.3.1 Overview

In the **Terminals->Overview->Overview** menu, you get an overview of all configured terminals.

Values in the Overview list

Field	Description
Description	Displays the terminal description.
Phone Type	Displays the telephone type.
Interface / Location	For ISDN, system and analogue terminals, displays the interface at which you're connected to the system. The configured location is displayed for IP terminals.
Internal Numbers	Displays the configured internal number.

Chapter 7 Call Routing

The functions for external calls and automatic route selections for external calls are defined in call routing.

7.1 Outgoing Services

In the **Call Routing->Outgoing Services** menu, you can configure the performance features **Direct Call**, **Call Forwarding**, **Dial Control** and **Priority Numbers**.

7.1.1 Direct Call

In the **Call Routing->Outgoing Services->Direct Call** menu, you configure numbers dialled directly without the subscriber on the phone having to dial a number him/herself.

You wish to set up a telephone for which the connection to a specific number is established without entering the number (e.g. emergency telephone). You are not at home. However, there is someone at home who needs to be able to reach you quickly and easily by telephone if necessary (e. g. children or grandparents). If you have set up the "Direct Call" function for one or more telephones, the receiver of the corresponding telephone only needs to be lifted. After a time period without further entries set in configuration, the system automatically dials the configured direct call number.

If you do not dial within the specified period from picking up the receiver, automatic dialling is initiated.


The time for the direct call is set under **System Management->Global Settings->Timer->Direct Call**.



Note

In the system, up to 10 direct call destinations with names and telephone numbers can be set up by the administrator. These destinations should then only be assigned to the terminals by the user via the user configuration interface. In the configuration, system direct call, or a direct call specifically configured for the terminal, can then be set by the user.

7.1.1.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

The **Call Routing->Outgoing Services->Direct Call->New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the entry.
Direct Call Number	Enter the number to be automatically dialed if no number is to be dialed for a certain time after the receiver has been picked up.

7.1.2 Call Forwarding

In the **Call Routing->Outgoing Services->Call Forwarding** menu, you configure call forwarding of external calls for an internal subscriber.

You are temporarily away from your office, but don't want to miss a call. With call forwarding to another number, e.g. your mobile, you can receive your calls even when you are not at your desk. You can forward calls on your number to any call number. It can occur **Immediately**, **On no reply** or **On Busy**. Call forwarding **On no reply** and **On Busy** can exist concurrently. If you are not near your telephone, for example, the call is forwarded to another number (e.g. your mobile phone) after a short period. If you are making a call at your desk, other caller may receive the busy signal. You can forward these callers e.g. to a colleague or the secretary by using call forwarding on busy.

Every internal subscriber to the system can forward her calls to another number. Calls can be forwarded to internal subscriber numbers, internal team numbers or external numbers. When the number to which calls shall be forwarded is entered, the system automatically checks whether it's an internal or external number.

In a team, call forwarding can be set up for one subscriber in the team. This call continues to be signalled to the other team subscribers. Call forwarding to an internal or external subscriber is performed in the system.

Call forwarding to an internal number is performed in the system. If an internal call to an external number is to be forwarded, forwarding also occurs in the system. Here, the connection is on the bundle cleared for the subscriber doing the setup. If call forwarding occurs via an ISDN connection, one B channels remains in use; in case of forwarding from external to external, it's both B channels. Two possibilities exist for call forwarding of an external call to an external number:

- Call forwarding in the exchange: Call forwarding is conducted at the exchange if only one subscriber is entered in the call allocation for an external call. For call forwarding in

the exchange, the performance features Call Deflection (point-to-multipoint connection) or Partial Rerouting (point-to-point connection) must be enabled with the network operator for the relevant ISDN connections.


- Call forwarding in the system: Call forwarding occurs in the system if the required performance features for call forwarding at the exchange are not available for the relevant ISDN connections. If several telephones (e. g. a team), some of which have set up call forwarding, receive an external call, the corresponding call forwarding is performed in the system. Here, the external connection is set up over a bundle's B channel, cleared for the subscriber initiating the setup. This B-channel remains assigned for the duration of active call forwarding.



Note

If the system is connected to the external ISDN, for external-to-external connections, the system systematically attempts to initiate call forwarding via the exchange. For teams, there can be manual definition of whether call forwarding shall occur via the exchange or the system. If the system possesses no ISDN connections, or if Call Deflection (point-to-multipoint connection) or Partial Rerouting (point-to-point connection) has not been ordered from the network operator, call forwarding occurs solely in the system.

7.1.2.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

The **Call Routing->Outgoing Services->Call Forwarding->New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Internal Number	Select the internal number to which the incoming calls shall be forwarded.
Type of Call Forwarding	Select when incoming calls shall be forwarded to the specified internal number. Possible values: <ul style="list-style-type: none"> • <i>Immediately</i> • <i>On Busy</i>

Field	Description
	<ul style="list-style-type: none"> • <i>On no reply</i> (default value) • <i>On busy / On no reply</i>
Target Number "On no reply"	Enter the number to which incoming calls shall be forwarded after time.
Target Number "On busy"	Enter the number to which incoming calls shall be forwarded on busy.
Target Number "Immediate"	Enter the number to which incoming calls shall be forwarded immediately.

7.1.3 Dial Control

In the **Call Routing->Outgoing Services->Dial Control** menu, you block specific numbers/partial numbers, or release these .

You wish to prevent dialling of specific numbers in the system, e. g. the numbers of expensive value-added services. Enter these numbers or partial numbers into the dial ranges list of blocked numbers. All subscribers subject to dial ranges cannot dial these numbers. However, if you should need specific numbers from a blocked sector, you can clear these via the dial ranges list of cleared numbers.

You can block specific numbers or prefixes with the blocked numbers list. You can clear the blocked numbers or prefixes with the cleared numbers list. If a number entered as a cleared number is longer than one entered as a blocked number, this number can be dialled. When you dial a number, dialling after the blocked digit is terminated and you hear the busy tone. You can assign each user individually to the dial ranges in the user settings.

Example: Blocked number *01*, all external numbers that begin with *01* are blocked. Cleared number *012345*, dialling can proceed. All external numbers that begin with *012345* can be dialled. If two identical numbers (same number sequence and same number of digits, e. g. *01234* and *01234*) are entered in the list of cleared numbers as well as the list of blocked numbers, dialling of the number is prevented.




Note

Subscribers who enjoy full or partial dialling access (no outside line access) are authorised for dialling of cleared numbers via the list of cleared numbers.

Please ensure that the area code is entered in the configuration, otherwise, the block can be circumvented in the local network by prefixing the area code.

7.1.3.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

The **Call Routing->Outgoing Services->Dial Control->New** menu consists of the following fields:

Fields in the Basic Settings menu


Field	Description
Inhibited number	Enter the number that cannot be dialled.
Enabled number	Enter the number for which dialling is explicitly permitted.

7.1.4 Priority Numbers

In the **Call Routing->Outgoing Services->Priority Numbers** menu you configure numbers with particular special functions, e. g. emergency functions.

In your system configuration, you can enter numbers that must be accessible in an emergency. If you now dial one of these priority numbers, it is detected by the system and an ISDN B channel is automatically cleared. If the external ISDN B channels are already in use, one of the ISDN B channels is freed up and the calling subscribers hear the busy tone. An ongoing priority call is not interrupted.

7.1.4.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

The **Call Routing->Outgoing Services->Priority Numbers->New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the entry.

Field	Description
Priority Number	Enter the number which can even be dialled if all B channels are occupied. In this case, an external B channel is released for this connection and reassigned for the priority call. An ongoing priority call is not interrupted.

7.2 Automatic Route Selection

In the **Call Routing->Automatic Route Selection** menu, you can set up routes for external calls in addition to configured line occupancy. Here, bundles released for users can be selectively assigned to ongoing calls according to the dialled number, or new providers entered along with their network access prefixes. You then specifically define the routing for individually created zones for every weekday.

7.2.1 General

In the **Call Routing->Automatic Route Selection->General** menu, you enable the ARS - Automatic Route Selection - function and select the desired route level.

The menu **Call Routing->Automatic Route Selection->General** consists of the following fields:

Fields in the Basic Settings menu


Field	Description
ARS	<p>Select whether to enable the ARS performance feature (Automatic Route Selection).</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Routing Stage	<p>Select whether additional routes shall be used if an entered provider or bundle cannot be accessed.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>1 (No Fallback)</i>: If the entered provider or selected bundle is (Call Routing->Automatic Route Selection->Zones &Routing-> Edit/Add -> Mo-Su ->Routing Stage 1) not available, connection setup is terminated. • <i>2</i>: If the entered provider or selected bundle (Call Routing->Automatic Route Selection->Zones &Routing->

Field	Description
	<p>Edit/Add -> Mo-Su ->Routing Stage 1) is not available, there is an attempt to initiate the connection over the additional entered routing variant (Call Routing->Automatic Route Selection->Zones &Routing-> Edit/Add -> Mo-Su ->Routing Stage 2).</p> <ul style="list-style-type: none"> • 3 (default value): If neither of the two entered providers or bundles (Call Routing->Automatic Route Selection->Zones &Routing-> Edit/Add -> Mo-Su ->Routing Stage 1 and Routing Stage 2) is available, dialling occurs via the provider entered as the default for the user (Numbering->Class of Service->Add->Basic Settings->Trunk Line Selection with Line Access Number).

7.2.2 Interfaces / Provider

In the **Call Routing->Automatic Route Selection->Interfaces / Provider** menu, enter the routes or providers along with their network access profiles.

7.2.2.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

The **Call Routing->Automatic Route Selection->Interfaces / Provider->New** menu consists of the following fields:

Fields in the Basic Settings menu


Field	Description
Description	Enter a description for the entry.
Routing Mode	<p>Select how dialling shall be externally routed.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Default</i> (default value): The default procedure provides that when dialling externally, the prefix entered under Call-prefix is placed first. • <i>Route</i>: External dialling is set up via the bundle selected in Route.

Field	Description
Call-prefix	Enter the number to be placed as a prefix when making an external call, e.g. to set up a connection via a call-by-call provider.
Route	Only if Routing Mode = <i>Route</i> Select a bundle via which the external call shall proceed.

7.2.3 Zones & Routing

In the menu **Call Routing**->**Automatic Route Selection**->**Zones & Routing** you define the zones via which dialling shall proceed using specific routes or providers.

Configuration of the routing tables for the defined zones occurs individually for each week-day. For 2 routing tables, routing level 1 and routing level 2 can be created as fallback.

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

7.2.3.1 Numbers

In the **Numbers** area, enter the number or partial number of the zones for which you wish to configure the routing tables.

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the entry.
Zones	Configure the desired external zones which should be dialled via the desired entered provider/routes. Possible values: <ul style="list-style-type: none"> • <i>Number/Partial Number</i>: Enter the number or part of a number identifying a zone. • <i>Name</i>: Enter a name for this zone.

7.2.3.2 Mon - Sun

In the **Mon - Sun** area, select the desired times for each routing level, and the desired route or provider via which outgoing calls shall be routed from the entered time.

Fields in the <Weekday> menu

Field	Description
Routing Stage 1	Configure the switching times for routing level 1. For this, first select the Start Time from which routing shall occur over a specific interface or a specific network provider, and select the latter under Interface / Provider .
Routing Stage 2	Configure the switching times for routing level 2. For this, first select the Start Time from which routing shall occur over a specific interface or a specific network provider, and select the latter under Interface / Provider .

Chapter 8 Applications

Internal telephone performance features of the system are set up under **Applications**.

8.1 Calendar

In the **Applications->Calendar** menu, you can decide whether to make new entries or modifications in the calendar.

Every company has fixed business hours. You can enter these in the system's internal calendar. For example, all calls outside of business hours can be signalled to a exchange or an answering machine. During this period, your employees can perform other tasks, without being interrupted by telephone calls. The individual call options of a team are automatically switched through the calendars.


You wish to modify the external calling authorisations after business hours for specific subscribers. In the system configuration, you can set individually for each user whether the authorisation for external calls is automatically switched. The switch occurs according to the data in the assigned calendar.

You can set up five types of calendars in the system. The "Authorisation Class" and "Night Operation" calendars are intended for central switching and can only be set up once. The "Team Signalling", "Intercom Signalling" and "Redirect to internal/external number" calendars can be set up repeatedly. Several different switching times can be selected for each weekday.

In the configuration, a calendar can be assigned to all performance features for which several options can be defined (e.g. teams) Switching between the individual call options then occurs at the switching times of the assigned calendar.

8.1.1 Calendar

In the menu **Applications->Calendar->Calendar** you can view, modify or copy a previously set calendar as well as create new calendars.

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

8.1.1.1 General

In the **General** area you define the name of the calendar to be created.

The menu **Applications->Calendar->Calendar->General** consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Description	Enter a description for the calendar.
Application	<p>Select the application for which the calendar shall be used.</p> <p>Please note that this field cannot be edited with pre-existing entries. If another application is to be configured, you must create another entry and delete the existing one.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Team Signalling</i> (default value): Here, several calendars can be set up. • <i>Doorline Signalling</i>: Here, several calendars can be set up. • <i>Night Mode</i>: Here, only one calendar can be set up. • <i>Class of Service</i>: Here, only one calendar can be set up. • <i>Rerouting for internal/external Number</i>: Here, several calendars can be set up. • <i>Voice Mail System</i>: Here, several calendars can be set up. • <i>Alarm Input</i>: Here, several calendars can be set up.

8.1.1.2 Mon - Sun

In the **Mon - Sun** area you set up the switching days and times for this calendar.

The **Applications->Calendar->Calendar->Mon** menu consists of the following fields:

Fields in the <Weekday> menu

Field	Description
Switching Points	<p>Enter the desired switching times.</p> <p>For this, under Time, for each weekday select the desired switching points to which switching shall occur from any divergent active switching option in the desired switching options</p>

Field	Description
	<p>selected under Action.</p> <p>Depending on the application, the following switching options are available:</p> <ul style="list-style-type: none"> • <i>Team Signalling</i>: Call option 1 to call option 4 • <i>Doorcom Signalling</i>: Door Intercom call option 1 and door intercom call option 2 • <i>Night Mode</i>: Night operation on and night operation off • <i>Class of Service</i>: Authorisation class by default and authorisation class optional • <i>Rerouting for internal/external Number</i>: Redirect option 1 to redirect option 4
Use settings from	<p>Only if settings have already been performed for a weekday.</p> <p>Select from which weekday the settings should be imported.</p> <p>If you require specific settings for this day, select the option <i>Individual</i>.</p>

8.1.1.3 Exception

In the **Exception** area, select whether holidays shall be taken into account and, if so, how.

The menu **Applications->Calendar->Calendar->Exception** consists of the following fields:

Fields in the Settings holidays menu


Field	Description
Consider public holidays	<p>Select whether appointments entered in the Applications->Calendar->Public Holiday menu shall also be considered in this calendar.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Use settings from	<p>Only if Consider public holidays is enabled.</p>

Field	Description
	<p>Select from which weekday the settings for holidays should be imported. Configure weekdays in menu Applications->Calendar->Calendar->Mo - Su</p> <p>If you require specific settings for holidays, select the option <i>Individual</i>.</p>
Switching Points	<p>Only for Use settings from = <i>Individual</i></p> <p>Enter the desired switching times.</p> <p>For this, under Time, select the desired switching points to which switching shall occur from any divergent active switching option in the desired switching options selected under Action.</p> <p>Depending on the application, the following switching options are available:</p> <ul style="list-style-type: none"> • <i>Team Signalling</i>: Call option 1 to call option 4 • <i>Doorcom Signalling</i>: Door Intercom call option 1 and door intercom call option 2 • <i>Night Mode</i>: Night operation and night operation off • <i>Class of Service</i>: Authorisation class by default and authorisation class optional • <i>Rerouting for internal/external Number</i>: Redirect option 1 to redirect option 4

8.1.2 Public Holiday

In the **Applications->Calendar->Public Holiday** menu, you can enter holidays or any special days for which divergent settings should be made via the calendar. The holiday entries are sorted by date!

8.1.2.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

The menu **Applications->Calendar->Public Holiday->New** consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for a holiday.
Date (DD - MM)	Enter the date with day and month in two-digit form. Incorrect entries, e. g. 31.02 are accepted and saved but not executed by the system.


8.2 Rerouting

In the **Applications->Rerouting** menu, you configure how incoming calls should be handled by default in the system.

8.2.1 Rerouting Functions

In the **Applications->Rerouting->Rerouting Functions** menu you can set up various redirect options for **Immediately**, **On Busy**, **On No Reply** or **On Busy and On No Reply**. You then assign these redirect options to the external connections in the **Numbering->Call Distribution->Incoming Distribution** menu.

8.2.1.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create new redirect options.

The **Applications->Rerouting->Rerouting Functions->New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the redirect function.
Type of Rerouting Function	Select the desired exchange function. Possible values: <ul style="list-style-type: none"> • <i>Immediately</i> (default value) • <i>On Busy</i> • <i>On No Reply</i> • <i>On Busy and On No Reply</i>

Fields in the On Busy Settings menu

Field	Description
Size of Queue	<p>Only for Type of Rerouting Function = <i>On Busy</i> or <i>On Busy and On No Reply</i>.</p> <p>In this field, you can configure the maximum number of subscribers on hold. The queue may include up to 10 subscribers. Additional callers get a "busy" tone.</p> <p>Possible values are 0 (no queue) to 10. The default value is 0.</p>
Take Waiting Calls with	<p>Only for Type of Rerouting Function = <i>On Busy</i> or <i>On Busy and On No Reply</i>.</p> <p>Define what callers on hold shall hear (internal or configured music-on-hold, announcement).</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>MoH Wave 1</i> to <i>MoH Wave 8</i> • <i>MoH internal 1</i> (default value) • <i>MOH internal 2</i> • <i>Off</i>
Max waiting time in the queue	<p>Only for Type of Rerouting Function = <i>On Busy</i> or <i>On Busy and On No Reply</i>.</p> <p>Define maximum time a caller can remain on hold. After expiration of this time, the caller shall be transferred to the defined redirect destination. Leave <i>Endless</i> for an unlimited queue (corresponds to value 0). Disable <i>Endless</i>, to enter the desired value.</p>

Fields in the On No Reply Settings menu

Field	Description
Time for Rerouting on No Reply	<p>Define maximum time a caller can remain on hold if she cannot reach the destination number. After expiration of this time, the caller shall be transferred to the defined redirect destination.</p> <p>The default value is 30 seconds.</p>

Fields in the Further Settings menu

Field	Description
Announcement	<p>Select whether the incoming call shall be redirected to an announcement.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Off</i> (default value): The incoming call is not redirected to an announcement. • <i>MoH Wave 1 to MoH Wave 8</i>
Target Number	<p>Select the internal number to which the incoming call shall be redirected.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>No Number (Disconnect)</i>: The call is terminated, the connection ended. • <i><Extension number></i>: If a destination number is entered, the call is forwarded.
Transfer with	<p>The caller hears the defined announcement or music while her call is being transferred.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Ring tone</i> • <i>MoH Wave 1 to MoH Wave 8</i> • <i>MOH internal 1</i> • <i>MOH internal 2</i> • <i><Wave file></i>

Announcement before query

You have set up a general information call number which customers with various problems or requests ring up. Naturally, no single employee or team can provide information in every subject areas. So the caller would need to be transferred to the individual departments. If you knew beforehand which requests (subject area) a caller had, you could immediately transfer him to the competent department. Thus, your callers don't have to be initially accepted and transferred by an exchange. Every caller decides for him/herself with which employee he/she wishes to be connected.

With the performance feature **Auto Attendant with DISA** calls are automatically accepted by the system. The caller then hears an announcement with information about which

entries are possible during or after the announcement. Once the entry is made, the announcement ends and the caller is transferred to an internal subscriber or team. If the caller provides a false or no entry, he/she is transferred to the defined redirect destination (internal subscriber or team). While being transferred, the caller hears a ring tone or the system's music-on-hold.



Note


DISA - Direct Inward System Access Once a call is received by the system, the caller is automatically transferred after a code number is entered. This code is assigned to an internal number in the system. Entry of a number or code must occur during the announcement. Once the announcement (Wave file) ends, no more entries are accepted. There follows redirect to a defined redirect destination. The performance feature **Auto Attendant with DISA** is an integral part of the system and can accept up to 28 calls simultaneously.

Fields in the Announcement/Auto Attendant Settings menu

Field	Description
Call Switching	<p>Select how incoming calls are to be transferred.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Announcement without DISA</i> (default value): The configured announcement is played. There follows either transfer to the configured internal number, or the connection is interrupted and the caller hears the busy tone. • <i>DISA, dial internal numbers</i>: The caller is prompted to enter an internal number. The call is forwarded to the number. • <i>DISA, dial code numbers</i>: The caller is prompted to enter a code number from 0 to 9. The desired internal numbers are assigned to the codes. The caller is then transferred to the configured internal number.
Number of playbacks	Select how many times the announcement shall be continuously repeated. At conclusion, the caller hears the busy tone.
Auto Attendant with DISA	<p>Only if Call Switching = <i>DISA, dial code numbers</i></p> <p>For ever desired DISA code number, select the desired internal number to which the caller shall be transferred.</p>

8.2.2 Rerouting Applications

In the **Applications->Rerouting->Rerouting Applications** menu, you can configure when which redirect option is to be enabled. You can switch the various options either via calendar or manually.

Choose the  icon to edit existing entries. Select the **New** button to create new redirect applications.

8.2.2.1 General

In the **General** area, you perform basic settings for a redirect application.

The **Applications->Rerouting->Rerouting Applications->New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the redirect application.
Type of Rerouting Application	Select the destination to which an incoming call shall be redirected. Possible values: <ul style="list-style-type: none"> • <i>Trunk Number</i> (default value) • <i>Extension</i> • <i>Global</i>
Switch call signalling	Select how to switch between options Possible values: <ul style="list-style-type: none"> • <i>No calendar, only manually</i> • <i><Calendar></i>

8.2.2.2 Variant 1 - 4

In the **Variant** area, you configure the redirect options. You can define up to 4 options.

The menu **Applications->Rerouting->Rerouting Applications->Variant** consists of the

following fields:

Fields in the Basic Settings menu.

Field	Description
Assignment	Choose the redirect function to which you wish to assign the selected option.

8.3 Voice Applications

In the **Applications->Voice Applications** menu, you configure you system's wave files.

A professional greeting, especially on the telephone, constitutes a company's visiting card. Voice applications make this possible for every business. Indeed, while being transferred, the caller receives information that's individually tailored, e. g. according to department, or is simply entertained with pleasant music-on-hold.

You wish to employ special music as music-on-hold, or specific announcements for your clients. You can load your self-produced Wave files to the system.

User-specific voice and music files can be saved in the system. Storage space for 2 MoH melodies is available in the system basic settings. The available storage space can be extended with an SD card. The length of the language and music files that can be saved is based upon the SD card used. Voice and music data is saved in Wave format.

The following voice applications can be defined in the system:

- Announcement before query
- Announcement without query/Infobox
- Wake-up call
- Music on hold

You can find additional information on function, configuration and operation in the description of the individual performance features.

Basic settings of voice applications

The voice applications can be assigned to individual performance features in two different ways.

Every user employing a voice application with this connection always hears the corresponding voice announcement or music from the start. A newly-arrived user hears the voice announcement or music from the start. The number of users who can simultaneously use such a voice application is limited to 28.

Please note that externally played music or voice application music are free of third-party copyrights (GEMA free). Files in other formats must be converted into the company-specific Wave format before being saved in the system.





Note



Please note that Wave files must be available in the following format:

- Bit rate: 128 kbps
- Sampling size: 16 bits
- Channels 1 (mono)
- Sampling rate: 8 kHz
- Audio format: PCM

8.3.1 Wave Files

In the **Applications->Voice Applications->Wave Files** menu, you can configure your announcement/melody files and volume. You also have the option to play back voicemail messages or download these to your PC. To save a message, click on the  icon. The download dialog then opens. To listen to a message, click on the .

8.3.1.1 Edit

Choose the  icon to edit existing entries. Select  to change the entry.

MoH internal 1 and *MoH internal 2* are files specified in the system and can thus not be deleted.

The **Applications->Voice Applications->Wave Files->Edit** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the Wave file.
Select file	Click Browse... and select the Wave file to be loaded into the system through the Explorer window.
Volume	Select the volume at which the Wave file shall be played by default. Select <i>0</i> to play the file at a predefined default volume.

Field	Description
	<p>You can gradually diminish the volume using the negative values, and increase it with the positive ones.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • -5 • -4 • -3 • -2 • -1 • 0 (default value) • +1 • +2 • +3

8.4 System Phonebook

In the **Applications->System Phonebook** menu, you can enter and administer numbers in the system phone book.

The employees in your company must phone many customers. This is where the system phone book comes in. You need not enter the customer's number but can extract the name via the system telephone display, and dial. Customer names and telephone numbers can be centrally administered by an employee. If a customer whose number has been entered in the phone book calls, his/her name appears in the system telephone display. The system features an integrated phone book in which you can save phone book entries of up to 24-digits (numbers) and up to 20-character names (text).

When creating a telephone book entry, a **Speed Dial Number** code is assigned to each entry. Authorised telephones can initiate speed dial from the phone book via these speed dial numbers.

System telephones

System telephones can dial from the system phone book via a special menu. To search for a telephone entry, enter the first letters (max. 8) of the desired name and confirm the entry. The system always provides 8 phone book entries, which you can view successively. Select the desired entry and confirm with **OK**. You must now begin to dial within 5 seconds. The system telephone redialling list displays the name of the dialled subscriber instead of her number. If a system telephone receives a call whose number and name are

saved in the system phone book, the caller's name is indicated in the system telephone display.



Note

The user's other numbers (**Mobile Number** and **Home Number**) are only displayed in the system telephone phone book menu. They are not displayed in the **System Phonebook** menu of the user interface. Entries in the system telephone phone book menu with the (M) mark refer to an entered **Mobile Number** of a user; those with the (H) mark to **Home Number**.




Note

hybird support LDAP (Lightweight Directory Access Protocol) for providing the entries of the system phonebook to other devices. Name, Number as well as mobile and private numbers can be transferred this way.

8.4.1 Entries

In the **Applications->System Phonebook->Entries** menu, all configured telephone book entries are displayed with the corresponding speeddial index. The entries in the **Description** column are sorted alphabetically. Click the column title of any column to sort entries in ascending or descending order.

8.4.1.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

The menu **Applications->System Phonebook->Entries->New** consists of the following fields:

Fields in the Phonebook Entry menu

Field	Description
Description	Enter a description for the entry. Subsequent sorting in the phone book follows the initial letters of the entry.
Phone Number	Enter the telephone number (internal or external).
Speed Dial Number	Enter a speed dial code. If a speed dial code is entered, counting is automatic; i.e. speed dial is automatically assigned.

Field	Description
	Numbers from 0 to 999 are possible.
Call Through	<p>Select whether the telephone number for the Call Through function has been activated. If a telephone number is approved for this, and the caller uses this number for the Call Through functions, the caller's authorisation to use the function is checked against the phonebook record.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

8.4.2 Import / Export

You can import and export phone book data in the **Applications->System Phonebook->Import / Export** menu. You can import data exported from Microsoft Outlook, for example. The phone book data stored in your device is exported to a text file.

The **Applications->System Phonebook->Import / Export** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Action	<p>Select the desired action.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <i>Export</i> (default value): You can export the names saved in Applications->System Phonebook->Entries into a text file (specifying phone number, speed dial, call through). <i>Import</i>: You can import a text file in the following format: The file imported must consist of individual rows in the following format: name, phone number, speed dial, call through (1 = enabled, 2 = disabled). <p>Example:</p> <p>Name,Phone Number,Speeddial Number,Call Through</p> <p>Hans,123456,1,1</p> <p>Klaus,234567,2,2</p>

Field	Description
	Max,345678,3,1
Separator	<p>Only for Action = <i>Import</i> and Default File Format not enabled</p> <p>Enter the separator type in the import file.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Comma</i> (default value) • <i>Semicolon</i> • <i>Space</i> • <i>Tabulator</i>
Select file	Only for Action = <i>Import</i> select the file to be imported.

You also have the option to import a CSV file.

If the data record consists of more than one column, you have the option to generate two address book entries from the data record for the import (e.g. one for business and one private entry.) To do this, specify the data to be used as the name and phone number in an additional import step. If you want to generate only one phonebook entry, select the blank option in all selection fields for the second record **Phonebook Import**.

The **Applications->System Phonebook->Import / Export->Phonebook Import** menu consists of the following fields:

Fields in the Phonebook Import menu

Field	Description
Phone Number	Select which data is to be used from a data record as the phonenummer.
Name	Select which columns are to be used from a data record as the name. You have the option to use two elements here (e.g. fore-name and surname). The middle input field can be used to place a character string between the two elements here. The default separator used is a comma.

Speed dial is automatically assigned. By default, call through is disabled.

8.4.3 General

In the menu **Applications->System Phonebook->General** you define the user name and password for system phone book administration. In the phone book area, the administrator can view and modify the phone book, as well as import and export data.

The **Applications->System Phonebook->General** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Web Access Username	Enter a user name for the system telephone book administrator.
Web Access Password	Enter a password for the system telephone book administrator.
Delete Phonebook	If you wish to remove the existing system phone book with all of its entries, enable the option Delete . You will then be asked for confirmation Do you really want to delete all entries of the phonebook? . Confirm your entry by clicking OK .

8.5 Call Data Records

In the **Applications->Call Data Records** menu, you configure the recording of incoming and outgoing calls.

The capture of call data records provides an overview of the telephone usage in your company.

All external calls can be saved in the device in the form of call data records. These data records contain important information about the individual calls.

You must enable recording of connection data in the **Numbering->User Settings->Class of Services->Applications** menu. The function is not activated in the ex works state.

8.5.1 Outgoing

The **Applications->Call Data Records->Outgoing** menu contains information that permits the monitoring of outgoing activities.

The **Applications->Call Data Records->Outgoing** menu consists of the following fields:

Fields in the Outgoing menu

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Duration	Displays the duration of the connection.
User	Displays the user who called.
Int. No.	Displays the user's internal number.
Called Number	Displays the dialled number.
Project Code	Displays the call project number, if any.
Interface	Displays the interface over which the external connection was routed.
Costs	Displays the connection charge, but only if the provider transmits the corresponding data.

8.5.2 Incoming

The **Applications->Call Data Records->Incoming** menu contains information that permits the monitoring of incoming activities.

The **Applications->Call Data Records->Incoming** menu consists of the following fields:

Fields in the Incoming menu

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Duration	Displays the duration of the connection.
User	Displays the user who was called.
Int. No.	Displays the user's internal number.

Field	Description
External Number	Displays the caller's number.
Project Code	Displays the call project number, if any.
Interface	Displays the interface over which the connection from outside was routed.

8.5.3 General

In the **Applications->Call Data Records->General** menu, you can define how connection data are saved in the system.

The **Applications->Call Data Records->General** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Web Access User-name	Enter a user name for the call data administrator.
Web Access Password	Enter a password for the call data administrator.
Save outgoing calls	Select which outgoing connections should be saved. Possible values: <ul style="list-style-type: none"> • <i>None</i> (default value) • <i>All</i> • <i>With Project Code only</i>
Save incoming calls	Select which incoming connections should be saved. Possible values: <ul style="list-style-type: none"> • <i>None</i> (default value) • <i>All</i> • <i>With Project Code only</i>
Privacy Number Truncation	Select whether to save the number in abbreviated form. If, for data privacy reasons, the number is to be only partially

Field	Description
	<p>displayed, you can select the number of positions not to be displayed here. For Outgoing Calls and for Incoming Calls you can separately enter the number of hidden digits. The hiding of digits occurs from right to left.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>No</i> (default value) • <i>All</i> • <i>1 to 9</i>
Transfer call data records via Serial 2	<p>Select whether to export call data records over the serial interface (Serial 2) after each call which enables you to connect an external charge metering software solution (hotel application).</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

Fields in the Actions menu

Field	Description
Export call data records	If you wish to save the current connection data record in an external file, click Export and save the file under the desired storage location and file name.
Delete call data records	If you wish to delete the current connection data record from the system storage, click Delete .

8.6 Mini Call Center

The mini call centre is an integrated call centre solution for up to 16 agents. It provides the ideal solution for small groups with high dynamic telecommunication volumes (e. g. insides sales, support, order acceptance/processing, customer service). Here, a specific solution with its own administrator has been integrated. The mini call centre is characterised by:

- Flexible allocation of agents and lines
- Dynamic adaptation according to call volume
- Call allocation with off-time for the agent
- Statistical data for agents and lines.

8.6.1 Status

In the **Applications->Mini Call Center->Status** menu, you can view the current status of lines and logged-in agents in a block, along with the subscribers assigned to lines.


The menu **Applications->Mini Call Center->Status** consists of the following fields:

Values in the Status list

Field	Description
View	View allows you to select which call centre to display.
Line	Displays the mini call centre line.
Agents assigned	Displays the number of agents assigned to this line.
Agents logged on	Displays the number of agents logged-in on this line.
Agents in Wrap-up	Displays the number of agents in post-processing time.
Active Calls	Displays the number of active connections.
Waiting Calls	Displays the number of waiting incoming calls.
Answered of Calls Today	Displays the current number of accepted calls for this day.
Lost Calls Today	Displays the current number of missed calls for this day.

8.6.2 Lines

In the **Applications->Mini Call Center->Lines** menu, lines are assigned to external and internal numbers, and the name of the call centre to which the line belongs is displayed.

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

8.6.2.1 General

In the **General** area, you perform basic settings for a line.

The menu **Applications->Mini Call Center->Lines->General** consists of the following

fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the line.
External Number	Select a number configured as mini call centre for the external connection of this call centre line.
Internal Number	Enter the desired internal number for this line.
Call Center Description	Select <i>New</i> and enter a name for the new mini call centre. Or select the name of a mini call centre which has already been generated.

Fields in the Further Settings menu

Field	Description
Switch call signalling	Select whether the call options for this line shall be switched over a configured calendar and, if so, over which. Possible values: <ul style="list-style-type: none"> • <i>No calendar, only manually</i> • <i><Calendar></i>
Active Variant	Select which call option shall be enabled by default after configuration for this line.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Team Speed Timer	Enter the time after which call forwarding to the next free agent assigned to this line shall occur.

8.6.2.2 Variant 1 - 4

In the area **Variant**, you set up call options for the mini call centre.

The menu **Applications->Mini Call Center->Lines->Variant** consists of the following

fields:

Fields in the Settings menu

Field	Description
Automatic Call Pick-up with	<p>Select whether an incoming call shall be automatically accepted and, if so, with which announcement or melody.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>Select the Wave file to be used for the call acceptance. All preset and additionally-loaded Wave files in the system can be selected.</p>

Fields in the Rerouting Functions menu

Field	Description
Rerouting on no response	<p>Select whether and, if so, with which option an incoming call shall be redirected after the entered time.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i>: There shall be no redirect on no-reply. • <i><Team></i>: The incoming call is forwarded to the selected team after the time specified in Time until rerouting.
Further Rerouting	<p>Select additional redirect functions. You must first configure these in Applications->Rerouting->Rerouting Functions. Then, the following values may be selected:</p> <ul style="list-style-type: none"> • <i>Off</i>: No additional redirect functions. • <i>Immediately</i>: Immediately transfers the call according to a configured redirect function . • <i>On Busy</i>: Transfers the call according to a configured redirect function on engaged.
Rerouting Function	<p>Only for Further Rerouting = <i>Immediately</i> or Further Rerouting = <i>On Busy</i></p> <p>Select a configured redirect option for immediate redirect, or on busy.</p>
Busy when	<p>Only for Further Rerouting = <i>On Busy</i></p>

Field	Description
	Select from how many busy agents the lines shall be considered busy.

8.6.2.3 Log on / Log off

In the **Log on / Log off** area, select which of the assigned agents shall be logged into the line.

The menu **Applications->Mini Call Center->Lines->Log on / Log off** consists of the following fields:


Fields in the Log on / Log off menu

Field	Description
Numbers	Displays the internal number and description of the assigned agent.
Status	Select whether the agent is logged into the line. The agent is logged in by selecting <i>Logged on</i> .

8.6.3 Agents

In the **Applications->Mini Call Center->Agents** menu, lines are assigned to agents. An agent can operate one or more mini call centre lines.

8.6.3.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

The menu **Applications->Mini Call Center->Agents->New** consists of the following fields:

Fields in the Basic Settings menu

Field	Description
User	Select the configured user who shall serve as a call centre agent. You configure required users in the Numbering->User Settings->User menu.
Internal Number	Select the user's internal number to be used for the call centre.

Fields in the Assigned Lines menu

Field	Description
Select lines	Select the lines for which the agent shall be responsible. The name of the corresponding call centre is displayed again when lines are selected in order to improve the overview. Under Assign select whether the entry should be enabled.

Fields in the Wrap-up Settings menu

Field	Description
Wrap-up Time	Enter the time available to this agent for post-processing after concluding a call. No further call can be assigned to this agent during this period. The agent has the option of temporarily extending the period with a telephone procedure.

8.6.4 General

In the **Applications->Mini Call Center->General** menu, you can set up an HTML web interface access for the mini call centre manager. The latter can then monitor the status of lines and agents, and modify the settings for lines and agents.

The **Applications->Mini Call Center->General** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Web Access User-name	Enter a user name for the mini call centre administrator. When a user logs into the user interface under this name, he/she has access to the user interface with selected parameters for administration of the call centre.
Web Access Password	Enter a password for the mini call centre administrator.

8.7 Doorcom Units

You can connect a door intercom as an intercom adapter to an analogue connection of your system.

If a door intercom adapter is connected to your system, you can speak with a visitor at the door from every authorised telephone. You can assign particular telephones to each ring

button. These phones then ring if the ring button is pressed. On analogue telephones, the signal on the telephone matches the intercom call. In place of the internal telephones, an external telephone can also be configured as the call destination for the ring button. Your door intercom can have up to 4 ring buttons. The door opener can be pressed during an intercom call. It is not possible activate the door opener if an intercom call is not taking place.




Note

All functions of the door intercom (intercom adapter) are controlled via the code numbers indicated in the intercom user's manual. The system does not support the intercom with specific codes.

8.7.1 Doorcom Units

In the **Applications->Doorcom Units->Doorcom Units** menu, select the internal analogue connection (FXS) to which an intercom adapter shall be connected. Then dial the internal number for the connection, and optionally the codes for call acceptance.

8.7.1.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to create new entries.

The menu **Applications->Doorcom Units->Doorcom Units->New** consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Interface	Select the interface to which an intercom adapter shall be connected. All free FXS interfaces are available.
Internal Number	Select the configured internal number to be assigned to the intercom adapter. The number is created in the Numbering->User Settings->User menu.
Code for Doorcom Call Acceptance	Pressing a bell button on the intercom sets off a call in the system. To establish a connection between a called subscriber and the intercom adapter, that subscriber must pick up the receiver and dial the code number for call acceptance. Enter this code for call acceptance. If a subscriber accepts a call from the

Field	Description
	intercom adapter, the PABX automatically dials the code number required to set up the connection. The subscriber need not make any more entries.

8.7.2 Doorcom Signalling

In the **Applications->Doorcom Units->Doorcom Signalling** you configure the signalling variant for call acceptance via a intercom adapter. Two intercom call options are available.

The code number for the bell button is the number the intercom adapter dials into the system when the bell button is pressed. You can perform an internal call allocation for each bell button. Please note that guidelines for connecting the intercom adapter depend on the respective manufacturer. For this, read the operating instructions provided by the manufacturer of the intercom adapter.

8.7.2.1 General

In the **General** area you set up the basic features of intercom signalling.

The menu **Applications->Doorcom Units->Doorcom Signalling->General** consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Select one of the configured intercom settings previously created in the Applications->Doorcom Units->Doorcom Units menu.
Bell ID	Enter an unambiguous four-digit code for the bell. Pressing a bell button on the intercom adapter initiates a call to the terminals entered in the assigned intercom call option.
Bell Name	Enter a name for the bell.
Switch signalling	Select whether the intercom call options for this bell shall be switched over a configured calendar and, if so, over which. For every ring, you can create up to two intercom call variants in the Applications->Doorcom Units->Doorcom Signalling->New->Variant menu. Possible values:

Field	Description
	<ul style="list-style-type: none"> • <i>No calendar, only manually</i> • <i><Calendar></i>
Active Doorcom Variant	Select which intercom call option shall be enabled by default for this bell after configuration.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Call Signalisation Timer	Enter the time in seconds for which the door intercom call shall be signalled. The default value is 40 seconds.
Team Speed Timer	Here, enter the Team Speed Timer following which call forwarding after time shall be performed. The default value is 15 seconds.
Simultaneous on no response	It is possible for all numbers assigned to this door intercom signalling to be called simultaneously after a specified time. The default value is 60 seconds.

8.7.2.2 Doorcom Signalling Variant 1 and 2

In the **Doorcom Signalling Variant** area, you configure both intercom call options for this signalling profile.

The **Applications->Doorcom Units->Doorcom Signalling->Intercom call variant** consists of the following fields:

Fields in the Basic Settings menu.


Field	Description
Assignment	Select where pressing of the bell button shall be signalled. Possible values: <ul style="list-style-type: none"> • <i>Internal</i>: Signalling occurs on an internal number. • <i>External</i>: Signalling occurs to an external number.
Internal Assignment	Select the internal numbers on which pressing of the door bell

Field	Description
	shall be signalled. With Add you add an internal number.
External Assignment	Enter the external telephone number to which pressing the door bell shall be signalled.
Signalling	<p>You can call the internal number with a broadcast call.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Simultaneous</i> (default value): All assigned terminals are called simultaneously. If a telephone is busy, call waiting can be used. • <i>Linear</i>: All assigned terminals are called in the sequence of their entry in configuration. If a terminal is engaged, the next free terminal is called. The call is signalled ca. 15 seconds per subscriber. The period can be set between 1 and 99 seconds (per bell) in the configuration. If subscribers are on the phone or logged out, there is not forwarding time for these. • <i>Rotating</i>: This call is a special case of the linear call. After all terminals are called, call signalling begins again with the first entered terminal. The call is signalled until the caller replaces the receiver or the call is ended by the intercom adapter (after ca. 2 minutes). • <i>Adding</i>: The terminals are called in the sequence of their entry in the configuration subscriber list. Every terminal that has already been called is called again, until all entered terminals are called. In the configuration, you can define when each next terminal is called. • <i>Linear, Simultaneous on No Reply</i>: You have set linear for the door intercom call. After the defined time has run out, you can also set in the configuration that all team subscribers are then called in parallel (simultaneously). • <i>Rotating, Simultaneous on No Reply</i>: You have set rotating for the door intercom call. After the defined time has run out, you can also set in the configuration that all intercom subscribers are then called in parallel (simultaneously).

8.8 Alarm Calls

The hybrid products' FXS interface can be configured as an alarm input. E. g. an alarm button can be connected to one of these interfaces. When the button is pressed, an alarm call is triggered to either up to eight internal numbers or one of two external numbers. If necessary, one of the switch contacts can be activated during an alarm call. The function can, optionally, be switched on using a calendar or you can switch between the two possible signalling variants.

8.8.1 Alarm Calls

Choose the  icon to edit existing entries. Select the **New** button to create new alarm inputs.

8.8.1.1 General

In the **General** area you set up the alarm inputs' basic features.

The **Applications->Alarm Calls->Alarm Calls->General** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Status	<p>Enable or disable the alarm input function.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Description	Enter a unique name for the alarm.
Interface	Select the interface to be used for alarm.
Internal Number	Select an internal number to be used for the alarm.
Switch signalling	<p>Specify how the alarm that has been set up is to be switched on.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>No calendar, only manually</i>: Manual switch is enabled. • <i><calendar entry></i>: Select one of the calendar entries that

Field	Description
	has been configured for the alarm.
Active Variant	Select the call options that are to be enabled. You can configure the options as soon as you have confirmed the entry in the General tab with OK .

The menu **Advanced Settings** consists of the following fields:

Fields in the menu **Advanced Settings**

Field	Description
Alarm Signalling Period	Enter the length of time for which an alarm is to be signalled, in seconds. The default value is <i>30</i> seconds.
Repeat after	Specify the time between the alarm repeats, in seconds. A value of between <i>1</i> and <i>600</i> seconds is possible. The default value is <i>10</i> seconds. Call repeats are not possible via a FXO interface.
Number of repeats	Specify the number of repeats if the alarm is not taken. A value of between 1 and 10 repeats is possible. The default value is <i>2</i> . Call repeats are not possible via a FXO interface.
External Connection Timer	Specify the maximum duration of an external call once it has been accepted (in seconds). A value of between <i>1</i> and <i>600</i> seconds is possible. The default value is <i>60</i> seconds.
Info Message (UUS1)	Optionally, a message (max. 32 characters) can be sent to ISDN terminals.
Relay Contact	If a relay is to be switched on during the alarm: Select the relay that is to be used. Configuration of the Relay is done in the menu Physical Interfaces->Relay .
Wave-File	Select whether and which saved WAV file is to be played when the alarm call is taken.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Off</i> (default value): A caller on hold shall hear no music-on-hold. • <i><WAV file></i>: The subscriber called will hear the selected WAV file.
Number of playbacks	<p>Select how many times in a row the announcement is to be played.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Endlessly</i> (default value) • <i>1 to 10</i>

8.8.1.2 Variant 1 and 2

You can configure two versions of the alarm call. One version will normally use the option to call internal extensions, while the other will use the option to call external subscribers.

Fields in the menu Basic Settings

Field	Description
Assignment	<p>You can assign up to eight internal numbers or two external numbers to each alarm. Define whether an alarm's calls are to be signalled to the internal or external subscribers.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>External</i>: The external number that was entered is called. Alternatively, two external numbers can be called for an alarm. • <i>Internal</i> (default value): The subscribers assigned to the selected numbers are called based on the signalling defined. For one alarm, eight internal subscribers can be called simultaneously.
First External Number	<p>Only for Assignment = <i>External</i> Enter the first number of the external subscriber.</p>
Second External Number	<p>Only for Assignment = <i>External</i> Enter the second number of the external subscriber.</p>

Field	Description
Internal Assignment	<p>Only for Assignment = <i>Internal</i> Select the internal subscribers.</p> <p>Use Add to add more internal numbers.</p>

8.9 Voice Mail System

The voicemail system is an intelligent answering machine for those who use your **hybird**. An individual voicemail box can be configured for each extension. All subscribers can hear, save or delete their messages from any telephone using a personal PIN code.

Subscribers can have themselves informed of incoming e-mails. Recorded messages can be automatically transferred to any e-mail address.

General settings of the voicemail system are performed on your **hybird**. Operation of the individual voicemail boxes occurs via telephone.

Every subscriber can use her individual voicemail box by transferring calls to her voicemail box.



Note

If you wish to use a voicemail box, you'll need an installed SD card. You may need load the required folder structure with the announcement texts on the SD card. Choose in the **Maintenance->Software & Configuration** menu the option *Import Voice Mail Wave Files*.




Caution

Do not remove the SD card during any read or write access to avoid losing data or damaging the card. Watch the relevant LED on the top of the device: it will flicker during any read or write access.


8.9.1 Voice Mail Boxes

In the **Applications->Voice Mail System->Voice Mail Boxes** menu, a list of the individual voicemail boxes for specific subscribers is displayed, insofar as voicemail boxes have been configured.

Values in the list Voice Mail Boxes

Field	Description
Internal Number	Displays the number of the individual subscriber for which the voicemail box is configured.
User	Displays the name of the individual subscriber for which the voicemail box is configured.
Language	Displays the language of the announcement text on the voicemail box. <i>Default</i> means that the centrally-set language, defined for the entire voicemail system in the Applications->Voice Mail System ->General menu, is used.
Notification	Indicates whether the subscriber is informed of missed calls.
Active Variant	Indicates the current status of the voicemail box (<i>In the Office</i> or <i>Out of Office</i>).
License Allocation	Indicates whether a licence is currently assigned to a voicemail box.
	<div style="border: 1px solid gray; padding: 10px;"> <p> Note</p> <p>The number of configured voicemail boxes may exceed the number of existing licences. However, you must make sure that the number of currently used voicemail boxes is covered by the number of licences.</p> </div>


8.9.1.1 Edit or New


Choose the  icon to edit existing entries. Select the **New** button to create new entries.

The menu **Applications->Voice Mail System ->Voice Mail Boxes ->New** consists of the following fields:

Fields in the menu Basic Setup

Field	Description
Internal Number	Select the internal number of the subscriber for which you wish to set up a voicemail box. You may choose among the num-

Field	Description
	bers configured in the Numbering->User Settings->User menu.
Voice Mail Language	<p>Select the desired language for the voicemail box announcements.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Deutsch</i>: The voicemail box uses German texts. • <i>Dutch</i>: The voicemail box uses Dutch texts. • <i>English</i>: The voicemail box uses English texts. • <i>Italian</i>: The voicemail box uses Italian texts. • <i>French</i>: The voicemail box uses French texts. • <i>Default</i> (default value): The voicemail box uses the language centrally defined for the entire voicemail system in the Applications->Voice Mail->General menu. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>Note</p> <p>You'll only require a setting that departs from <i>Default</i> if you wish to operate voicemail boxes with various languages within your voicemail system.</p> </div>
E-Mail Address (from User Settings)	Here is displayed the user e-mail address to which a notification shall be sent if a message has been left on the voicemail box. The e-mail address is saved in the Numbering->User Settings->User->Basic Settings menu.
E-Mail Notification	<p>Once a message has been left on the voicemail box, the subscriber can be notified.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i> (default value): The subscriber is not notified. • <i>E-Mail</i>: The subscriber is informed of a present message via e-mail. • <i>E-Mail with Attachment</i>: Once a caller has left a message, the subscriber receives an e-mail with a recording of the message in the attachment.

Field	Description
	<ul style="list-style-type: none"> <i>User defined</i>: If the administrator activates the <i>User defined</i> function, the e-mail alert settings can be changed by the user in the User Access. If the administrator sets a different value, a block is placed on changes from the user. <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;">  <p>Note</p> <p>Once a subscriber has received notification of a new message in an e-mail, the Status of the notification is changed according to the settings in the User Access. You can configure the status behaviour in the User Access->Voice Mail System->Settings menu under E-Mail forwarding behavior.</p> </div>
Max Recording Time	Enter the maximum recording time per message. The possible values are 5 to 300 seconds, the default value is 180 seconds.
Calendar for status "Out of Office"	<p>When the subscriber is out, the voicemail box can be switched over a calendar.</p> <p>If a calendar is to be used, it needs to be configured with the setting Application = <i>Voice Mail System</i> in the menu Applications->Calendar.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <i>No calendar, only manually</i> (default value): The subscriber can manually switch the voicemail box on and off. <Calendar>: Using the selected calendar, the voicemail box can be switched on or off at the times defined there.

Fields in the menu User Settings

Field	Description
Status of Mail Box Owner	<p>Define in which mode the mailbox shall be used when starting the voicemail system.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <i>In the Office</i> (default value): Select this setting if the subscriber is in the office when the voicemail system is started.

Field	Description
	<ul style="list-style-type: none"> • <i>Out of Office</i>: Select this setting if the subscriber is out of office when the voicemail system is started.
Check PIN	<p>Select whether the currently configured voicemail box should be protected with a PIN.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>You can change the PIN for the personal voice box in the Numbering->User Settings->Users->Authorizations under PIN for Phone Access.</p>
Mode for status "In the Office"	<p>The voicemail box can be operated with two different settings during office hours.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Announcement and Record</i> (default value): A caller hears an announcement and can leave a message. • <i>Announcement only</i>: A caller hears an announcement, but cannot leave a message.
Mode for status "Out of Office"	<p>The voicemail box can be operated with two different settings outside of office hours.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Announcement only</i> (default value): A caller hears an announcement, but cannot leave a message. • <i>Announcement and Record</i>: A caller hears an announcement and can leave a message.

8.9.2 Status

In the **Applications->Voice Mail->Status** menu, the status of the individual voicemail boxes for specific subscribers is indicated. You can see how many calls have gone into which voicemail box, and how many "old" calls are already present.

Values in the System Messages list

Field	Description
Internal Number	Displays the number of the individual subscriber for which the voicemail box is configured.
User	Displays the name of the individual subscriber for which the voicemail box is configured.
New Calls	Displays the calls which have not yet been listened to by the subscriber.
Old Calls	Displays the calls which have already been listened to or stored by the subscriber.

8.9.3 General

In this menu, you can configure the general settings for your voicemail system.

The menu **Applications->Voice Mail->General** consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Voice Mail System	Select whether to activate your voicemail system. The function is enabled with <i>Enabled</i> . The function is enabled by default.
Description	Only for Voice Mail System enabled. Enter a description for your voicemail system. This description is displayed on the telephone when a call goes in to the voice mail system. The default value is <i>Voice Mail</i> .
Internal Number	Only for Voice Mail System enabled. Enter the internal number under which to access your voicemail system. The default value is <i>50</i> .
Language	Select the language for the entire voicemail system.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Deutsch</i> (default value) • <i>Dutch</i> • <i>English</i> • <i>Italian</i> • <i>French</i> <p>Diverging from the language set here, a language can be individually set for each voice mail box in the Applications->Voice Mail->Voice Mail Boxes->New menu.</p>

Fields in the menu Mail Settings

Field	Description
SMTP Server	Enter the address (IP address or valid DNS name) of the e-mail server to be used for sending the e-mails.
SMTP Server Port	Enter the port to be used for sending e-mails. The default value is <i>25</i> .
Return Address	Enter any address to be used as sender when sending e-mails. This address merely serves to identify e-mails in the inbox.
SMTP User Name	Enter the user name for the SMTP server.
SMTP Password	Enter the password for the SMTP server user.

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Lifetime	<p>Voicemail messages are deleted after an adjustable period of time.</p> <p>Possible values are <i>10</i> to <i>60</i> days. The default value is <i>60</i>.</p>

Chapter 9 LAN


In this menu, you configure the addresses in your LAN and can structure your local network using VLANs.

9.1 IP Configuration

In this menu, you can edit the IP configuration of the LAN and Ethernet interfaces of your device.

9.1.1 Interfaces

The existing IP interfaces are listed in the **LAN->IP Configuration->Interfaces** menu. You can edit the IP configuration of the interfaces or create virtual interfaces for special applications. Here is a list of all of the interfaces (logical Ethernet interfaces and others created in the subsystems) configured in the **System Management->Interface Mode / Bridge Groups->Interfaces** menu.

Use the  to edit the settings of an existing interface (bridge groups, Ethernet interfaces in routing mode).

You can use the **New** button to create virtual interfaces. However, this is only needed in special applications (e.g. BRRP).

Depending on the option selected, different fields and options are available. All the configuration options are listed below.



Note

Please note:

If your device has obtained an IP address dynamically from a DHCP server operated in your network for the basic configuration, the fallback IP address is deleted automatically and your device will no longer function over this address.


However, if you have set up a connection to the device over the fallback IP address or have assigned an IP address with the **Dime Manager** in the basic configuration, you will only be able to access your device over this IP address. The device will no longer obtain an IP configuration dynamically over DHCP.

Example of subnets

If your device is connected to a LAN that consists of two subnets, you should enter a second **IP Address / Netmask**.

The first subnet has two hosts with the IP addresses 192.168.42.1 and 192.168.42.2, for example, and the second subnet has two hosts with the IP addresses 192.168.46.1 and 192.168.46.2. To be able to exchange data packets with the first subnet, your device uses the IP address 192.168.42.3, for example, and 192.168.46.3 for the second subnet. The netmasks for both subnets must also be indicated.

9.1.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create virtual interfaces.

The **LAN->IP Configuration->Interfaces->/New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Based on Ethernet Interface	<p>This field is only displayed if you are editing a virtual routing interface.</p> <p>Select the Ethernet interface for which the virtual interface is to be configured.</p>
Address Mode	<p>Select how an IP address is assigned to the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Static</i> (default value): The interface is assigned a static IP address in IP Address / Netmask. • <i>DHCP</i>: An IP address is assigned to the interface dynamically via DHCP.
IP Address / Netmask	<p>Only for Address Mode = Static</p> <p>With Add, add a new address entry, enter the IP Address and the corresponding Netmask of the virtual interface.</p>
Interface Mode	<p>Only for physical interfaces in routing mode.</p> <p>Select the configuration mode of the interface.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Untagged</i> (default value): The interface is not assigned for a specific purpose. • <i>Tagged (VLAN)</i>: This option only applies for routing interfaces. <p>You use this option to assign the interface to a VLAN. This is done using the VLAN ID, which is displayed in this mode and can be configured. The definition of a MAC address in MAC Address is optional in this module.</p>
MAC Address	<p>Only with virtual interfaces and only for Interface Mode = <i>Untagged</i></p> <p>Enter the MAC address associated with the interface. For virtual interfaces, you can use the MAC address of the physical interface under which the virtual interface was created, but this is not necessary. You can also allocate a virtual MAC address. The first 6 characters of the MAC are preset (but can be changed).</p>
VLAN ID	<p>Only for Interface Mode = <i>Tagged (VLAN)</i></p> <p>This option only applies for routing interfaces. Assign the interface to a VLAN by entering the VLAN ID of the relevant VLAN.</p> <p>Possible values are 1 (default value) to 4094.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
DHCP MAC Address	<p>Only for Address Mode = <i>DHCP</i></p> <p>If Use built-in is activated (default setting), the hardware MAC address of the Ethernet interface is used. In the case of physical interfaces, the current MAC address is entered by default.</p> <p>If you disable Use built-in, you enter a MAC address for the virtual interface, e.g. <i>00:e1:f9:06:bf:03</i>.</p> <p>Some providers use hardware-independent MAC addresses to</p>

Field	Description
	allocate their clients IP addresses dynamically. If your provider has assigned you a MAC address, enter this here.
DHCP Hostname	<p>Only for Address Mode = <i>DHCP</i></p> <p>Enter the host name requested by the provider. The maximum length of the entry is 45 characters.</p>
DHCP Broadcast Flag	<p>Only for Address Mode = <i>DHCP</i></p> <p>Choose whether or not the BROADCAST bit is set in the DHCP requests for your device. Some DHCP servers that assign IP addresses by UNICAST do not respond to DHCP requests with the set BROADCAST bit. In this case, it is necessary to send DHCP requests in which this bit is not set. In this case, disable this option.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Proxy ARP	<p>Select whether your device is to respond to ARP requests from its own LAN on behalf of defined remote terminals.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
TCP-MSS Clamping	<p>Select whether your device is to apply MSS Clamping. To prevent IP packets fragmenting, the MSS (Maximum Segment Size) is automatically decreased by the device to the value set here.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default. Once enabled, the default value <i>1350</i> is entered in the input field.</p>

9.2 VLAN

By implementing VLAN segmentation in accordance with 802.1Q, you can configure VLANs on your device. The wireless ports of an access point, in particular, are able to remove the VLAN tag of a frame sent to the clients and to tag received frames with a pre-defined VLAN ID. This functionality makes an access point nothing less than a VLAN-compliant switch with the enhancement of grouping clients into VLAN groups. In general, VLAN segmenting can be configured with all interfaces.

VLAN for Bridging and VLAN for Routing

In the **LAN->VLAN** menu, VLANs (virtual LANs) are configured with interfaces that operate in Bridging mode. Using the **VLAN** menu, you can make all the settings needed for this and query their status.




Caution

For interfaces that operate in Routing mode, you only assign a VLAN ID to the interface. You define this via the parameters **Interface Mode** = *Tagged (VLAN)* and field **VLAN ID** in menu **LAN->IP Configuration->Interfaces->New**.

9.2.1 VLANs


In this menu, you can display all the VLANs already configured, edit your settings and create new VLANs. By default, the *Management* VLAN is available, to which all interfaces are assigned.

9.2.1.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button in order to create new VLANs.

The **LAN->VLAN->VLANs->New** menu consists of the following fields:

Fields in the Configure VLAN menu

Field	Description
VLAN Identifier	Enter the number that identifies the VLAN. In the  menu, you

Field	Description
	can no longer change this value. Possible values are 1 to 4094.
VLAN Name	Enter a unique name for the VLAN. A character string of up to 32 characters is possible.
VLAN Members	Select the ports that are to belong to this VLAN. You can use the Add button to add members. For each entry, also select whether the frames to be transmitted from this port are to be transmitted <i>Tagged</i> (i.e. with VLAN information) or <i>Untagged</i> (i.e. without VLAN information).

9.2.2 Port Configuration

In this menu, you can define and view the rules for receiving frames at the VLAN ports.

The **LAN->VLANs->Port Configuration** menu consists of the following fields:

Fields in the Port Configuration menu

Field	Description
Interface	Shows the port for which you define the PVID and processing rules.
PVID	Assign the selected port the required PVID (Port VLAN Identifier). If a packet without a VLAN tag reaches this port, it is assigned this PVID.
Drop untagged frames	If this option is enabled, untagged frames are discarded. If the option is disabled, untagged frames are tagged with the PVID defined in this menu.
Drop non-members	If this option is enabled, all tagged frames that are tagged with a VLAN ID to which the selected port does not belong are discarded.

9.2.3 Administration

In this menu, you make general settings for a VLAN. The options must be configured separately for each bridge group.

The **LAN->VLANs->Administration** menu consists of the following fields:

Fields in the Bridge Group br<ID> VLAN Options menu

Field	Description
Enable VLAN	Enable or disable the specified bridge group for VLAN. The function is enabled with <i>Enabled</i> . The function is not activated by default.
Management VID	Select the VLAN ID of the VLAN in which your device is to operate.

Chapter 10 Networking

10.1 Routes


Default Route

With a default route, all data is automatically forwarded to one connection if no other suitable route is available. If you set up access to the Internet, you must configure the route to your Internet Service Provider (ISP) as a default route. If, for example, you configure a corporate network connection, only enter the route to the head office or branch office as a default route if you do not configure Internet access over your device. If, for example, you configure both Internet access and a corporate network connection, enter a default route to the ISP and a network route to the head office. You can enter several default routes on your device, but only one default route can be active at any one time. If you enter several default routes, you should thus note differing values for **Metric**.

10.1.1 IPv4 Route Configuration

A list of all configured routes is displayed in the **Network->Routes->IPv4 Route Configuration** menu.

10.1.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create additional routes.


If the *Extended* option is selected for the **Route Class**, an extra configuration section opens.

The **Network->Routes->IPv4 Route Configuration->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Route Type	Select the type of route. Possible values:

Field	Description
	<ul style="list-style-type: none"> • <i>Default Route via Interface</i>: Route via a specific interface which is to be used if no other suitable route is available. • <i>Default Route via Gateway</i>: Route via a specific gateway which is to be used if no other suitable route is available. • <i>Host Route via Interface</i>: Route to an individual host via a specific interface. • <i>Host Route via Gateway</i>: Route to an individual host via a specific gateway. • <i>Network Route via Interface (default value)</i>: Route to a network via a specific interface. • <i>Network Route via Gateway</i>: Route to a network via a specific gateway. <p>Only for interfaces that are operated in DHCP client mode:</p> <p>Even if an interface is configured for DHCP client mode, routes can still be configured for data traffic via that interface. The settings received from the DHCP server are then copied, along with those configured here, to the active routing table. This enables, e. g., in the case of dynamically changing gateway addresses, particular routes to be maintained, or routes with different metrics (i. e. of differing priority) to be specified. However, if the DHCP server sends static routes, the settings configured here are not copied to the routing.</p> <ul style="list-style-type: none"> • <i>Default Route Template per DHCP</i>: The routing information is taken entirely from the DHCP server. Only advanced parameters can be additionally configured. This route remains unchanged by other routes created for this interface and is copied to the routing table in parallel with them. • <i>Host Route Template per DHCP</i>: The settings received by DHCP are supplemented by routing information about a particular host. • <i>Network Route Template per DHCP</i>: The settings received by DHCP are supplemented by routing information about a particular network.

Field	Description
	 Note <p>When the DHCP lease expires or when the device is re-started, the routes that consist from the combination of DHCP settings and those made here are initially deleted once more from the active routing. If the DHCP is reconfigured they are re-generated and re-activated.</p>
Interface	Select the interface to be used for this route.
Route Class	<p>Select the type of Route Class.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Standard</i>: Defines a route with the default parameters. • <i>Extended</i>: Select whether the route is to be defined with extended parameters. If the function is active, a route is created with extended routing parameters such as source interface and source IP address, as well as protocol, source and destination port, type of service (TOS) and the status of the device interface.

Fields in the menu Route Parameters

Field	Description
Local IP Address	<p>Only for Route Type = <i>Default Route via Interface, Host Route via Interface OR Network Route via Interface</i></p> <p>Enter the IP address of the host to which your device is to forward the IP packets.</p>
Destination IP Address/Netmask	<p>Only for Route Type <i>Host Route via Interface OR Network Route via Interface</i></p> <p>Enter the IP address of the destination host or destination network.</p> <p>When Route Type = <i>Network Route via Interface</i></p> <p>Also enter the relevant netmask in the second field.</p>

Field	Description
Gateway IP Address	<p>Only for Route Type = <i>Default Route via Gateway, Host Route via Gateway</i> or <i>Network Route via Gateway</i></p> <p>Enter the IP address of the gateway to which your device is to forward the IP packets.</p>
Metric	<p>Select the priority of the route.</p> <p>The lower the value, the higher the priority of the route.</p> <p>Value range from 0 to 15. The default value is 1.</p>

Fields in the menu **Extended Route Parameters**

Field	Description
Description	Enter a description for the IP route.
Source Interface	<p>Select the interface over which the data packets are to reach the device.</p> <p>The default value is <i>None</i>.</p>
Source IP Address/ Netmask	Enter the IP address and netmask of the source host or source network.
Layer 4 Protocol	<p>Select a protocol.</p> <p>Possible values: <i>ICMP, IGMP, TCP, UDP, GRE, ESP, AH, OSPF, PIM, L2TP, Any</i>.</p> <p>The default value is <i>Any</i>.</p>
Source Port	<p>Only for Layer 4 Protocol = <i>TCP</i> or <i>UDP</i></p> <p>Enter the source port.</p> <p>First select the port number range.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Any</i> (default value): The route is valid for all port numbers. • <i>Single</i>: Enables the entry of a port number. • <i>Range</i>: Enables the entry of a range of port numbers. • <i>Privileged</i>: Entry of privileged port numbers: 0 ... 1023.


Field	Description
	<ul style="list-style-type: none"> • <i>Server</i>: Entry of server port numbers: 5000 ... 32767. • <i>Clients 1</i>: Entry of client port numbers: 1024 ... 4999. • <i>Clients 2</i>: Entry of client port numbers: 32768 ... 65535. • <i>Not privileged</i>: Entry of unprivileged port numbers: 1024 ... 65535. <p>Enter the appropriate values for the individual port or start port of a range in Port and, for a range, the end port in to Port.</p>
Destination Port	<p>Only for Layer 4 Protocol = <i>TCP</i> or <i>UDP</i></p> <p>Enter the destination port.</p> <p>First select the port number range.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Any</i> (default value): The route is valid for all port numbers. • <i>Single</i>: Enables the entry of a port number. • <i>Range</i>: Enables the entry of a range of port numbers. • <i>Privileged</i>: Entry of privileged port numbers: 0 ... 1023. • <i>Server</i>: Entry of server port numbers: 5000 ... 32767. • <i>Clients 1</i>: Entry of client port numbers: 1024 ... 4999. • <i>Clients 2</i>: Entry of client port numbers: 32768 ... 65535. • <i>Not privileged</i>: Entry of unprivileged port numbers: 1024 ... 65535. <p>Enter the appropriate values for the individual port or start port of a range in Port and, for a range, the end port in to Port.</p>
DSCP / TOS Value	<p>Select the Type of Service (TOS).</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Ignore</i> (default value): The type of service is ignored. • <i>DSCP Binary Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format). • <i>DSCP Decimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format).

Field	Description
	<ul style="list-style-type: none"> • <i>DSCP Hexadecimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111. • <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63. • <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F. <p>Enter the relevant value for <i>DSCP Binary Value</i>, <i>DSCP Decimal Value</i>, <i>DSCP Hexadecimal Value</i>, <i>TOS Binary Value</i>, <i>TOS Decimal Value</i> and <i>TOS Hexadecimal Value</i>.</p>
Mode	<p>Select when the interface defined in Route Parameters->Interface is to be used.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Dialup and wait</i> (default value): The route can be used if the interface is "up". If the interface is "dormant", then dial and wait until the interface is "up". • <i>Authoritative</i>: The route can always be used. • <i>Dialup and continue</i>: The route can be used when the interface is "up". If the interface is "dormant", then select and use the alternative route (rerouting) until the interface is "up". • <i>Never dialup</i>: The route can be used when the interface is "up". • <i>Always dialup</i>: The route can be used when the interface is "up". If the interface is "dormant", then dial and wait until the interface is "up". In this case, an alternative interface with a poorer metric is used for routing until the interface is "up".

10.1.2 IPv4 Routing Table

A list of all IPv4 routes is displayed in the **Network->Routes->IPv4 Routing Table** menu. The routes do not all need to be active, but can be activated at any time by relevant data traffic.

Fields in the menu IPv4 Routing Table

Field	Description
Destination IP Address	Displays the IP address of the destination host or destination network.
Netmask	Displays the netmask of the destination host or destination network.
Gateway	Displays the gateway IP address. Nothing is displayed here when routes are received by DHCP.
Interface	Displays the interface used for this route.
Metric	Displays the route's priority. The lower the value, the higher the priority of the route
Route Type	Displays the route type.
Extended Route	Displays whether a route has been configured with advanced parameters.
Delete	You can delete entries with the  symbol.

10.1.3 Options

Back Route Verify

The term Back Route Verify describes a very simple but powerful function. If a check is activated for an interface, incoming data packets are only accepted over this interface if outgoing response packets are routed over the same interface. You can therefore prevent the acceptance of packets with false IP addresses - even without using filters.

The **Networking->Routes->Options** menu consists of the following fields:

Fields in the Back Route Verify menu

Field	Description
Mode	Select how the interfaces to be activated for Back Route Verify are to be specified. Possible values: <ul style="list-style-type: none"> • <i>Enable for all interfaces</i>: Back Route Verify is activated for all interfaces. • <i>Enable for specific interfaces</i> (default value): A

Field	Description
	<p>list of all interfaces is displayed in which Back Route Verify is only enabled for specific interfaces.</p> <ul style="list-style-type: none"> • <i>Disable for all interfaces</i>: Back route verify is disabled for all interfaces.
No.	<p>Only for Mode = <i>Enable for specific interfaces</i></p> <p>Displays the serial number of the list entry.</p>
Interface	<p>Only for Mode = <i>Enable for specific interfaces</i></p> <p>Displays the name of the interface.</p>
Back Route Verify	<p>Only for Mode = <i>Enable for specific interfaces</i></p> <p>Select whether <i>Back Route Verify</i> is to be activated for the interface.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>By default, the function is deactivated for all interfaces.</p>

10.2 NAT

Network Address Translation (NAT) is a function on your device for defined conversion of source and destination addresses of IP packets. If NAT is activated, IP connections are still only allowed by default in one direction, outgoing (forward) (= protective function). Exceptions to the rule can be configured (in [NAT Configuration](#) on page 194).

10.2.1 NAT Interfaces

A list of all NAT interfaces is displayed in the **Networking->NAT->NAT Interfaces** menu.

For every NAT interface, the *NAT active*, *Loopback active*, *Silent Deny* and *PPTP Passthrough* can be selected.

In addition, *Portforwardings* displays how many port forwarding rules were configured for this interface.

Options in the menu NAT Interfaces

Field	Description
NAT active	Select whether NAT is to be activated for the interface. The function is disabled by default.
Loopback active	The NAT loopback function also enables network address translation for connectors whereby NAT is not activated. This is often used in order to interpret queries from the LAN as if they were coming from the WAN. You can use this to test the server services. The function is disabled by default.
Silent Deny	Select whether IP packets are to be silently denied by NAT. If this function is deactivated, the sender of the denied IP packet is informed by means of an appropriate ICMP or TCP RST message. The function is disabled by default.
PPTP Passthrough	Select whether the setup and operation of several simultaneous, outgoing PPTP connections from hosts in the network are also to be permitted if NAT is activated. The function is disabled by default. If PPTP Passthrough is enabled, the device itself cannot be configured as a tunnel endpoint.
Port	Shows the number of portforwarding rules configured in Networking->NAT->NAT Configuration .

10.2.2 NAT Configuration

In the **Networking->NAT->NAT Configuration** menu you can exclude data from NAT simply and conveniently as well as translate addresses and ports. For outgoing data traffic you can configure various NAT methods, i.e. you can determine how an external host establishes a connection to an internal host.

10.2.2.1 New

Choose the **New** button to set up NAT.

The **Networking->NAT->NAT Configuration ->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter a description for the NAT configuration.
Interface	Select the interface for which NAT is to be configured. Possible values: <ul style="list-style-type: none"> • <i>Any</i> (default value): NAT is configured for all interfaces. • <i><Interface name></i>: Select one of the interfaces from the list.
Type of traffic	Select the type of data traffic for which NAT is to be configured. Possible values: <ul style="list-style-type: none"> • <i>incoming (Destination NAT)</i> (default value): The data traffic that comes from outside. • <i>outgoing (Source NAT)</i>: Outgoing data traffic. • <i>excluding (Without NAT)</i>: Data traffic excluded from NAT.
NAT method	Only for Type of traffic = <i>outgoing (Source NAT)</i> Select the NAT method for outgoing data traffic. The starting point for choosing the NAT method is a NAT scenario in which an "internal" source host has initiated an IP connection to an "external" destination host over the NAT interface, and in which an internally valid source address and internally valid source port are translated to an externally valid source address and an externally valid source port. Possible values: <ul style="list-style-type: none"> • <i>full-cone</i> (UDP only): Any given external host may send IP packets via the external address and the external port to the initiating source address and the initial source port. • <i>restricted-cone</i> (UDP only): Like full-cone NAT; as external host, however, only the initial "external" destination host is allowed. • <i>port-restricted-cone</i> (UDP only): Like restricted-cone NAT; however, exclusively data from the initial destination

Field	Description
	<p>port are allowed.</p> <ul style="list-style-type: none"> • <i>symmetric</i> (standard value) any protocol: Outbound, an externally valid source address and an externally valid source port are administratively set. Inbound, only response packets within the existing connection are allowed.

In the **NAT Configuration** -> **Specify original traffic** menu, you can configure for which data traffic NAT is to be used.

Fields in the menu **Specify original traffic**

Field	Description
Service	<p>Not for Type of traffic = <i>outgoing</i> (Source NAT) and NAT method = <i>full-cone, restricted-cone</i> or <i>port-restricted-cone</i>.</p> <p>Select one of the preconfigured services.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>User-defined</i> (default value) • <i><service name></i>
Action	<p>Only for Type of traffic = <i>excluding</i> (Without NAT)</p> <p>Select which data packets are to be excluded by NAT.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Off</i> (default value): All the data packets that match the following parameters that are to be configured (protocol, source IP address/network mask, destination IP address/netmask, etc.) are excluded by NAT. • <i>Do not exclude</i>: All the data packets that do not match the following parameters that are to be configured (protocol, source IP address/network mask, destination IP address/netmask, etc.) are excluded by NAT.
Protocol	<p>Only for certain services.</p> <p>Not for Type of traffic = <i>outgoing</i> (Source NAT) and NAT method = <i>full-cone, restricted-cone</i> or <i>port-restricted-cone</i>. In this case UDP is automatically defined.</p>

Field	Description
	<p>Select a protocol. According to the selected Service, different protocols are available.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Any</i> (default value)• <i>AH</i>• <i>Chaos</i>• <i>EGP</i>• <i>ESP</i>• <i>GGP</i>• <i>GRE</i>• <i>HMP</i>• <i>ICMP</i>• <i>IGMP</i>• <i>IGP</i>• <i>IGRP</i>• <i>IP</i>• <i>IPinIP</i>• <i>IPv6</i>• <i>IPX in IP</i>• <i>ISO-IP</i>• <i>Kryptolan</i>• <i>L2TP</i>• <i>OSPF</i>• <i>PUP</i>• <i>RDP</i>• <i>RSVP</i>• <i>SKIP</i>• <i>TCP</i>• <i>TLSP</i>• <i>UDP</i>• <i>VRRP</i>• <i>XNS-IDP</i>

Field	Description
Source IP Address/Netmask	<p>Only for Type of traffic = <i>incoming (Destination NAT)</i> or <i>excluding (Without NAT)</i></p> <p>Enter the source IP address and corresponding netmask of the original data packets, as the case arises.</p>
Original Destination IP Address/Netmask	<p>Only for Type of traffic = <i>incoming (Destination NAT)</i></p> <p>Enter the destination IP address and corresponding netmask of the original data packets, as the case arises.</p>
Original Destination Port/Range	<p>Only for Type of traffic = <i>incoming (Destination NAT)</i>, Service = <i>user-defined</i> and Protocol = <i>TCP, UDP, TCP/UDP</i></p> <p>Enter the destination port or the destination port range of the original data packets. The default setting <i>-All-</i> means that the port is not specified.</p>
Original Source IP Address/Netmask	<p>Only for Type of traffic = <i>outgoing (Source NAT)</i></p> <p>Enter the source IP address and corresponding netmask of the original data packets, as the case arises.</p>
Original Source Port/Range	<p>Only for Type of traffic = <i>outgoing (Source NAT)</i>, NAT method = <i>symmetric</i>, Service = <i>user-defined</i> and Protocol = <i>TCP, UDP, TCP/UDP</i></p> <p>Enter the source port of the original data packets. The default setting <i>-All-</i> means that the port remains unspecified.</p> <p>If you select <i>Specify port</i> you can specify a single port, if you select <i>Specify port range</i> you can specify a continuous range of ports which will be applied for filtering the outgoing data traffic</p>
Source Port/Range	<p>Only for Type of traffic = <i>excluding (Without NAT)</i>, Service = <i>user-defined</i> and Protocol = <i>TCP, UDP, TCP/UDP</i></p> <p>Enter the source port or the source port range of the original data packets. The default setting <i>-All-</i> means that the port remains unspecified.</p>
Destination IP Ad-	<p>Only for Type of traffic = <i>excluding (Without NAT)</i> or</p>

Field	Description
Address/Netmask	<p><i>outgoing (Source NAT)</i> and NAT method = symmetric</p> <p>Enter the destination IP address and corresponding netmask of the original data packets, as the case arises.</p>
Destination Port/Range	<p>Only for Type of traffic = outgoing (Source NAT), NAT method = symmetric, Service = user-defined and Protocol = TCP, UDP, TCP/UDP or Type of traffic = excluding (Without NAT), Service = user-defined and Protocol = TCP, UDP, TCP/UDP</p> <p>Enter the destination port or the destination port range of the original data packets. The default setting <i>-All-</i> means that the port remains unspecified.</p>

In the **NAT Configuration -> Replacement Values** menu you can define, depending on whether you're dealing with inbound or outbound data traffic, new addresses and ports, to which specific addresses and ports from the **NAT Configuration -> Specify original traffic** menu can be translated.

Fields in the menu Replacement Values

Field	Description
New Destination IP Address/Netmask	<p>Only for Type of traffic = incoming (Destination NAT)</p> <p>Enter the destination IP address and corresponding netmask to which the original destination IP address is to be translated.</p>
New Destination Port	<p>Only for Type of traffic = incoming (Destination NAT), Service = user-defined and Protocol = TCP, UDP, TCP/UDP</p> <p>Leave the destination port as it appears or enter the destination port to which the original destination port is to be translated.</p> <p>Select <i>Original</i> to leave the original destination port. If you disable <i>Original</i>, an input field appears and you can enter a new destination port.</p> <p><i>Original</i> is active by default.</p>
New Source IP Address/Netmask	<p>Only for Type of traffic = outgoing (Source NAT) and NAT method = symmetric</p> <p>Enter the source IP address to which the original source IP ad-</p>

Field	Description
	dress is to be translated, with corresponding netmask, as the case arises.
New Source Port	<p>Only for Type of traffic = <i>outgoing</i> (Source NAT), NAT method = <i>symmetric</i>, Service = <i>user-defined</i> and Protocol = <i>TCP, UDP, TCP/UDP</i></p> <p>Leave the source port as it appears or enter a new source port to which the original source port is to be translated.</p> <p><i>Original</i> leaves the original source port. If you disable <i>Original</i>, an input field appears in which you can enter a new source port. <i>Original</i> is active by default.</p> <p>If you select <i>Specify port range</i> for Original Source Port/Range, you can choose from the following options:</p> <ul style="list-style-type: none"> • <i>Use Original Source Port/Range</i>: The range specified for Original Source Port/Range is not changed, all port numbers are retained. • <i>Verwende Port/Bereich beginnend bei</i>: There is an input field for you to specify the port number with which to start the port range that replaces the original port range. The count of ports is retained.

10.3 QoS

QoS (Quality of Service) makes it possible to distribute the available bandwidths effectively and intelligently. Certain applications can be given preference and bandwidth reserved for them. This is an advantage, especially for time-critical applications such as VoIP.

The QoS configuration consists of three parts:

- Creating IP filters
- Classifying data
- Prioritising data

10.3.1 QoS Filter

In the **Networking->QoS->QoS Filter** menu IP filters are configured.

The list also displays any configured entries from **Networking->Access Rules->Rule Chains**.

10.3.1.1 New

Choose the **New** button to define more IP filters.

The **Networking->QoS->QoS Filter->New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter the name of the filter.
Service	<p>Select one of the preconfigured services. The extensive range of services configured ex works includes the following:</p> <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i> • <i>charge</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>The default value is <i>User defined</i>.</p>
Protocol	<p>Select a protocol.</p> <p>The <i>Any</i> option (default value) matches any protocol.</p>
Type	<p>Only for Protocol = <i>ICMP</i></p> <p>Select the type.</p> <p>Possible values: <i>Any, Echo reply, Destination unreachable, Source quench, Redirect, Echo, Time exceeded, Timestamp, Timestamp reply</i>.</p> <p>See RFC 792.</p> <p>The default value is <i>Any</i>.</p>

Field	Description
Connection State	<p>With Protocol = <i>TCP</i>, you can define a filter that takes the status of the TCP connections into account.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Established</i>: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter. • <i>Any</i> (default value): All TCP packets match the filter.
Destination IP Address/Netmask	Enter the destination IP address of the data packets and the corresponding netmask.
Destination Port/Range	<p>Only for Protocol = <i>TCP</i> or <i>UDP</i></p> <p>Enter a destination port number or a range of destination port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>-All-</i> (default value): The destination port is not specified. • <i>Specify port</i>: Enter a destination port. • <i>Specify port range</i>: Enter a destination port range.
Source IP Address/Netmask	Enter the source IP address of the data packets and the corresponding netmask.
Source Port/Range	<p>Only for Protocol = <i>TCP</i> or <i>UDP</i></p> <p>Enter a source port number or a range of source port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>-All-</i> (default value): The destination port is not specified. • <i>Specify port</i>: Enter a destination port. • <i>Specify port range</i>: Enter a destination port range.
DSCP/TOS Filter (Layer 3)	<p>Select the Type of Service (TOS).</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Ignore</i> (default value): The type of service is ignored. • <i>DSCP Binary Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP

Field	Description
	<p>packets (indicated in binary format, 6 bit).</p> <ul style="list-style-type: none"> • <i>DSCP Decimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • <i>DSCP Hexadecimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111. • <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63. • <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.
COS Filter (802.1p/Layer 2)	<p>Enter the service class of the IP packets (Class of Service, CoS).</p> <p>Possible values are whole numbers between 0 and 7. Value range 0 to 7.</p> <p>The default value is 0.</p>

10.3.2 QoS Classification

The data traffic is classified in the **Networking->QoS->QoS Classification** menu, i.e. the data traffic is associated using class IDs of various classes. To do this, create class plans for classifying IP packets based on pre-defined IP filters. Each class plan is associated to at least one interface via its first filter.

10.3.2.1 New


Choose the **New** button to create additional data classes.

The **Networking->QoS->QoS Classification->New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Class map	<p>Choose the class plan you want to create or edit.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none"> • <i>New</i> (default value): You can create a new class plan with this setting. • <i><Name of class plan></i>: Shows a class plan that has already been created, which you can select and edit. You can add new filters.
Description	<p>Only for Class map = <i>New</i></p> <p>Enter the name of the class plan.</p>
Filter	<p>Select an IP filter.</p> <p>If the class plan is new, select the filter to be set at the first point of the class plan.</p> <p>If the class plan already exists, select the filter to be attached to the class plan.</p> <p>To select a filter, at least one filter must be configured in the Networking->QoS->QoS Filter menu.</p>
Direction	<p>Select the direction of the data packets to be classified.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Incoming</i>: Incoming data packets are assigned to the class (Class ID) that is then to be defined. • <i>Outgoing</i> (default value): Outgoing data packets are assigned to the class (Class ID) that is then to be defined. • <i>Both</i>: Incoming and outgoing data packets are assigned to the class (Class ID) that is then to be defined.
High Priority Class	<p>Enable or disable the high priority class. If the high priority class is active, the data packets are associated with the class with the highest priority and priority 0 is set automatically.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Class ID	<p>Only for High Priority Class not active.</p> <p>Choose a number which assigns the data packets to a class.</p>

Field	Description
	<div data-bbox="515 206 1182 399" style="border: 1px solid #ccc; padding: 10px;">  <p>Note</p> <p>The class ID is a label to assign data packets to specific classes. (The class ID defines the priority.)</p> </div> <p>Possible values are whole numbers between 1 and 254.</p>
Set DSCP/TOS value (Layer 3)	<p>Here you can set or change the DSCP/TOS value of the IP data packets, based on the class (Class ID) that has been defined.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Preserve</i> (default value): The DSCP/TOS value of the IP data packets remains unchanged. • <i>DSCP Binary Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format). • <i>DSCP Decimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • <i>DSCP Hexadecimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111. • <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63. • <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.
Set COS value (802.1p/Layer 2)	<p>Here you can set/change the service class (Layer 2 priority) in the VLAN Ethernet header of the IP packets, based on the class (Class ID) that has been defined.</p> <p>Possible values are whole numbers between 0 and 7.</p> <p>The default value is <i>Preserve</i>.</p>
Interfaces	<p>Only for Class map = <i>New</i></p>

Field	Description
	When creating a new class plan, select the interfaces to which you want to link the class plan. A class plan can be assigned to multiple interfaces.

10.3.3 QoS Interfaces/Policies

In the **Networking->QoS->QoS Interfaces/Policies** menu, you set prioritisation of data.



Note

Data can only be prioritized in the outgoing direction.

Packets in the high-priority class always take priority over data with class IDs 1 - 254.

It is possible to assign or guarantee each queue and thus each data class a certain part of the total bandwidth of the interface. In addition, you can optimise the transmission of voice data (real time data).

Depending on the respective interface, a queue is created automatically for each class, but only for data traffic classified as outgoing and for data traffic classified in both directions. A priority is assigned to these automatic queues. The value of the priority is equal to the value of the class ID. You can change the default priority of a queue. If you add new queues, you can also use classes in other class plans via the class ID.

10.3.3.1 New

Choose the **New** button to create additional prioritisations.

The **Networking->QoS->QoS Interfaces/Policies->New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Interface	Select the interface for which QoS is to be configured.
Prioritisation Algorithm	Select the algorithm according to which the queues are to be processed. This activates and deactivates QoS on the selected interface.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Priority Queueing</i>: QoS is activated on the interface. The available bandwidth is distributed strictly according to the queue priority. • <i>Weighted Round Robin</i>: QoS is activated on the interface. The available bandwidth is distributed according to the weighting (weight) of the queue. Exception: High-priority packets are always handled with priority. • <i>Weighted Fair Queueing</i>: QoS is activated on the interface. The available bandwidth is distributed as “fairly” as possible among the (automatically detected) traffic flows in a queue. Exception: High-priority packets are always handled with priority. • <i>Disabled</i> (default value): QoS is deactivated on the interface. The existing configuration is not deleted, but can be activated again if required.
Traffic shaping	<p>Activate or deactivate data rate limiting in the send direction.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Maximum Upload Speed	<p>Only for Traffic shaping = enabled.</p> <p>Enter a maximum data rate for the queue in the send direction in kbits.</p> <p>Possible values are <i>0</i> to <i>1000000</i>.</p> <p>The default value is <i>0</i>, i.e. no limits are set, the queue can occupy the maximum bandwidth.</p>
Protocol Header Size below Layer 3	<p>Only for Traffic shaping = enabled.</p> <p>Choose the interface type to include the size of the respective overheads of a datagram when calculating the bandwidth.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>User defined</i> Value in byte. <p>Possible values are <i>0</i> to <i>100</i>.</p>

Field	Description
	<ul style="list-style-type: none"> • <i>Undefined (Protocol Header Offset=0)</i> (default value) <p>Can only be selected for Ethernet interfaces</p> <ul style="list-style-type: none"> • <i>Ethernet</i> • <i>Ethernet and VLAN</i> • <i>PPP over Ethernet</i> • <i>PPP over Ethernet and VLAN</i> <p>Can only be selected for IPSec interfaces:</p> <ul style="list-style-type: none"> • <i>IPSec over Ethernet</i> • <i>IPSec over Ethernet and VLAN</i> • <i>IPSec via PPP over Ethernet</i> • <i>IPSec via PPPoE and VLAN</i>
Encryption Method	<p>Only if an IPSec Peers is selected as Interface, Traffic shaping is <i>Active</i> and Protocol Header Size below Layer 3 is not <i>Undefiniert (Protocol Header Offset=0)</i></p> <p>Select the encryption method used for the IPSec connection. The encryption algorithm determines the length of the block cipher which is taken into account during bandwidth calculation.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>DES, 3DES, Blowfish, Cast - (cipher block size = 64 Bit)</i> • <i>AES128, AES192, AES256, Twofish - (cipher block size = 128 Bit)</i>
Real Time Jitter Control	<p>Only for Traffic shaping = enabled</p> <p>Real Time Jitter Control optimises latency when forwarding real time datagrams. The function ensures that large data packets are fragmented according to the available upload bandwidth.</p> <p>Real Time Jitter Control is useful for small upload bandwidths (< 800 kbps).</p> <p>Activate or deactivate Real Time Jitter Control.</p>

Field	Description
	<p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Control Mode	<p>Only for Real Time Jitter Control = enabled.</p> <p>Select the mode for optimising voice transmission.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>All RTP Streams</i>: All RTP streams are optimised. The function activates the RTP stream detection mechanism for the automatic detection of RTP streams. In this mode, the Real Time Jitter Control is activated as soon as an RTP stream has been detected. • <i>Inactive</i>: Voice data transmission is not optimised. • <i>Controlled RTP Streams only</i>: This mode is used if either the VoIP Application Layer Gateway (ALG) or the VoIP Media Gateway (MGW) is active. Real Time Jitter Control is activated by the control instances ALG or MGW. • <i>Always</i>: Real Time Jitter Control is always active, even if no real time data is routed.
Queues/Policies	<p>Configure the desired QoS queues.</p> <p>For each class created from the class plan, which is associated with the selected interface, a queue is generated automatically and displayed here (only for data traffic classified as outgoing and for data traffic classified as moving in both directions).</p> <p>Add new entries with Add. The Edit Queue/Policy menu opens.</p> <p>By creating a QoS policy a DEFAULT entry with the lowest priority 255 is automatically created.</p>

The menu **Edit Queue/Policy** consists of the following fields:

Fields in the Edit Queue/Policy menu

Field	Description
Description	Enter the name of the queue/policy.

Field	Description
Outbound Interface	Shows the interface for which the QoS queues are being configured.
Prioritisation queue	<p>Select the queue priority type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Class Based</i> (default value): Queue for data classified as “normal” • <i>High Priority</i>: Queue for data classified as “high priority” • <i>Default</i>: Queue for data that has not been classified or data of a class for which no queue has been configured.
Class ID	<p>Only for Prioritisation queue = <i>Class Based</i></p> <p>Select the QoS packet class to which this queue is to apply.</p> <p>To do this, at least one class ID must be given in the Networking->QoS->QoS Classification menu.</p>
Priority	<p>Only for Prioritisation queue = <i>Class Based</i></p> <p>Choose the priority of the queue. Possible values are <i>1 (high priority) to 254 (low priority)</i>.</p> <p>The default value is <i>1</i>.</p>
Weight	<p>Only for Prioritisation Algorithm = <i>Weighted Round Robin</i> or <i>Weighted Fair Queueing</i></p> <p>Choose the priority of the queue. Possible values are <i>1 to 254</i>.</p> <p>The default value is <i>1</i>.</p>
RTT Mode (Realtime Traffic Mode)	<p>Active or deactivate the real time transmission of the data.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>RTT mode should be activated for QoS classes in which real time data has priority. This mode improves latency when forwarding real time datagrams.</p>

Field	Description
	<p>It is possible to configure multiple queues when RTT mode is enabled. Queues with enabled RTT mode must always have a higher priority than queues with disabled RTT mode.</p>
Traffic Shaping	<p>Activate or deactivate data rate (=Traffic Shaping) limiting in the send direction.</p> <p>The data rate limit applies to the selected queue. (This is not the limit that can be defined on the interface.)</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Maximum Upload Speed	<p>Only for Traffic Shaping = enabled.</p> <p>Enter a maximum data rate for the queue in kbits.</p> <p>Possible values are 0 to 1000000.</p> <p>The default value is 0.</p>
Overbooking allowed	<p>Only for Traffic Shaping = enabled.</p> <p>Enable or disable the function. The function controls the bandwidth limit.</p> <p>If Overbooking allowed is activated, the bandwidth limit set for this queue can be exceeded, as long as free bandwidth exists on the interface.</p> <p>If Overbooking allowed is deactivated, the queue can never occupy bandwidth beyond the bandwidth limit that has been set.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Burst size	<p>Only for Traffic Shaping = enabled.</p> <p>Enter the maximum number of bytes that may still be transmitted temporarily when the data rate permitted for this queue has been reached.</p> <p>Possible values are 0 to 64000.</p>

Field	Description
	The default value is <i>0</i> .

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Dropping Algorithm	<p>Choose the procedure for rejecting packets in the QoS queue, if the maximum size of the queue is exceeded.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Tail Drop</i> (default value): The newest packet received is dropped. • <i>Head Drop</i>: The oldest packet in the queue is dropped. • <i>Random Drop</i>: A randomly selected packet is dropped from the queue.
Congestion Avoidance (RED)	<p>Enable or disable preventative deletion of data packets.</p> <p>Packets which have a data size of between Min. queue size and Max. queue size are preventively dropped to prevent queue overflow (RED=Random Early Detection). This procedure ensures a smaller long-term queue size for TCP-based data traffic, so that traffic bursts can also usually be transmitted without large packet losses.</p> <p>The function is activated with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Min. queue size	<p>Enter the lower threshold value for the process prevention of data congestion (RED) in bytes.</p> <p>Possible values are <i>0</i> to <i>262143</i>.</p> <p>The default value is <i>0</i>.</p>
Max. queue size	<p>Enter the upper threshold value for the process prevention of data congestion (RED) in bytes.</p> <p>Possible values are <i>0</i> to <i>262143</i>.</p> <p>The default value is <i>16384</i>.</p>

10.4 Access Rules

Accesses to data and functions are restricted with access lists (which user gets to use which services and files).

You define filters for IP packets in order to allow or block access from or to the various hosts in connected networks. This enables you to prevent undesired connections being set up via the gateway. Access lists define the type of IP traffic the gateway is to accept or deny. The access decision is based on information contained in the IP packets, e.g.:

- source and/or destination IP address
- packet protocol
- source and/or destination port (port ranges are supported)

Access lists are an effective means if, for example, sites with LANs interconnected over a bintec elmeg gateway wish to deny all incoming FTP requests or only allow Telnet sessions between certain hosts.

Access filters in the gateway are based on the combination of filters and actions for filter rules (= rules) and the linking of these rules to form rule chains. They act on the incoming data packets to allow or deny access to the gateway for certain data.

A filter describes a certain part of the IP data traffic based on the source and/or destination IP address, netmask, protocol and source and/or destination port.

You use the rules that you set up in the access lists to tell the gateway what to do with the filtered data packets, i.e. whether it should allow or deny them. You can also define several rules, which you arrange in the form of a chain to obtain a certain sequence.

There are various approaches for the definition of rules and rule chains:

Allow all packets that are not explicitly denied, i.e.:

- Deny all packets that match Filter 1.
- Deny all packets that match Filter 2.
- ...
- Allow the rest.

or

Allow all packets that are explicitly allowed, i.e.:

- Allow all packets that match Filter 1.
- Allow all packets that match Filter 2.

- ...
- Deny the rest.

or

Combination of the two possibilities described above.

A number of separate rule chains can be created. The same filter can also be used in different rule chains.

You can also assign a rule chain individually to each interface.



Caution

Make sure you don't lock yourself out when configuring filters:


If possible, access your gateway for filter configuration over the serial console interface or ISDN Login.

10.4.1 Access Filter

This menu is for configuration of access filter. Each filter describes a certain part of the IP traffic and defines, for example, the IP addresses, the protocol, the source port or the destination port.

A list of all access filters is displayed in the **Networking->Access Rules->Access Filter** menu.

10.4.1.1 Edit or New

Choose the  icon to edit existing entries. To configure access filters, select the **New** button.

The **Networking->Access Rules->Access Filter->New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter a description for the filter.
Service	Select one of the preconfigured services. The extensive range of services configured ex works includes the following:

Field	Description
	<ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i> • <i>charge</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>The default value is <i>User defined</i>.</p>
Protocol	<p>Select a protocol.</p> <p>The <i>Any</i> option (default value) matches any protocol.</p>
Type	<p>Only if Protocol = <i>ICMP</i></p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Any</i> • <i>Echo reply</i> • <i>Destination unreachable</i> • <i>Source quench</i> • <i>Redirect</i> • <i>Echo</i> • <i>Time exceeded</i> • <i>Timestamp</i> • <i>Timestamp reply</i> <p>The default value is <i>Any</i>.</p> <p>See RFC 792.</p>
Connection State	<p>Only if Protocol = <i>TCP</i></p> <p>You can define a filter that takes the status of the TCP connections into account.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none"> • <i>Any</i> (default value): All TCP packets match the filter. • <i>Established</i>: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter.
Destination IP Address/Netmask	<p>Enter the destination IP address and netmask of the data packets.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Any</i> (default value) • <i>Host</i>: Enter the IP address of the host. • <i>Network</i>: Enter the network address and the related netmask.
Destination Port/Range	<p>Only if Protocol = <i>TCP, UDP</i></p> <p>Enter a destination port number or a range of destination port numbers that matches the filter.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>-All-</i> (default value): The filter is valid for all port numbers • <i>Specify port</i>: Enables the entry of a port number. • <i>Specify port range</i>: Enables the entry of a range of port numbers.
Source IP Address/Netmask	<p>Enter the source IP address and netmask of the data packets.</p>
Source Port/Range	<p>Only if Protocol = <i>TCP, UDP</i></p> <p>Enter a source port number or the range of source port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>-All-</i> (default value): The filter is valid for all port numbers • <i>Specify port</i>: Enables the entry of a port number. • <i>Specify port range</i>: Enables the entry of a range of port numbers.
DSCP/TOS Filter (Layer 3)	<p>Select the Type of Service (TOS).</p>


Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Ignore</i> (default value): The type of service is ignored. • <i>DSCP Binary Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). • <i>DSCP Decimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • <i>DSCP Hexadecimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111. • <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63. • <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.
COS Filter (802.1p/Layer 2)	<p>Enter the service class of the IP packets (Class of Service, CoS).</p> <p>Possible values are whole numbers between 0 and 7.</p> <p>The default value is <i>Ignore</i>.</p>

10.4.2 Rule Chains

Rules for IP filters are configured in the **Rule Chains** menu. These can be created separately or incorporated in rule chains.

In the **Networking->Access Rules->Rule Chains** menu, all created filter rules are listed.

10.4.2.1 Edit or New


Choose the  icon to edit existing entries. To configure access lists, select the **New** button.

The **Networking->Access Rules->Rule Chains->New** menu consists of the following

fields:

Fields in the Basic Parameters menu

Field	Description
Rule Chain	<p>Select whether to create a new rule chain or to edit an existing one.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>New</i> (default value): You can create a new rule chain with this setting. • <i><Name of class plan></i>: Select an already existing rule chain, and thus add another rule to it.
Description	Enter the name of the rule chain.
Access Filter	<p>Select an IP filter.</p> <p>If the rule chain is new, select the filter to be set at the first point of the rule chain.</p> <p>If the rule chain already exists, select the filter to be attached to the rule chain.</p>
Action	<p>Define the action to be taken for a filtered data packet.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Allow</i> (default value): Allow packet if it matches the filter. • <i>Allow if filter does not match</i>: Allow packet if it does not match the filter. • <i>Deny if filter matches</i>: Deny packet if it matches the filter. • <i>Deny if filter does not match</i>: Deny packet if it does not match the filter. • <i>Ignore</i>: Use next rule.


To set the rules of a rule chain in a different order select the  button in the list menu for the entry to be shifted. A dialog box opens, in which you can decide under **Move** whether the entry *below* (default value) or *above* another rule of this rule chain is to be shifted.

10.4.3 Interface Assignment

In this menu, the configured rule chains are assigned to the individual interfaces and the gateway's behavior is defined for denying IP packets.

A list of all configured interface assignments is displayed in the **Networking->Access Rules->Interface Assignment** menu.

10.4.3.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to configure additional assignments.

The **Networking->Access Rules->Interface Assignment->New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Interface	Select the interface for which a configured rule chain is to be assigned.
Rule Chain	Select a rule chain.
Silent Deny	<p>Define whether the sender is to be informed if an IP packet is denied.</p> <ul style="list-style-type: none"> • <i>Enabled</i> (default value): The sender is not informed. • <i>Disabled</i>: The sender receives an ICMP message.
Reporting Method	<p>Define whether a syslog message is to be generated if a packet is denied.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>No report</i>: No syslog message. • <i>Info</i> (default value): A syslog message is generated with the protocol number, source IP address and source port number. • <i>Dump</i>: A syslog message is generated with the contents of the first 64 bytes of the denied packet.

10.5 Drop In

"Drop-in mode" allows you to split a network into smaller segments without having to divide the IP network into subnets. Several interfaces can be combined in a drop-in group and assigned to a network to do this. All of the interfaces are then configured with the same IP address.

Within a segment, network components which are connected to a connection can then be grouped and, for example, be protected by firewall. Data traffic from network components between individual segments which are assigned to different ports are then controlled according to the configured firewall rules.

10.5.1 Drop In Groups

The **Networking->Drop In->Drop In Groups** menu displays a list of all the **Drop In Groups**. Each **Drop In** group represents a network.

10.5.1.1 New

Select the **New** button to set up other **Drop In Groups**.

The **Networking->Drop In->Drop In Groups->New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Group Description	Enter a unique name for the Drop In group.
Mode	Select which mode is to be used to send the MAC addresses of network components. Possible values: <ul style="list-style-type: none"> • <i>Transparent</i> (default value): ARP packets and IP packets belonging to the drop-in network are routed transparently (unchanged). • <i>Proxy</i>: ARP packets and IP packets related to the drop-in network are forwarded with the MAC address of the corresponding interface.
Network Configuration	Select how an IP address / netmask is assigned to the Drop In network.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Static</i> (default value) • <i>DHCP</i>
Network Address	<p>Only for Network Configuration = <i>Static</i></p> <p>Enter the network address of the Drop In network.</p>
Netmask	<p>Only for Network Configuration = <i>Static</i></p> <p>Enter the corresponding netmask.</p>
Local IP Address	<p>Only for Network Configuration = <i>Static</i></p> <p>Enter the local IP address. This IP address must be identical for all the Ethernet ports in a network.</p>
DHCP Client on Interface	<p>Only for Network Configuration = <i>DHCP</i></p> <p>Here you can select an Ethernet interface on your router which is to act as the DHCP client.</p> <p>You need this setting, for example, if your provider's router is being used as the DHCP server.</p> <p>You can choose from the interfaces available to your device; however the interface must be a member of the drop-in group.</p>
ARP Lifetime	<p>Determines the time period for which the ARP entries will be held in the cache.</p> <p>The default value is <i>3600</i> seconds.</p>
DNS assignment via DHCP	<p>The gateway can modify DHCP packets which pass through the drop-in group and identify itself as an available DNS server.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Unchanged</i> (default value) • <i>Own IP Address</i>
Exclude from NAT (DMZ)	<p>Here you can take data traffic from NAT.</p> <p>Use this function to, for example, ensure that certain web serv-</p>

Field	Description
	<p>ers in a DMZ can be accessed.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Interface Selection	<p>Select all the ports which are to be included in the Drop In group (in the network).</p> <p>Add new entries with Add.</p>

Chapter 11 Multicast

What is multicasting?

Many new communication technologies are based on communication from one sender to several recipients. Therefore, modern telecommunication systems such as voice over IP or video and audio streaming (e.g. IPTV or Webradio) focus on reducing data traffic, e.g. by offering TriplePlay (voice, video, data). Multicast is a cost-effective solution for effective use of bandwidth because the sender of the data packet, which can be received by several recipients, only needs to send the packet once. The packet is sent to a virtual address defined as a multicast group. Interested recipients log in to these groups.

Other areas of use

One classic area in which multicast is used is for conferences (audio/video) with several recipients. The most well-known are probably the MBone Multimedia Audio Tool (VAT), Video Conferencing Tool (VIC) and Whiteboard (WB). VAT can be used to hold audio conferences. All subscribers are displayed in a window and the speaker(s) are indicated by a black box. Other areas of use are of particular interest to companies. Here, multicasting makes it possible to synchronise the databases of several servers, which is valuable for multinationals or even companies with just a few locations.

Address range for multicast

For IPv4 the IP addresses 224.0.0.0 to 239.255.255.255 (224.0.0.0/4) are reserved for multicast in the class D network. An IP address from this range represents a multicast group to which several recipients can log in. The multicast router then forwards the required packets to all subnets with logged in recipients.

Multicast basics

Multicast is connectionless, which means that any trouble-shooting or flow control needs to be guaranteed at application level.

At transport level, UDP is used almost exclusively, as, in contrast to TCP, it is not based on a point-to-point connection.

At IP level, the main difference is therefore that the destination address does not address

a dedicated host, but rather a group, i.e. during the routing of multicast packets, the decisive factor is whether a recipient is in a logged-in subnet.

In the local network, all hosts are required to accept all multicast packets. For Ethernet or FDD, this is based on MAC mapping, where the group address is encoded into the destination MAC address. For routing between several networks, the routers first need to make themselves known to all potential recipients in the subnet. This is achieved by means of Membership Management protocols such as IGMP for IPv4 and MLP for IPv6.

Membership Management protocol

In IPv4, IGMP (Internet Group Management Protocol) is a protocol that hosts can use to provide the router with multicast membership information. IP addresses of the class D address range are used for addressing. An IP address in this class represents a group. A sender (e.g. Internet radio) sends data to this group. The addresses (IP) of the various senders within a group are called the source (addresses). Several senders (with different IP addresses) can therefore transmit to the same multicast group, leading to a 1-to-n relationship between groups and source addresses. This information is forwarded to the router by means of reports. In the case of incoming multicast data traffic, a router can use this information to decide whether a host in its subnet wants to receive it. Your device supports the current version IGMP V3, which is upwardly compatible, which means that both V3 and V1/V2 hosts can be managed.

Your device supports the following multicast mechanisms:

- Forwarding: This relates to static forwarding, i.e. incoming data traffic for a group is passed in all cases. This is a useful option if multicast data traffic is to be permanently passed.
- IGMP: IGMP is used to gather information about the potential recipients in a subnet. In the case of a hop, incoming multicast data traffic can thus be selected.



Tip

With multicast, the focus is on excluding data traffic from unwanted multicast groups. Note that if forwarding is combined with IGMP, the packets can be forwarded to the groups specified in the forwarding request.

11.1 General

11.1.1 General

In the **Multicast->General->General** menu you can disable or enable the multicast function.

The **Multicast->General->General** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Multicast Routing	<p>Select whether Multicast Routing should be used.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

11.2 IGMP

IGMP (Internet Group Management Protocol, see RFC 3376) is used to signal the information about group (membership) in a subnet. As a result, only the packets explicitly wanted by a host enter the subnet.

Special mechanisms ensure that the requirements of the individual clients are taken into consideration. At the moment there are three versions of IGMP (V1 - V3); most current systems use V3, and less often V2.


Two packet types play a central role in IGMP: queries and reports.

Queries are only transmitted from a router. If several IGMP routers exist in a network, the router with the lowest IP address is the "querier". We differentiate here between a general query (sent to 224.0.0.1), a group-specific query (sent to a group address) and the group-and-source-specific query (sent to a specific group address). Reports are only sent by hosts to respond to queries.

11.2.1 IGMP

In this menu, you configure the interfaces on which IGMP is to be enabled.

11.2.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to configure IGMP on other interfaces.

The **Multicast->IGMP->IGMP->New** menu consists of the following fields:

Fields in the IGMP Settings menu

Field	Description
Interface	Select the interface on which IGMP is to be enabled, i.e. queries are sent and responses are accepted.
Query Interval	Enter the interval in seconds in which IGMP queries are to be sent. Possible values are <i>0 to 600</i> . The default value is <i>125</i> .
Maximum Response Time	For the sending of queries, enter the time interval in seconds within which hosts must respond. The hosts randomly select a time delay from this interval before sending the response. This spreads the load in networks with several hosts, improving performance. Possible values are <i>0,0 to 25,0</i> . The default value is <i>10,0</i> .
Robustness	Select the multiplier for controlling the timer values. A higher value can e.g. compensate for packet loss in a network susceptible to loss. If the value is too high, however, the time between logging off and stopping of the data traffic can be increased (leave latency). Possible values are <i>2 to 8</i> . The default value is <i>2</i> .
Last Member Query Interval	Define the time after a query for which the router waits for an answer. If you shorten the interval, it will be more quickly detected that the last member has left a group so that no more packets for this group should be forwarded to this interface. Possible values are <i>0,0 to 25,0</i> . The default value is <i>1,0</i> .

Field	Description
IGMP State Limit	Limit the number of reports/queries per second for the selected interface.
Mode	Specify whether the interface defined here only works in host mode or in both host mode and routing mode. Possible values: <ul style="list-style-type: none"> • <i>Routing</i> (default value): The interface is operated in Routing mode. • <i>Host</i>: The interface is only operated in host mode.

IGMP Proxy

IGMP Proxy enables you to simulate several locally connected interfaces as a subnet to an adjacent router. Queries coming in to the IGMP Proxy interface are forwarded to the local subnets. Local reports are forwarded on the IPGM Proxy interface.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
IGMP Proxy	Select whether your device is to forward the hosts' IGMP messages in the subnet via its defined Proxy Interface .
Proxy Interface	Only for IGMP Proxy = enabled Select the interface on your device via which queries are to be received and collected.

11.2.2 Options

In this menu, you can enable and disable IGMP on your system. You can also define whether IGMP is to be used in compatibility mode or only IGMP V3 hosts are to be accepted.

The **Multicast->IGMP->Options** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
IGMP Status	<p>Select the IGMP status.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Auto</i> (default value): Multicast is activated automatically for hosts if the hosts open applications that use multicast. • <i>Up</i>: Multicast is always on. • <i>Down</i>: Multicast is always off.
Mode	<p>Only for IGMP Status = <i>Up</i> or <i>Auto</i></p> <p>Select Multicast Mode.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Compatibility Mode</i> (default value): The router uses IGMP version 3. If it notices a lower version in the network, it uses the lowest version it could detect. • <i>Version 3 only</i>: Only IGMP version 3 is used.
Maximum Groups	Enter the maximum number of groups to be permitted, both internally and in reports.
Maximum Sources	Enter the maximum number of sources that are specified in version 3 reports and the maximum number of internally managed sources per group.
IGMP State Limit	<p>Enter the maximum permitted total number of incoming queries and messages per second.</p> <p>The default value is 0, i.e. the number of IGMP status messages is not limited.</p>

11.3 Forwarding

11.3.1 Forwarding

In this menu, you specify which multicast groups are always passed between the interfaces of your device.

11.3.1.1 New

Choose the **New** button to create forwarding rules for new multicast groups.

The **Multicast->Forwarding->Forwarding->New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
All Multicast Groups	<p>Select whether all multicast groups, i.e. the complete multicast address range 224.0.0.0/4, are to be forwarded from the defined Source Interface to the defined Destination Interface. To do this, check <i>Enabled</i></p> <p>Disable the option if you only want to forward one defined multicast group to a particular interface.</p> <p>The option is deactivated by default.</p>
Multicast Group Address	<p>Only for All Multicast Groups = not active.</p> <p>Enter here the address of the multicast group you want to forward from a defined Source Interface to a defined Destination Interface.</p>
Source Interface	Select the interface on your device to which the selected multicast group is sent.
Destination Interface	Select the interface on your device to which the selected multicast group is to be forwarded.

Chapter 12 WAN

This menu offers various options for configuring accesses or connections from your LAN to the WAN. You can also optimise voice transmission here for telephone calls over the Internet.

12.1 Internet + Dialup

In this menu, you can set up Internet access or dialup connections.

In addition, you can create address pools for the dynamic assignment of IP addresses.

To enable your device to set up connections to networks or hosts outside your LAN, you must configure the partners you want to connect to on your device. This applies to outgoing connections (your device dials its WAN partner) and incoming connections (a remote partner dials the number of your device).

If you want to set up Internet access, you must set up a connection to your Internet Service Provider (ISP). For broadband Internet access, your device provides the PPP-over-Ethernet (PPPoE), PPP-over-PPTP and PPP-over-ATM (PPPoA) protocols. You can also configure Internet access over ISDN.



Note




Note your provider's instructions.


Dialin connections over ISDN are used to establish a connection to networks or hosts outside your LANs.

All the entered connections are displayed in a list, which contains the **Description**, the **User Name**, the **Authentication** and the current **Status**.

The **Status** field can have the following values:

Possible values for Status

Field	Description
	connected
	not connected (dialup connection); connection setup possible
	not connected (e.g. because of an error during setup of an outgoing connection, a renewed attempt is only possible after a

Field	Description
	specified number of seconds)
	administratively set to down (deactivated); connection setup not possible for leased lines:

Default Route

With a default route, all data is automatically forwarded to one connection if no other suitable route is available. Access to the Internet should always be set up as the default route to the Internet Service Provider (ISP). Further information on possible route types can be found under **Networking->Routes**.

Activating NAT

With Network Address Translation (NAT), you conceal your whole network to the outside world behind one IP address. You should certainly do this for your connection to the Internet Service Provider (ISP).

Only outgoing sessions are allowed initially if NAT is activated. To allow certain connections from outside to hosts within the LAN, these must be explicitly defined and admitted.

Connection Idle Timeout

The connection idle timeout is determined in order to clear the connection automatically if it is not being used, i.e. if data is no longer being sent, to help you save costs.

Block after Connection Failure

You use this function to set up a waiting time for outgoing connection attempts after which your device's connection attempt is regarded as having failed.

Authentication

When a call is received on ISDN connections, the calling party number is always sent over the ISDN D-channel. This number enables your device to identify the caller (CLID), provided the caller is entered on your device. After identification with CLID, your device can additionally carry out PPP authentication with the connection partner before it accepts the call.

Your device needs the necessary data for this, which you should enter here, for all PPP connections. Establish the type of authentication process that should be performed, then

enter a common password and two codes. You get this information, for example, from your Internet Service Provider (ISP) or the system administrator at your head office. If the data you entered on your device is the same as the caller's data, the call is accepted. The call is rejected if the data is not the same.

Callback

The callback mechanism can be used for every connection over an ISDN or over an AUX interface to obtain additional security regarding the connection partner or to clearly allocate the costs of connections. A connection is not set up until the calling party has been clearly identified by calling back. Your device can answer an incoming call with a callback or request a callback from a connection partner. Identification can be based on the calling party number or PAP/CHAP/MS-CHAP authentication. Identification is made in the former case without call acceptance, as the calling party number is transferred over the ISDN D-channel, and in the latter case with call acceptance.

Channel Bundling

Your device supports dynamic and static channel bundling for dialup connections. Channel bundling can only be used for ISDN connections for a bandwidth increase or as a backup. Only one B-channel is initially opened when a connection is set up.

Dynamic

Dynamic channel bundling means that your device connects other ISDN B-channels to increase the throughput for connections if this is required, e.g. for large data rates. If the amount of data traffic drops, the additional B-channels are closed again.

If devices from other manufacturers are to be used at the far end, ensure that these support dynamic channel bundling for a bandwidth increase or as a backup.

Static

In static channel bundling, you specify right from the start how many B-channels your device is to use for connections, regardless of the transferred data rate.

12.1.1 PPPoE

A list of all PPToE interfaces is displayed in the **WAN->Internet + Dialup->PPPoE** menu.

PPP over Ethernet (PPPoE) is the use of the Point-to-Point Protocol (PPP) network protocol over an Ethernet connection. Today, PPPoE is used for ADSL connections in Germany. In Austria, the Point To Point Tunnelling Protocol (PPTP) was originally used for ADSL access. However, PPPoE is now offered here too by some providers.

12.1.1.1 New

Choose the **New** button to set up new PPPoE interfaces.

The menu **WAN->Internet + Dialup->PPPoE->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter a name to uniquely identify the PPPoE partner. The first character in this field must not be a number. No special characters or umlauts must be used.
PPPoE Mode	<p>Select whether you want to use a standard Internet connection over PPPoE (<i>Standard</i>) or your Internet access is to be set up over several interfaces (<i>Multilink</i>). If you choose <i>Multilink</i>, you can connect several DSL connections from a provider over PPP as a static bundle in order to obtain more bandwidth. Each of these DSL connections should use a separate Ethernet connection for this. At the moment, many providers are still in the process of preparing the PPPoE Multilink function.</p> <p>For PPPoE Multilink, we recommend using your device's Ethernet switch in Split-Port mode and to use a separate Ethernet interface e.g. <i>en1-1</i>, <i>en1-2</i> for each PPPoE connection.</p> <p>If you also want to use an external modem for PPPoE Multilink, you must run your device's Ethernet switch in Split-Port mode.</p>
PPPoE Ethernet Interface	<p>Only for PPPoE Mode = <i>Standard</i></p> <p>Select the Ethernet interface specified for a standard PPPoE connection.</p> <p>If you want to use an external DSL modem, select the Ethernet port to which the modem is connected.</p> <p>When using the internal DSL modem, select here the EthoA interface configured in WAN->ATM->Profiles->New.</p>
PPPoE Interfaces for Multilink	<p>Only for PPPoE Mode = <i>Multilink</i></p> <p>Select the interfaces you want to use for your Internet connection. Click the Add button to create new entries.</p>

Field	Description
User Name	Enter the user name.
Password	Enter the password.
VLAN	Certain Internet service providers require a VLAN-ID. Activate this function to be able to enter a value under VLAN ID .
VLAN ID	Only if VLAN is enabled. Enter the VLAN-ID that you received from your provider.
Always on	Select whether the interface should always be activated. The function is enabled with <i>Enabled</i> . The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	Only if Always on is disabled. Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are <i>0</i> to <i>3600</i> (seconds). <i>0</i> deactivates the short hold. The default value is <i>300</i> . Example: <i>10</i> for FTP transmission, <i>20</i> for LAN-to-LAN transmission, <i>90</i> for Internet connections.

Fields in the IP Mode and Routes menu

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: <ul style="list-style-type: none"> • <i>Get IP Address</i> (default value): Your device is dynamically assigned an IP address.

Field	Description
	<ul style="list-style-type: none"> • <i>Static</i>: You enter a static IP address.
Default Route	<p>Select whether the route to this connection partner is to be defined as the default route.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Create NAT Policy	<p>Specify whether Network Address Translation (NAT) is to be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Local IP Address	<p>Only if IP Address Mode = <i>Static</i></p> <p>Enter the static IP address of the connection partner.</p>
Route Entries	<p>Only if IP Address Mode = <i>Static</i></p> <p>Define other routing entries for this connection partner.</p> <p>Add new entries with Add.</p> <ul style="list-style-type: none"> • <i>Remote IP Address</i>: IP address of the destination host or network. • <i>Netmask</i>: Netmask for Remote IP Address. If no entry is made, your device uses a default netmask. • <i>Metric</i>: The lower the value, the higher the priority of the route (range of values 0... 15). The default value is 1.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is 60.
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked.

Field	Description
	<p>Possible values are <i>0</i> to <i>100</i>.</p> <p>The default value is <i>5</i>.</p>
Authentication	<p>Select the authentication protocol for this connection partner. Select the authentication specified by your provider.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>PAP</i> (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted. • <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP. • <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • <i>PAP/CHAP/MS-CHAP</i>: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.) • <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only. • <i>None</i>: Some providers use no authentication. In this case, select this option.
DNS Negotiation	<p>Select whether your device receives IP addresses for Primary DNS Server and Secondary DNS Server from the connection partner or sends these to the connection partner.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Prioritize TCP ACK Packets	<p>Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
LCP Alive Check	<p>Select whether the availability of the remote terminal is to be checked by sending LCP echo requests or replies. This makes</p>

Field	Description
	<p>it possible to switch to a backup connection more quickly in the event of line faults.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
MTU	<p>Enter the maximum packet size (Maximum Transfer Unit, MTU) in bytes that is allowed for the connection.</p> <p>With default value <i>Automatic</i>, the value is specified by link control at connection setup.</p> <p>If you disable <i>Automatic</i>, you can enter a value.</p> <p>Possible values are <i>1</i> to <i>8192</i>.</p> <p>The default value is <i>0</i>.</p>

12.1.2 PPTP

A list of all PPTP interfaces is displayed in the **WAN->Internet + Dialup->PPTP** menu.

In this menu, you configure an Internet connection that uses the Point Tunnelling Protocol (PPTP) to set up a connection. This is required in Austria, for example.

12.1.2.1 New

Choose the **New** button to set up new PPTP interfaces.

The menu **WAN->Internet + Dialup->PPTP->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	<p>Enter a name for uniquely identifying the internet connection.</p> <p>The first character in this field must not be a number No special characters or umlauts must be used.</p>
PPTP Ethernet Interface	<p>Select the IP interface over which packets are to be transported to the remote PPTP terminal.</p> <p>If you want to use an external DSL modem, select the Ethernet</p>

Field	Description
	<p>port to which the modem is connected.</p> <p>When using the internal DSL modem, select here the EthoA interface configured in Physical Interfaces->ATM->Profiles->New, e.g. <i>ethoa50-0</i>.</p>
User Name	Enter the user name.
Password	Enter the password.
Always on	<p>Select whether the interface should always be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>Only activate this option if you have Internet access with a flat-rate charge.</p>
Connection Idle Timeout	<p>Only if Always on is disabled.</p> <p>Enter the idle interval in seconds. This determines how many seconds should pass between sending the last traffic data packet and clearing the connection.</p> <p>Possible values are <i>0</i> to <i>3600</i> (seconds). <i>0</i> deactivates the timeout.</p> <p>The default value is <i>300</i>.</p> <p>Example: <i>10</i> for FTP transmission, <i>20</i> for LAN-to-LAN transmission, <i>90</i> for Internet connections.</p>

Fields in the IP Mode and Routes menu

Field	Description
IP Address Mode	<p>Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Get IP Address</i> (default value): Your device is automatically assigned a temporarily valid IP address from the provider.

Field	Description
	<ul style="list-style-type: none"> • <i>Static</i>: You enter a static IP address.
Default Route	<p>Select whether the route to this connection partner is to be defined as the default route.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Create NAT Policy	<p>Specify whether Network Address Translation (NAT) is to be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Local IP Address	<p>Only for IP Address Mode = <i>Static</i></p> <p>Assign an IP address from your LAN to the PPT interface, which is to be used as your device's internal source address.</p>
Route Entries	<p>Only if IP Address Mode = <i>Static</i></p> <p>Define other routing entries for this PPTP partner.</p> <p>Add new entries with Add.</p> <ul style="list-style-type: none"> • <i>Remote IP Address</i>: IP address of the destination host or network. • <i>Netmask</i>: Netmask for Remote IP Address. If no entry is made, your device uses a default netmask. • <i>Metric</i>: The lower the value, the higher the priority of the route (range of values 0... 15). The default value is 1.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is 60.
Maximum Number of	Enter the number of unsuccessful attempts to setup a connec-

Field	Description
Dialup Retries	<p>tion before the interface is blocked.</p> <p>Possible values are <i>0</i> to <i>100</i>.</p> <p>The default value is <i>5</i>.</p>
Authentication	<p>Select the authentication protocol for this Internet connection. Select the authentication specified by your provider.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>PAP</i> (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted. • <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP. • <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • <i>PAP/CHAP/MS-CHAP</i>: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.) • <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only. • <i>None</i>: Some providers use no authentication. In this case, select this option.
DNS Negotiation	<p>Select whether your device receives IP addresses for Primary DNS Server and Secondary DNS Server from the connection partner or sends these to the connection partner.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Prioritize TCP ACK Packets	<p>Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

Field	Description
PPTP Address Mode	<p>Displays the address mode. The value cannot be changed.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Static</i>: The Local PPTP IP Address will be assigned to the selected Ethernet port.
Local PPTP IP Address	<p>Assign the PPTP interface an IP address that is used as the source address.</p> <p>The default value is <i>10.0.0.140</i>.</p>
Remote PPTP IP Address	<p>Enter the IP address of the PPTP partner.</p> <p>The default value is <i>10.0.0.138</i>.</p>
LCP Alive Check	<p>Select whether the availability of the remote terminal is to be checked by sending LCP echo requests or replies. This makes it possible to switch to a backup connection more quickly in the event of line faults.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

12.1.3 ISDN

A list of all ISDN interfaces is displayed in the **WAN->Internet + Dialup->ISDN** menu.

In this menu, you configure the following ISDN connections:

- Internet access over ISDN
- LAN to LAN connection over ISDN
- Remote (Mobile) dial-in
- Use of the ISDN Callback function

12.1.3.1 New

Choose the **New** button to set up new ISDN interfaces.

The menu **WAN->Internet + Dialup->ISDN->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	<p>Enter a name for uniquely identifying the connection partner.</p> <p>The first character in this field must not be a number No special characters or umlauts must be used.</p>
Connection Type	<p>Select which layer 1 protocol your device should use.</p> <p>This setting applies for outgoing connections to the connection partner and only for incoming connections from the connection partner if they could be identified on the basis of the calling party number.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>ISDN 64 kbps</i>: For 64-kbps ISDN data connections. • <i>ISDN 56 kbps</i>: For 56-kbps ISDN data connections.
User Name	Enter your device code (local PPP user name).
Remote User (for Dial-in only)	Enter the code of the remote terminal (remote PPP user name).
Password	Enter the password.
Always on	<p>Select whether the interface should always be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>Only activate this option if you have Internet access with a flat-rate charge.</p>
Connection Idle Timeout	<p>Only if Always on is disabled.</p> <p>Enter the idle interval in seconds. This determines how many seconds should pass between sending the last traffic data packet and clearing the connection.</p> <p>Possible values are <i>0</i> to <i>3600</i> (seconds). <i>0</i> deactivates the timeout. The default value is <i>20</i>.</p>

Fields in the IP Mode and Routes menu

Field	Description
IP Address Mode	<p>Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Static</i> (default value): You enter a static IP address. • <i>Provide IP Address</i>: Your device dynamically assigns an IP address to the remote terminal. • <i>Get IP Address</i>: Your device is dynamically assigned an IP address.
Default Route	<p>Only for IP Address Mode = <i>Static</i> and <i>Get IP Address</i></p> <p>Select whether the route to this connection partner is to be defined as the default route.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Create NAT Policy	<p>Only for IP Address Mode = <i>Static</i> and <i>Get IP Address</i></p> <p>When you configure an ISDN Internet connection, specify whether Network Address Translation (NAT) is to be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Local IP Address	<p>Only if IP Address Mode = <i>Static</i></p> <p>Assign the IP address from your LAN to the ISDN interface which is to be used as your device's internal source address.</p>
Route Entries	<p>Only if IP Address Mode = <i>Static</i></p> <p>Define other routing entries for this connection partner.</p> <ul style="list-style-type: none"> • <i>Remote IP Address</i>: IP address of the destination host or network. • <i>Netmask</i>: Netmask for Remote IP Address If no entry is made, your device uses a default netmask. • <i>Metric</i>: The lower the value, the higher the priority of the route (range of values 0... 15). The default value is 1.

Field	Description
IP Assignment Pool	<p>Only if IP Address Mode = <i>Provide IP Address</i></p> <p>Select IP pools configured in the WAN->Internet + Dialup->IP Pools menu. If an IP pool has not been configured here yet, the message <i>Not yet defined</i> appears in this field.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Block after connection failure for	<p>Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed.</p> <p>The default value is <i>300</i>.</p>
Maximum Number of Dialup Retries	<p>Enter the number of unsuccessful attempts to setup a connection before the interface is blocked.</p> <p>Possible values are <i>0</i> to <i>100</i>.</p> <p>The default value is <i>5</i>.</p>
Usage Type	<p>If necessary, select a special interface use.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <i>Standard</i> (default value): No special type is selected. <i>Dialin only</i>: The interface is used for incoming dialup connections and callbacks initiated externally. <i>Multi-User (Dialin only)</i>: The interface is defined as multi-user connection partner, i.e. several clients dial in with the same user name and password.
Authentication	<p>Select the authentication protocol for this PPTP partner.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <i>PAP</i> (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.

Field	Description
	<ul style="list-style-type: none"> • <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP. • <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • <i>PAP/CHAP/MS-CHAP</i>: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.) • <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only. • <i>None</i>: Some providers use no authentication. In this case, select this option.
Encryption	<p>Only for Authentication = <i>MS-CHAPv2</i></p> <p>If necessary, select the type of encryption that should be used for data traffic to the connection partner. This is only possible if STAC or MS-STAC compression is not activated for the connection. If Encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i> (default value): MPP encryption is not used. • <i>Enabled</i>: MPP encryption V2 with 128 bit is used to RFC 3078. • <i>Windows compatible</i>: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
Callback Mode	<p>Select the Callback Mode function.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i> (default value): Your device does not call back. • <i>Active</i>: Select one of the following options: <ul style="list-style-type: none"> • <i>No PPP negotiation</i>: Your device calls the connection partner to request a callback. • <i>Windows Client Mode</i>: Your device calls the connection partner to request a callback via CBCP (Callback Control Protocol). Needed for Windows clients. • <i>Passive</i>: Select one of the following options: <ul style="list-style-type: none"> • <i>PPP Negotiation or CLID</i>: Your device calls back immediately when requested to do so by the connection partner.

Field	Description
	<ul style="list-style-type: none"> • <i>Windows Server Mode</i>: Your device calls back after a period of time suggested by the Microsoft client (NT: 10 seconds, new systems: 12 seconds. It uses the call number (Entries->Call Number) with the Mode <i>Outgoing</i> or <i>Both</i> entered for the connection partner. If no number is entered, the required number can be reported by the caller in a PPP negotiation. This setting should be avoided where possible for security reasons. At present, this cannot be avoided when connecting mobile Microsoft clients via a DCN. • <i>Delayed, CLID only</i>: Your device calls back after approx. four seconds if your device is requested to do so by the connection partner. Only makes sense for CLID. • <i>Windows Server Mode, Callback optional</i>: like <i>Windows Server Mode</i> with the option of termination. This setting should be avoided for security reasons. The Microsoft client also has the option of aborting callback and maintaining the initial connection to your device without callback. This only applies if no fixed, outgoing number has been configured for the connection partner. This is done by closing the dialog box that appears with Cancel.

Fields in the Bandwith on Demand Options menu

Field	Description
Channel Bundling	<p>Select whether channel bundling is to be used for ISDN connections with the connection partner, and if so, what type.</p> <p>Your device supports dynamic and static channel bundling for dialup connections. Only one B-channel is initially opened when a connection is set up. Dynamic channel bundling means that your device connects other ISDN B channels to increase the throughput for connections if this is required, e.g. for large data rates. If the amount of data traffic drops, the additional B-channels are closed again. In static channel bundling, you specify right from the start how many B-channels your device is to use, regardless of the transferred data rate.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i> (default value): No channel bundling, only one B-channel is ever available for connections.

Field	Description
	<ul style="list-style-type: none"> • <i>Static</i>: Static channel bundling. • <i>Dynamic</i>: Dynamic channel bundling.

Fields in the Dial Numbers menu

Field	Description
Entries	Add new entries with Add .

Fields in menu Dial Number Configuration (appears only for Entries = Add)

Field	Description
Mode	<p>Only if Entries = <i>Add</i></p> <p>The calling party number of the call is compared with the number entered under Call Number. Defines whether Call Number should be used for incoming or outgoing calls or for both.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Both</i> (default value): For incoming and outgoing calls. • <i>Incoming</i>: For incoming calls, where your connection partner dials in to your device. • <i>Outgoing</i>: For outgoing calls, where you dial your connection partner. <p>The calling party number of the incoming call is compared with the number entered under Call Number.</p>
Call Number	Enter the connection partner's numbers.
Number of Used Ports	Select which port is used.

Fields in the IP Options menu

Field	Description
OSPF Mode	<p>Select whether and how routes are propagated via the interface and/or OSPF protocol packets are sent.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Passive</i> (default value): OSPF is not activated for this interface, i.e. no routes are propagated or OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces.

Field	Description
	<ul style="list-style-type: none"> • <i>Active</i>: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface. • <i>Inactive</i>: OSPF is disabled for this interface.
Proxy ARP Mode	<p>Select whether and how ARP requests from your own LAN are to be responded to for the specified connection partner.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Inactive</i> (default value): Deactivates Proxy ARP for this connection partner. • <i>Up or Dormant</i>: Your device only responds to an ARP request if the status of the connection to the connection partner is <i>Up</i> or <i>Dormant</i>. In the case of <i>Dormant</i>, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • <i>Up only</i>: Your device responds to an ARP request only if the status of the connection to the connection partner is <i>Up</i>, i.e. a connection already exists to the connection partner.
DNS Negotiation	<p>Select whether your device receives IP addresses for Primary DNS Server and Secondary DNS Server and WINS Server Primary and Secondary from the connection partner or sends these to the connection partner.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

12.1.4 IP Pools


The **IP Pools** menu displays a list of all IP pools.

Your device can operate as a dynamic IP address server for PPP connections. You can use this function by providing one or more pools of IP addresses. These IP addresses can be assigned to dialling-in connection partners for the duration of the connection.

Any host routes entered always have priority over IP addresses from the address pools. This means that, if an incoming call has been authenticated, your device first checks whether a host route is entered in the routing table for this caller. If not, your device can allocate an IP address from an address pool (if available). If address pools have more than one IP address, you cannot specify which connection partner receives which ad-

dress. The addresses are initially assigned in order. If a new dial-in takes place within an interval of one hour, an attempt is made to allocate the same IP address that was assigned to this partner the previous time.

12.1.4.1 Edit or New

Choose the **New** button to set up new IP address pools. Choose the  icon to edit existing entries.

The menu **WAN->Internet + Dialup->IP Pools->New** consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	<p>Primary: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool.</p> <p>Secondary: Optionally, enter the IP address of an alternative DNS server.</p>

12.2 Real Time Jitter Control

When telephoning over the Internet, voice data packets normally have the highest priority. Nevertheless, if the upstream bandwidth is low, noticeable delays in voice transmission can occur when other packets are routed at the same time.

The real time jitter control function solves this problem. So that the "line" is not blocked for too long for the voice data packets, the size of the other packets can be reduced, if required, during a telephone call.

12.2.1 Controlled Interfaces

In the **WAN->Real Time Jitter Control->Controlled Interfaces** a list of functions is displayed for which the Real Time Jitter Control function is configured.

12.2.1.1 New

Click the **New** button to optimise voice transmission for other interfaces.

The menu **WAN->Real Time Jitter Control->Controlled Interfaces->New** consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Interface	Define for which interfaces voice transmission is to be optimised.
Control Mode	<p>Select the mode for the optimisation.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Controlled RTP Streams only</i> (default value): By means of the data routed via the media gateway, the system detects voice data traffic and optimises the voice transmission. • <i>All RTP Streams</i>: All RTP streams are optimised. • <i>Inactive</i>: Voice data transmission is not optimised. • <i>Always</i>: Voice data transmission is always optimised.
Maximum Upload Speed	Enter the maximum available upstream bandwidth in kbp/s for the selected interface.

Chapter 13 VPN

A connection that uses the Internet as a "transport medium" but is not publicly accessible is referred to as a VPN (Virtual Private Network). Only authorised users have access to such a VPN, which is seemingly also referred to as a VPN tunnel. Normally the data transported over a VPN is encrypted.

A VPN allows field staff or staff working from home offices to access data on the company's network. Subsidiaries can also connect to head office over VPN.

Various protocols are available for creating a VPN tunnel, e.g. IPSec or PPTP.

The connection partner is authenticated with a password, using preshared keys or certificates.

With IPSec the data is encrypted using AES or 3DES, for example; with PPTP, you can use MPPE.

13.1 IPSec

IPSec enables secure connections to be set up between two locations (VPN). This enables sensitive business data to be transferred via an unsecure medium such as the Internet. The devices used function here as the endpoints of the VPN tunnel. IPSec involves a number of Internet Engineering Task Force (IETF) standards, which specify mechanisms for the protection and authentication of IP packets. IPSec offers mechanisms for encrypting and decrypting the data transferred in the IP packets. The IPSec implementation can also be smoothly integrated in a Public Key Infrastructure (PKI, see [Certificates](#) on page 41). IPSec implementation achieves this firstly by using the Authentication Header (AH) protocol and Encapsulated Security Payload (ESP) protocol and secondly through the use of cryptographic key administration mechanisms like the Internet Key Exchange (IKE) protocol.

Additional Traffic Filter

bintec elmeg gateways support two different methods of setting up IPSec connections:

- a method based on policies and
- a method based on routing.

The policy-based method uses data traffic filters to negotiate the IPSec phase 2 SAs. This allows for a very "fine-grained" filter to be applied to the IP packet, even at the level of the protocol and the port.

The routing-based method offers various advantages over the policy-based method, e.g., NAT/PAT within a tunnel, IPSec in combination with routing protocols and the creation of VPN backup scenarios. With the routing-based method, the configured or dynamically learned routes are used to negotiate the IPSec phase 2 SAs. Although this method does simplify many configurations, problems may also be caused by competing routes or the "coarser" filtering of data traffic.

The **Additional Traffic Filter** parameter fixes this problem. You can apply a "finer" filter, i.e. you can enter the source IP address or the source port. If a **Additional Traffic Filter** is configured, this is used to negotiate the IPSec phase 2 SAs; the route now only determines which data traffic is to be routed.

If an IP packet does not match the defined **Additional Traffic Filter**, it is rejected.

If an IP packet meets the requirements in an **Additional Traffic Filter**, IPSec phase 2 negotiation begins and data traffic is transferred over the tunnel.

**Note**

The parameter **Additional Traffic Filter** is exclusively relevant for the initiation of the IPSec connection, it is only used for outgoing traffic.

**Note**


Please note that the phase 2 policies must be configured identically on both of the IPSec tunnel endpoints.

13.1.1 IPSec Peers

An endpoint of a communication is defined as peer in a computer network. Each peer offers its services and uses the services of other peers.

A list of all configured IPSec Peers is displayed in the **VPN->IPSec->IPSec Peers** menu.

Peer Monitoring

The menu for monitoring a peer is called by selecting the  button for the peer in the peer list. See [Values in the IPSec Tunnels list](#) on page 391.

13.1.1.1 New

Choose the **New** button to set up more IPsec peers.

The menu **VPN->IPsec->IPsec Peers->New** consists of the following fields:

Fields in the menu Peer Parameters

Field	Description
Administrative Status	<p>Select the status to which you wish to set the peer after saving the peer configuration.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Up</i> (default value): The peer is available for setting up a tunnel immediately after saving the configuration. • <i>Down</i>: The peer is initially not available after the configuration has been saved.
Description	<p>Enter a description of the peer that identifies it.</p> <p>The maximum length of the entry is 255 characters.</p>
Peer Address	<p>Enter the official IP address of the peer or its resolvable host name.</p> <p>The entry can be omitted in certain configurations, whereby your device then cannot initiate an IPsec connection.</p>
Peer ID	<p>Select the ID type and enter the peer ID.</p> <p>This entry is not necessary in certain configurations.</p> <p>The maximum length of the entry is 255 characters.</p> <p>Possible ID types:</p> <ul style="list-style-type: none"> • <i>Fully Qualified Domain Name (FQDN)</i> • <i>E-mail Address</i> • <i>IPV4 Address</i> • <i>ASN.1-DN (Distinguished Name)</i> • <i>Key ID: Any string</i> <p>On the peer device, this ID corresponds to the Local ID Value.</p>

Field	Description
Internet Key Exchange	<p>Select the version of the Internet Exchange Protocol to be used.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>IKEv1</i> (default value): Internet Key Exchange Protocol Version 1 • <i>IKEv2</i>: Internet Kex Exchange Protocol Version 2
Authentication Method	<p>Only for Internet Key Exchange = IKEv2</p> <p>Select the authentication method.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Preshared Keys</i> (default value): If you do not use certificates for the authentication, you can select Preshared Keys. These are configured during peer configuration in the IPSec Peers. The preshared key is the shared password. • <i>RSA Signature</i>: Phase 1 key calculations are authenticated using the RSA algorithm.
Local ID Type	<p>Only for Internet Key Exchange = IKEv2</p> <p>Select the local ID type.</p> <p>Possible ID types:</p> <ul style="list-style-type: none"> • <i>Fully Qualified Domain Name (FQDN)</i> • <i>E-mail Address</i> • <i>IPV4 Address</i> • <i>ASN.1-DN (Distinguished Name)</i> • <i>Key ID</i>: Any string
Local ID	<p>Only for Internet Key Exchange = IKEv2</p> <p>Enter the ID of your device.</p> <p>For Authentication Method = DSA Signature or RSA Signature the option Use Subject Name from certificate is displayed.</p> <p>When you enable the option Use Subject Name from certificate, the first alternative subject name indicated in the certificate</p>

Field	Description
	<p>is used, or, if none is specified, the subject name of the certificate is used.</p> <p>Note: If you use certificates for authentication and your certificate contains alternative subject names (see Certificates on page 41), you must make sure your device selects the first alternative subject name by default. Make sure you and your peer both use the same name, i.e. that your local ID and the peer ID your partner configures for you are identical.</p>
Preshared Key	<p>Enter the password agreed with the peer.</p> <p>The maximum length of the entry is 50 characters. All characters are possible except for <code>0x</code> at the start of the entry.</p>

Fields in the menu Interface Routes

Field	Description
IP Address Assignment	<p>Select the configuration mode of the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Static</i> (default value): Enter a static IP address. • <i>IKE Config Mode Client</i>: Can only be selected for IKEv1. Select this option if your gateway receives an IP address from the server as IPSec client. • <i>IKE Config Mode Server</i>: Select this option if your gateway assigns an IP address as server for connecting clients. This is taken from the selected IP Assignment Pool.
Config Mode	<p>Only where IP Address Assignment = <i>IKE Config Mode Server</i> or <i>IKE Config Mode Client</i></p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Pull</i> (default value): The client requests the IP address and the gateway answers the request. • <i>Push</i>: The gateway suggests an IP address to the client and the client must either accept or reject this. <p>This value must be identical for both sides of the tunnel.</p>
IP Assignment Pool	<p>Only if IP Address Assignment = <i>IKE Config Mode Server</i></p>

Field	Description
	Select an IP pool configured in the VPN->IPSec->IP Pools menu. If an IP pool has not been configured here yet, the message <i>Not yet defined</i> appears in this field.
Default Route	<p>Only for IP Address Assignment = <i>Static</i> or <i>IKE Config Mode Client</i></p> <p>Select whether the route to this IPSec peer is to be defined as the default route.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Local IP Address	<p>Only for IP Address Assignment = <i>Static</i> or <i>IKE Config Mode Server</i></p> <p>Enter the WAN IP address of your IPSec tunnel. This can be the same IP address as the address configured on your router as the LAN IP address.</p>
Metric	<p>Only for IP Address Assignment = <i>Static</i> or <i>IKE Config Mode Client</i> and Default Route = <i>Enabled</i></p> <p>Select the priority of the route.</p> <p>The lower the value, the higher the priority of the route.</p> <p>Value range from <i>0</i> to <i>15</i>. The default value is <i>1</i>.</p>
Route Entries	<p>Only for IP Address Assignment = <i>Static</i> or <i>IKE Config Mode Client</i></p> <p>Define routing entries for this connection partner.</p> <ul style="list-style-type: none"> • <i>Remote IP Address</i>: IP address of the destination host or LAN. • <i>Netmask</i>: Netmask for <i>Remote IP Address</i>. • <i>Metric</i>: The lower the value, the higher the priority of the route (possible values <i>0</i>.. <i>15</i>). The default value is <i>1</i>.

Fields in the menu **Additional Traffic Filter**

Field	Description
Additional Traffic Filter	Only for Internet Key Exchange = <i>IKEv1</i> Use Add to create a new filter.

Additional data traffic filters

bintec elmeg Gateways support two different methods for establishing IPsec connections:

- a method based on policies and
- a method based on routing.

The policy-based method uses data traffic filters to negotiate the IPsec phase 2 SAs. This enables the filtering of the IP packets to be very "fine grained" down to protocol and port level.

The routing-based method offers various advantages over the policy-based method, e.g., NAT/PAT within a tunnel, IPsec in combination with routing protocols and the creation of VPN backup scenarios. With the routing-based method, the configured or dynamically learned routes are used to negotiate the IPsec phase 2 SAs. While it is true that this method simplifies many configurations, at the same time there can be problems due to competing routes or the "coarser" filtering of the data traffic.

The **Additional Traffic Filter** parameter fixes this problem. You can filter more "finely", i. e. you can, e. g., specify the source IP address or the source port. If there is a **Additional Traffic Filter** configured, it is used to negotiate the IPsec phase 2 SAs; the route only determines which data traffic is to be routed.

If an IP packet does not match the defined **Additional Traffic Filter** it is discarded.

If an IP packet meets the requirements in an **Additional Traffic Filter**, IPsec phase 2 negotiation begins and data traffic is transferred over the tunnel.



Note

The parameter **Additional Traffic Filter** is only relevant to the initiator of the IPsec connection, it only applies to outgoing data traffic.



Note

Please note that the phase 2 policies must be configured identically on both of the IPsec tunnel endpoints.

Add new entries with **Add**.

The menu **VPN->IPSec->IPSec Peers->New->Add** consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter a description for the filter.
Protocol	Select a protocol. The <i>Any</i> option (default value) matches all protocols.
Source IP Address/Netmask	Enter, if required, the source IP address and netmask of the data packets. Possible values: <ul style="list-style-type: none"> • <i>Any</i> • <i>Host</i>: Enter the IP address of the host. • <i>Network</i> (default value): Enter the network address and the related netmask.
Source Port	Only for Protocol = <i>TCP</i> or <i>UDP</i> Enter the source port of the data packets. The default setting - <i>All</i> - (= -1) means that the port remains unspecified.
Destination IP Address/Netmask	Enter the destination IP address and corresponding netmask of the data packets.
Destination Port	Only for Protocol = <i>TCP</i> or <i>UDP</i> Enter the destination port of the data packets. The default setting - <i>All</i> - (= -1) means that the port remains unspecified.

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Advanced IPSec Options

Field	Description
Phase-1 Profile	Select a profile for Phase 1. Besides user-defined profiles, pre-defined profiles are available. Possible values:

Field	Description
	<ul style="list-style-type: none"> • <i>None (use default profile)</i>: Uses the profile marked as standard in VPN->IPSec->Phase-1 Profiles • <i>Multi-Proposal</i>: Uses a special profile which contains the proposals for Phase 1 3DES/MD5, AES/MD5 and Blowfish/MD5 regardless of the proposal selection in menu VPN->IPSec->Phase-1 Profiles. • <i><Profilname></i>: Uses a profile configured in menu VPN->IPSec->Phase-1 Profiles for Phase 1.
Phase-2 Profile	<p>Select a profile for Phase 2. Besides user-defined profiles, pre-defined profiles are available.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None (use default profile)</i>: Uses the profile marked as standard in VPN->IPSec->Phase-2 Profiles • <i>Multi-Proposal</i>: Uses a special profile which contains the proposals for Phase 2 3DES/MD5, AES-128/MD5 and Blowfish/MD5 regardless of the proposal selection in menu VPN->IPSec->Phase-2 Profiles. • <i><Profilname></i>: Uses a profile configured in menu VPN->IPSec->Phase-2 Profiles for Phase 2.
XAUTH Profile	<p>Select a profile created in VPN->IPSec->XAUTH Profiles if you wish to use this IPSec peer XAuth for authentication.</p> <p>If XAuth is used together with IKE Config Mode, the transactions for XAuth are carried out before the transactions for IKE Config Mode.</p>
Number of Admitted Connections	<p>Choose how many users can connect using this peer profile.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>One User</i> (default value): Only one peer can be connected with the data defined in this profile. • <i>Multiple Users</i>: Several peers can be connected with the data defined in this profile. The peer entry is duplicated for each connection request with the data defined in this profile.
Start Mode	<p>Select how the peer is to be switched to the active state.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none"> • <i>On Demand</i> (default value): The peer is switched to the active state by a trigger. • <i>Always up</i>: The peer is always active.

Fields in the menu **Advanced IP Options**

Field	Description
Public Interface	Specify the public (or WAN) interface that this peer is to use to connect to its VPN partner. If you select <i>Chosen by Routing</i> , the decision as to via which interface the data traffic is routed is made based on the current routing table. If you select an interface, the interface is used taking into consideration the setting under Public Interface Mode .
Public Interface Mode	Specify how strictly the setting under Public Interface is handled. Possible values: <ul style="list-style-type: none"> • <i>Enforce</i>: Only the selected interface is used, whatever the priorities in the current routing table. • <i>Preferred</i>: Depending on the priorities in the current routing table, the selected interface is used if no more favourable route is available via a different interface.
Public Source IP Address	<p>If you are operating more than one Internet connection in parallel, here you can specify the public IP address that is to be used as the source address for the peer's data traffic. Select whether the Public Source IP Address is to be enabled.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>In the input field, enter the public IP address that is to be used as the sender address.</p> <p>The function is disabled by default.</p>
Back Route Verify	<p>Select whether a check on the back route should be activated for the interface to the connection partner.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
MobiKE	<p>Only for peers with IKEv2.</p> <p>MobiKE In cases of changing public IP addresses, enables</p>

Field	Description
	<p>only these addresses to be updated in the SAs without the SAs themselves having to be renegotiated.</p> <p>The function is enabled by default.</p> <p>Note that MobIKE requires a current IPsec client, e. g. the current Windows 7 or Windows 8 client or the latest version of the bintec elmeg IPsec client.</p>
Proxy ARP	<p>Select whether your device is to respond to ARP requests from its own LAN on behalf of the specific connection partner.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Inactive</i> (default value): Deactivates Proxy ARP for this IPsec peer. • <i>Up or Dormant</i>: Your device only responds to an ARP request if the status of the connection to the IPsec peer is <i>Up</i> (active) or <i>Dormant</i> (dormant). In the case of <i>Dormant</i>, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • <i>Up only</i>: Your device responds to an ARP request only if the status of the connection to the IPsec peer is <i>Up</i> (active), i.e. a connection already exists to the IPsec peer.

IPsec Callback

bintec elmeg devices support the DynDNS service to enable hosts without fixed IP addresses to obtain a secure connection over the Internet. This service enables a peer to be identified using a host name that can be resolved by DNS. You do not need to configure the IP address of the peer.

The DynDNS service does not signal whether a peer is actually online and cannot cause a peer to set up an Internet connection to enable an IPsec tunnel over the Internet. This possibility is created with IPsec callback: Using a direct ISDN call to a peer, you can signal that you are online and waiting for the peer to set up an IPsec tunnel over the Internet. If the called peer currently has no connection to the Internet, the ISDN call causes a connection to be set up. This ISDN call costs nothing (depending on country), as it does not have to be accepted by your device. The identification of the caller from his or her ISDN number is enough information to initiate setting up a tunnel.

To set up this service, you must first configure a call number for IPsec callback on the passive side in the **Physical Interfaces->ISDN Ports->MSN Configuration->New** menu.

The value *IPSec* is available for this purpose in the field **Service**. This entry ensures that incoming calls for this number are routed to the IPSec service.

If callback is active, the peer is caused to initiate setting up an IPSec tunnel by an ISDN call as soon as this tunnel is required. If callback is set to passive, setting up a tunnel to the peer is always initiated if an ISDN call is received on the relevant number (**MSN** in menu **Physical Interfaces->ISDN Ports->MSN Configuration->New** for **Service** *IPSec*). This ensures that both peers are reachable and that the connection can be set up over the Internet. The only case in which callback is not executed is if SAs (Security Associations) already exist, i.e. the tunnel to the peer already exists.



Note

If a tunnel is to be set up to a peer, the interface over which the tunnel is to be implemented is activated first by the IPSec Daemon. If IPSec with DynDNS is configured on the local device, the own IP address is propagated first and then the ISDN call is sent to the remote device. This ensures that the remote device can actually reach the local device if it initiates the tunnel setup.

Transfer of IP Address over ISDN

Transferring the IP address of a device over ISDN (in the D channel and/or B channel) opens up new possibilities for the configuration of IPSec VPNs. This enables restrictions that occur in IPSec configuration with dynamic IP addresses to be avoided.



Note

To use the IP address transfer over ISDN function, you must obtain a free-of-charge extra licence.

You can obtain the licence data for extra licences via the online licensing pages in the support section at www.bintec-elmeg.com. Please follow the online licensing instructions.

Before System Software Release 7.1.4, IPSec ISDN callback only supported tunnel setup if the current IP address of the initiator could be determined by indirect means (e.g. via DynDNS). However, DynDNS has serious disadvantages, such as the latency until the IP address is actually updated in the database. This can mean that the IP address propagated via DynDNS is not correct. This problem is avoided by transferring the IP address over ISDN. This type of transfer of dynamic IP addresses also enables the more secure ID Protect mode (main mode) to be used for tunnel setup.

Method of operation: Various modes are available for transferring your own IP address to the peer: The address can be transferred free in the D channel or in the B channel, but here the call must be accepted by the remote station and therefore incurs costs. If a peer whose IP address has been assigned dynamically wants to arrange for another peer to set up an IPsec tunnel, it can transfer its own IP address as per the settings described in *Fields in the menu IPsec Callback* on page 264. Not all transfer modes are supported by all telephone companies. If you are not sure, automatic selection by the device can be used to ensure that all the available possibilities can be used.

**Note**

The callback configuration should be the same on the two devices so that your device is able to identify the IP address information from the called peer.

The following roles are possible:

- One side takes on the active role, the other the passive role.
- Both sides can take on both roles (both).

The IP address transfer and the start of IKE phase 1 negotiation take place in the following steps:

- (1) Peer A (the callback initiator) sets up a connection to the Internet in order to be assigned a dynamic IP address and be reachable for peer B over the Internet.
- (2) Your device creates a token with a limited validity and saves it together with the current IP address in the MIB entry belonging to peer B.
- (3) Your device sends the initial ISDN call to peer B, which transfers the IP address of peer A and the token as per the callback configuration.
- (4) Peer B extracts the IP address of peer A and the token from the ISDN call and assigns them to peer A based on the calling party number configured (the ISDN number used by peer A to send the initial call to peer B).
- (5) The IPsec Daemon at peer B's device can use the transferred IP address to initiate phase 1 negotiation with peer A. Here the token is returned to peer A in part of the payload in IKE negotiation.
- (6) Peer A is now able to compare the token returned by peer B with the entries in the MIB and so identify the peer without knowing its IP address.

As peer A and peer B can now mutually identify each other, negotiations can also be conducted in the ID Protect mode using preshared keys.

**Note**

In some countries (e.g. Switzerland), the call in the D channel can also incur costs. An incorrect configuration at the called side can mean that the called side opens the B channel the calling side incurs costs.

The following options are only available on devices with an ISDN connection:

Fields in the menu IPsec Callback

Field	Description
Mode	<p>Select the Callback Mode.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Inactive</i> (default value): IPsec callback is deactivated. The local device neither reacts to incoming ISDN calls nor initiates ISDN calls to the remote device. • <i>Passive</i>: The local device only reacts to incoming ISDN calls and, if necessary, initiates setting up an IPsec tunnel to the peer. No ISDN calls are sent to the remote device to cause this to set up an IPsec tunnel. • <i>Active</i>: The local device sends an ISDN call to the remote device to cause this to set up an IPsec tunnel. The device does not react to incoming ISDN calls. • <i>Both</i>: Your device can react to incoming ISDN calls and send ISDN calls to the remote device. The setting up of an IPsec tunnel is executed (after an incoming ISDN call) and initiated (by an outgoing ISDN call).
Incoming Phone Number	<p>Only for Mode = <i>Passive</i> or <i>Both</i></p> <p>Enter the ISDN number from which the remote device calls the local device (calling party number). Wildcards may also be used.</p>
Outgoing Phone Number	<p>Only for Mode = <i>Active</i> or <i>Both</i></p> <p>Enter the ISDN number with which the local device calls the remote device (called party number). Wildcards may also be used.</p>
Transfer own IP ad-	Select whether the IP address of your own device is to be

Field	Description
Transfer over ISDN/GSM	<p>transferred over ISDN for IPsec callback.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Transfer Mode	<p>Only for Transfer own IP address over ISDN/GSM = enabled</p> <p>Select the mode in which your device is to attempt to transfer its IP address to the peer.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Autodetect best mode</i>: Your device automatically determines the most favourable mode. It first tries all D channel modes before switching to the B channel. (Costs are incurred for using the B channel.) • <i>Autodetect only D Channel Modes</i>: Your device automatically determines the most favourable D channel mode. The use of the B channel is excluded. • <i>Use specific D Channel Mode</i>: Your device tries to transfer the IP address in the mode set in the Mode field. • <i>Try specific D Channel Mode, fall back to B Channel</i>: Your device tries to transfer the IP address in the mode set in the Mode field. If this does not succeed, the IP address is transferred in the B channel. (This incurs costs.) • <i>Use only B Channel Mode</i>: Your device transfers the IP address in the B channel. This incurs costs.
D Channel Mode	<p>Only for Transfer Mode = <i>Use specific D Channel Mode</i> or <i>Try specific D Channel Mode, fall back to B Channel</i></p> <p>Select the D channel mode in which your device tries to transfer the IP address.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>LLC</i> (default value): The IP address is transferred in the "LLC information elements" of the D channel. • <i>SUBADDR</i>: The IP address is transferred in the subaddress "information elements" of the D channel. • <i>LLC and SUBADDR</i>: The IP address is transferred in both

Field	Description
	the "LLC" and "subaddress information elements".

13.1.2 Phase-1 Profiles

A list of all configured tunnel profiles is displayed in the **VPN->IPSec->Phase-1 Profiles** menu.

In the **Default** column, you can mark the profile to be used as the default profile.

13.1.2.1 New

Choose the **New** (at **Create new IKEv1 Profile** or **Create new IKEv2 Profile**) button to create additional profiles.

The menu **VPN->IPSec->Phase-1 Profiles->New** consists of the following fields:

Fields in the Phase-1 (IKE) Parameters menu

Field	Description
Description	Enter a description that uniquely defines the type of rule.
Proposals	<p>In this field, you can select any combination of encryption and message hash algorithms for IKE phase 1 on your device. The combination of six encryption algorithms and four message hash algorithms gives 24 possible values in this field. At least one proposal must exist. Therefore the first line of the table cannot be deactivated.</p> <p>Encryption algorithms (Encryption):</p> <ul style="list-style-type: none"> • <i>3DES</i> (default value): 3DES is an extension of the DES algorithm with an effective key length of 112 bits, which is rated as secure. It is the slowest algorithm currently supported. • <i>Twofish</i>: Twofish was a final candidate for the AES (Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower. • <i>Blowfish</i>: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish. • <i>CAST</i>: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES.

Field	Description
	<ul style="list-style-type: none"> • <i>DES</i>: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits. • <i>AES</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. The partner's AES key length is used here. If this has also selected the parameter <i>AES</i> , a key length of 128 bits is used. • <i>AES-128</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 128 bits. • <i>AES-192</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 192 bits. • <i>AES-256</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 256 bits. <p>Hash algorithms (Authentication):</p> <ul style="list-style-type: none"> • <i>MD5</i> (default value): MD5 (Message Digest #5) is an older hash algorithm. It is used with a 96 bit digest length for IPSec. • <i>SHA1</i>: SHA1 (Secure Hash Algorithm #1) is a hash algorithm developed by NSA (United States National Security Association). It is rated as secure, but is slower than MD5. It is used with a 96 bit digest length for IPSec. • <i>RipeMD 160</i>: RipeMD 160 is a 160 bit hash algorithm. It is used as a secure replacement for MD5 and RipeMD. • <i>Tiger192</i>: Tiger 192 is a relatively new and very fast algorithm. <p>Please note that the description of the encryption and authentication or the hash algorithms is based on the author's knowledge and opinion at the time of creating this User Guide. In particular, the quality of the algorithms is subject to relative aspects and may change due to mathematical or cryptographic developments.</p>

Field	Description
DH Group	<p>Only for Phase-1 (IKE) Parameters</p> <p>The Diffie-Hellman group defines the parameter set used as the basis for the key calculation during phase 1. "MODP" as supported by bintec elmeg devices stands for "modular exponentiation".</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>1 (768 Bit)</i>: During the Diffie-Hellman key calculation, modular exponentiation at 768 bits is used to create the encryption material. • <i>2 (1024 Bit)</i>: During the Diffie-Hellman key calculation, modular exponentiation at 1024 bits is used to create the encryption material. • <i>5 (1536 Bit)</i>: During the Diffie-Hellman key calculation, modular exponentiation at 1536 bits is used to create the encryption material.
Lifetime	<p>Create a lifetime for phase 1 keys.</p> <p>As for RFC 2407, the default value is eight hours, which means the key must be renewed once eight hours have elapsed.</p> <p>The following options are available for defining the Lifetime:</p> <ul style="list-style-type: none"> • Input in Seconds: Enter the lifetime for phase 1 key in seconds. The value can be a whole number from 0 to 2147483647. The default value is <i>14400</i>. • Input in kBytes: Enter the lifetime for phase 1 keys as amount of data processed in kBytes. The value can be a whole number from 0 to 2147483647. The default value is <i>0</i>. The default value as per RFC is used <i>0</i> seconds and <i>0</i> Kbytes are entered.
Authentication Method	<p>Only for Phase-1 (IKE) Parameters</p> <p>Select the authentication method.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Preshared Keys</i> (default value): If you do not use certificates for the authentication, you can select Preshared Keys. These are configured during peer configuration in the

Field	Description
	<p>IPSec->IPSec Peers. The preshared key is the shared password.</p> <ul style="list-style-type: none"> • <i>DSA Signature</i>: Phase 1 key calculations are authenticated using the DSA algorithm. • <i>RSA Signature</i>: Phase 1 key calculations are authenticated using the RSA algorithm. • <i>RSA Encryption</i>: In RSA encryption the ID payload is also encrypted for additional security.
Local Certificate	<p>Only for Phase-1 (IKE) Parameters</p> <p>Only for Authentication Method = <i>DSA Signature</i>, <i>RSA Signature</i> or <i>RSA Encryption</i></p> <p>This field enables you to select one of your own certificates for authentication. It shows the index number of this certificate and the name under which it is saved. This field is only shown for authentication settings based on certificates and indicates that a certificate is essential.</p>
Mode	<p>Only for Phase-1 (IKE) Parameters</p> <p>Select the phase 1 mode.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Aggressive</i> (default value): The Aggressive Mode is necessary if one of the peers does not have a static IP address and preshared keys are used for authentication. It requires only three messages to configure a secure channel. • <i>Main Mode (ID Protect)</i>: This mode (also designated Main Mode) requires six messages for a Diffie-Hellman key calculation and thus for configuring a secure channel, over which the IPSec SAs can be negotiated. A condition is that both peers have static IP addresses if preshared keys are used for authentication. <p>Also define whether the selected mode is used exclusively (Strict), or the peer can also propose another mode.</p>
Local ID Type	<p>Only for Phase-1 (IKE) Parameters</p> <p>Select the local ID type.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Fully Qualified Domain Name (FQDN)</i> • <i>E-mail Address</i> • <i>IPV4 Address</i> • <i>ASN.1-DN (Distinguished Name)</i>
Local ID Value	<p>Only for Phase-1 (IKE) Parameters</p> <p>Enter the ID of your device.</p> <p>For Authentication Method = <i>DSA Signature, RSA Signature</i> or <i>RSA Encryption</i> the Use Subject Name from certificate option is displayed.</p> <p>When you enable the Use Subject Name from certificate option, the first alternative subject name indicated in the certificate is used, or, if none is specified, the subject name of the certificate is used.</p> <p>Note: If you use certificates for authentication and your certificate contains alternative subject names (see Certificates on page 41), you must make sure your device selects the first alternative subject name by default. Make sure you and your peer both use the same name, i.e. that your local ID and the peer ID your partner configures for you are identical.</p>

Alive Check

During communication between two IPSec peers, one of the peers may become unavailable, e.g. due to routing problems or a reboot. However, this can only be detected when the end of the lifetime of the security connection is reached. Up until this point the data packets are lost. These are various methods of performing an alive check to prevent this happening. In the **Alive Check** field you can specify whether a method should be used to check the availability of a peer.

Two methods are available: Heartbeats and Dead Peer Detection.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Alive Check	<p>Only for Phase-1 (IKE) Parameters</p> <p>Select the method to be used to check the functionality of the IPsec connection.</p> <p>In addition to the default method Dead Peer Detection (DPD), the (proprietary) Heartbeat method is implemented. This sends and receives signals every 5 seconds, depending on the configuration. If these signals are not received after 20 seconds, the SA is discarded as invalid.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Autodetect</i> (default value): Your device detects and uses the mode supported by the remote terminal. • <i>Inactive</i>: Your device sends and expects no heartbeat. Set this option if you use devices from other manufacturers. • <i>Heartbeats (Expect only)</i>: Your device expects a heartbeat from the peer but does not send one itself. • <i>Heartbeats (Send only)</i>: Your device expects no heartbeat from the peer, but sends one itself. • <i>Heartbeats (Send &Expect)</i>: Your device expects a heartbeat from the peer and sends one itself. • <i>Dead Peer Detection</i>: Use DPD (dead peer detection) in accordance with RFC 3706. DPD uses a request-reply protocol to check the availability of the remote terminal and can be configured independently on both sides. This option only checks the availability of the peer if data is to be sent to it. • <i>Dead Peer Detection (Idle)</i>: Use DPD (dead peer detection) in accordance with RFC 3706. DPD uses a request-reply protocol to check the availability of the remote terminal and can be configured independently on both sides. This option is used to carry out a check at certain intervals depending on forthcoming data transfers. <p>Only for Phase-1 (IKEv2) Parameters</p> <p>Enable or disable alive check.</p> <p>The function is enabled by default.</p>
Block Time	<p>Define how long a peer is blocked for tunnel setups after a</p>

Field	Description
	<p>phase 1 tunnel setup has failed. This only affects locally initiated setup attempts.</p> <p>Possible values are <i>-1</i> to <i>86400</i> (seconds); <i>-1</i> means the value in the default profile is used and <i>0</i> means that the peer is never blocked.</p> <p>The default value is <i>30</i>.</p>
<p>NAT Traversal</p>	<p>NAT Traversal (NAT-T) also enables IPSec tunnels to be opened via one or more devices on which network address translation (NAT) is activated.</p> <p>Without NAT-T, incompatibilities may arise between IPSec and NAT (see RFC 3715, section 2). These primarily prevent the setup of an IPSec tunnel from a host within a LANs and behind a NAT device to another host or device. NAT-T enables these kinds of tunnels without conflicts with NAT device, activated NAT is automatically detected by the IPSec Daemon and NAT-T is used.</p> <p>Only for <i>IKEv1 profiles</i></p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Enabled</i> (default value): NAT Traversal is enabled. • <i>Disabled</i>: NAT Traversal is disabled. • <i>Force</i>: The device always behaves as it would if NAT were in use. <p>Only for <i>IKEv2 profiles</i></p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
<p>CA Certificates</p>	<p>Only for Phase-1 (IKE) Parameters</p> <p>Only for Authentication Method = <i>DSA Signature, RSA Signature or RSA Encryption</i></p> <p>If you enable the Trust the following CA certificates option, you can select up to three CA certificates that are accepted for this profile.</p>

Field	Description
	This option can only be configured if certificates are loaded.

13.1.3 Phase-2 Profiles

You can define profiles for phase 2 of the tunnel setup just as for phase 1.

In the **VPN->IPSec->Phase-2 Profiles** menu, a list of all configured IPSec phase 2 profiles is displayed.

In the **Default** column, you can mark the profile to be used as the default profile.

13.1.3.1 New

Choose the **New** button to create additional profiles.

The menu **VPN->IPSec->Phase-2 Profiles->New** consists of the following fields:

Fields in the Phase-2 (IPSEC) Parameters menu

Field	Description
Description	Enter a description that uniquely identifies the profile. The maximum length of the entry is 255 characters.
Proposals	In this field, you can select any combination of encryption and message hash algorithms for IKE phase 2 on your default. The combination of six encryption algorithms and two message hash algorithms gives 12 possible values in this field. Encryption algorithms (Encryption): <ul style="list-style-type: none"> • <i>3DES</i> (default value): 3DES is an extension of the DES algorithm with an effective key length of 112 bits, which is rated as secure. It is the slowest algorithm currently supported. • <i>-- ALL --</i>: All options can be used. • <i>AES</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. The partner's AES key length is used here. If this has also selected the parameter <i>AES</i> , a key length of 128 bits is used. • <i>AES-128</i>: Rijndael has been nominated as AES due to its

Field	Description
	<p>fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 128 bits.</p> <ul style="list-style-type: none"> • <i>AES-192</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 192 bits. • <i>AES-256</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 256 bits. • <i>Twofish</i>: Twofish was a final candidate for the AES (Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower. • <i>Blowfish</i>: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish. • <i>CAST</i>: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES. • <i>DES</i>: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits. <p>Hash algorithms (Authentication):</p> <ul style="list-style-type: none"> • <i>MD5</i> (default value): MD5 (Message Digest #5) is an older hash algorithm. It is used with a 96 bit digest length for IPsec. • <i>-- ALL --</i>: All options can be used. • <i>SHA1</i>: SHA1 (Secure Hash Algorithm #1) is a hash algorithm developed by NSA (United States National Security Association). It is rated as secure, but is slower than MD5. It is used with a 96 bit digest length for IPsec. <p>Note that RipeMD 160 and Tiger 192 are not available for message hashing in phase 2.</p>
Use PFS Group	<p>As PFS (Perfect Forward Secrecy) requires another Diffie-Hellman key calculation to create new encryption material, you must select the exponentiation features. If you enable PFS (<i>Enabled</i>), the options are the same as for the configuration of DH Group in the VPN->IPSec->Phase-1 Profiles menu. PFS is used to protect the keys of a renewed phase 2 SA, even if</p>

Field	Description
	<p>the keys of the phase 1 SA have become known.</p> <p>The field has the following options:</p> <ul style="list-style-type: none"> • <i>1 (768 Bit)</i>: During the Diffie-Hellman key calculation, modular exponentiation at 768 bits is used to create the encryption material. • <i>2 (1024 Bit)</i> (default value): During the Diffie-Hellman key calculation, modular exponentiation at 1024 bits is used to create the encryption material. • <i>5 (1536 Bit)</i>: During the Diffie-Hellman key calculation, modular exponentiation at 1536 bits is used to create the encryption material.
Lifetime	<p>Define how the lifetime is defined that will expire before phase 2 SAs need to be renewed.</p> <p>The new SAs are negotiated shortly before expiry of the current SAs. As for RFC 2407, the default value is eight hours, which means the key must be renewed once eight hours have elapsed.</p> <p>The following options are available for defining the Lifetime:</p> <ul style="list-style-type: none"> • Input in Seconds: Enter the lifetime for phase 2 key in seconds. The value can be a whole number from 0 to 2147483647. The default value is 7200. • Input in kBytes: Enter the lifetime for phase 2 keys as amount of data processed in Kbytes. The value can be a whole number from 0 to 2147483647. The default value is 0. <p>Rekey after: Specify the percentage in the course of the lifetime at which the phase 2 keys are to be regenerated.</p> <p>The percentage entered is applied to both the lifetime in seconds and the lifetime in Kbytes.</p> <p>The default value is 80 %.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
IP Compression	<p>Select whether compression is to be activated before data encryption. If data is compressed effectively, this can result in higher performance and a lower volume of data to be transferred. In the case of fast lines or data that cannot be compressed, you are advised against using this option as the performance can be significantly affected by the increased effort during compression.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Alive Check	<p>Select whether and how IPSec heartbeats are used.</p> <p>A bintec elmeg IPSec heartbeat is implemented to determine whether or not a Security Association (SA) is still valid. This function sends and receives signals every 5 seconds, depending on the configuration. If these signals are not received after 20 seconds, the SA is discarded as invalid.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Autodetect</i> (default value): Automatic detection of whether the remote terminal is a bintec elmeg device. If it is, <i>Heartbeats (Send &Expect)</i> (for a remote terminal with bintec elmeg) or <i>Inactive</i> (for a remote terminal without bintec elmeg) is set. • <i>Inactive</i>: Your device sends and expects no heartbeat. Set this option if you use devices from other manufacturers. • <i>Heartbeats (Expect only)</i>: Your device expects a heartbeat from the peer but does not send one itself. • <i>Send</i>: Your device expects no heartbeat from the peer, but sends one itself. • <i>Heartbeats (Send &Expect)</i>: Your device expects a heartbeat from the peer and sends one itself.
Propagate PMTU	<p>Select whether the PMTU (Path Maximum Transfer Unit) is to be propagated during phase 2.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

13.1.4 XAUTH Profiles

In the **XAUTH Profiles** menu a list of all XAUTH profiles is displayed.

Extended Authentication for IPSec (XAuth) is an additional authentication method for IPSec tunnel users.

The gateway can take on two different roles when using XAuth as it can act as a server or as a client:

- As a server the gateway requires a proof of authorisation.
- As a client the gateway provides proof of authorisation.

In server mode multiple users can obtain authentication via XAuth, e.g. users of Apple iPhones. Authorisation is verified either on the basis of a list or via a Radius Server. If using a one time password (OTP), the password check can be carried out by a token server (e.g. SecOVID from Kobil), which is installed behind the Radius Server. If a company's headquarters is connected to several branches via IPSec, several peers can be configured. A specific user can then use the IPSec tunnel over various peers depending on the assignment of various profiles. This is useful, for example, if an employee works alternately in different branches, if each peer represents a branch and if the employee wishes to have on-site access to the tunnel.

XAuth is carried out once IPSec IKE (Phase 1) has been completed successfully and before IKE (Phase 2) begins.

If XAuth is used together with IKE Config Mode, the transactions for XAuth are carried out before the transactions for IKE Config Mode.

13.1.4.1 New

Choose the **New** button to create additional profiles.

The **VPN->IPSec->XAUTH Profiles ->New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter a description for this XAuth profile.
Role	Select the role of the gateway for XAuth authentication. Possible values:


Field	Description
	<ul style="list-style-type: none"> • <i>Server</i> (default value): The gateway requires a proof of authorisation. • <i>Client</i>: The gateway provides proof of authorisation.
Mode	<p>Only for Role = <i>Server</i></p> <p>Select how authentication is carried out.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>RADIUS</i> (default value): Authentication is carried out via a Radius server. It is configured in the System Management->Remote Authentication->RADIUS menu and selected in the RADIUS Server Group ID field. • <i>Local</i>: Authentication is carried out via a local list.
Name	<p>Only for Role = <i>Client</i></p> <p>Enter the authentication name of the client.</p>
Password	<p>Only for Role = <i>Client</i></p> <p>Enter the authentication password.</p>
RADIUS Server Group ID	<p>Only for Role = <i>Server</i></p> <p>Select the desired list in System Management->Remote Authentication->RADIUS configured RADIUS group.</p>
Users	<p>Only for Role = <i>Server</i> and Mode = <i>Local</i></p> <p>If your gateway is configured as an XAuth server, the clients can be authenticated via a locally configured user list. Define the members of the user group of this XAUTH profile here by entering the authentication name of the client (Name) and the authentication password (Password). Add new members with Add.</p>

13.1.5 IP Pools

In the **IP Pools** menu a list of all IP pools for your configured IPSec connections is displayed.

If for an IPSec peer you have set **IP Address Assignment** *IKE Config Mode Server*, you must define the IP pools here from which the IP addresses are assigned.

13.1.5.1 Edit or New

Choose the **New** button to set up new IP address pools. Choose the  icon to edit existing entries.

The menu **VPN->IPSec->IP Pools->New** consists of the following fields:


Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	<p>Primary: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool.</p> <p>Secondary: Optionally, enter the IP address of an alternative DNS server.</p>

13.1.6 Options

The menu **VPN->IPSec->Options** consists of the following fields:

Fields in the Global Options menu

Field	Description
Enable IPSec	<p>Select whether you want to activate IPSec.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is active as soon as an IPSec Peer is configured.</p>
Delete complete IPSec configuration	<p>If you click the  icon, delete the complete IPSec configuration of your device.</p> <p>This cancels all settings made during the IPSec configuration. Once the configuration is deleted, you can start with a com-</p>

Field	Description
	<p>pletely new IPSec configuration.</p> <p>You can only delete the configuration if Enable IPSec = not activated.</p>
IPSec Debug Level	<p>Select the priority of the syslog messages of the IPSec subsystem to be recorded internally.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Emergency</i> (highest priority) • <i>Alert</i> • <i>Critical</i> • <i>Error</i> • <i>Warning</i> • <i>Notice</i> • <i>Information</i> • <i>Debug</i> (default value, lowest priority) <p>Syslog messages are only recorded internally if they have a higher or identical priority to that indicated, i.e. all messages generated are recorded at syslog level "debug".</p>

The **Advanced Settings** menu is for adapting certain functions and features to the special requirements of your environment, i.e. mostly interoperability flags are set. The default values are globally valid and enable your system to work correctly to other bintec elmeg devices, so that you only need to change these values if the remote terminal is a third-party product or you know special settings are necessary. These may be needed, for example, if the remote end operates with older IPSec implementations.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
IPSec over TCP	<p>Determine whether IPSec over TCP is to be used.</p> <p>IPSec over TCP is based on NCP pathfinder technology. This technology insures that data traffic (IKE, ESP, AH) between peers is integrated into a pseudo HTTPS session.</p> <p>The function is enabled with <i>Enabled</i>.</p>

Field	Description
	The function is disabled by default.
Send Initial Contact Message	<p>Select whether IKE Initial Contact messages are to be sent during IKE (phase 1) if no SAs with a peer exist.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Sync SAs with ISP interface state	<p>Select whether all SAs are to be deleted whose data traffic was routed via an interface on which the status has changed from <i>Up</i> to <i>Down</i>, <i>Dormant</i> or <i>Blocked</i>.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Use Zero Cookies	<p>Select whether zeroed ISAKMP Cookies are to be sent.</p> <p>These are equivalent to the SPI (Security Parameter Index) in IKE proposals; as they are redundant, they are normally set to the value of the negotiation currently in progress. Alternatively, your device can use zeroes for all values of the cookie. In this case, select <i>Enabled</i>.</p>
Zero Cookie Size	<p>Only for Use Zero Cookies = enabled.</p> <p>Enter the length in bytes of the zeroed SPI used in IKE proposals.</p> <p>The default value is <i>32</i>.</p>
Dynamic RADIUS Authentication	<p>Select whether RADIUS authentication is to be activated via IPsec.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

Fields in the PKI Handling Options menu

Field	Description
Ignore Certificate Request Payloads	Select whether certificate requests received from the remote end during IKE (phase 1) are to be ignored.

Field	Description
	<p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Send Certificate Request Payloads	<p>Select whether certificate requests are to be sent during IKE (phase 1).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Send Certificate Chains	<p>Select whether complete certificate chains are to be sent during IKE (phase 1).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p> <p>Deactivate this function if you do not wish to send the peer the certificates of all levels (from your level to the CA level).</p>
Send CRLs	<p>Select whether CRLs are to be sent during IKE (phase 1).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Send Key Hash Payloads	<p>Select whether key hash payloads are to be sent during IKE (phase 1).</p> <p>In the default setting, the public key hash of the remote end is sent together with the other authentication data. Only applies for RSA encryption. Activate this function with <i>Enabled</i> to suppress this behaviour.</p>

13.2 L2TP

The layer 2 tunnel protocol (L2TP) enables PPP connections to be tunnelled via a UDP connection.

Your bintec elmeg device supports the following two modes:

- L2TP LNS Mode (L2TP Network Server): for incoming connections only
- L2TP LAC Mode (L2TP Access Concentrator): for outgoing connections only

Note the following when configuring the server and client: An L2TP tunnel profile must be created on each of the two sides (LAC and LNS). The corresponding L2TP tunnel profile is used on the initiator side (LAC) to set up the connection. The L2TP tunnel profile is needed on the responder side (LNS) to accept the connection.

13.2.1 Tunnel Profiles

A list of all configured tunnel profiles is displayed in the **VPN->L2TP->Tunnel Profiles** menu.

13.2.1.1 New

Choose the **New** button to create additional tunnel profiles.

The menu **VPN->L2TP->Tunnel Profiles ->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	<p>Enter a description for the current profile.</p> <p>The device automatically names the profiles <i>L2TP</i> and numbers them, but the value can be changed.</p>
Local Hostname	<p>Enter the host name for LNS or LAC.</p> <ul style="list-style-type: none"> • <i>LAC</i>: The local hostname is used in outgoing tunnel setup messages to identify this device and is associated with the remote hostname of a tunnel profile configured on the LNS. These tunnel setup messages are SCCRQs (Start Control Connection Request) sent from the LAC and SCCRPs (Start Control Connection Reply) sent from the LNS. • <i>LNS</i>: Is the same as the value for Remote Hostname of the incoming tunnel setup message from the LAC.
Remote Hostname	<p>Enter the host name of the LNS or LAC.</p> <ul style="list-style-type: none"> • <i>LAC</i>: Defines the value for Local Hostname of the LNS (contained in the SCCRQs received from the LNS and the SCCRPs received from the LAC). A Local Hostname configured in the LAC must match Remote Hostname configured for the intended profile in the LNS and vice versa. • <i>LNS</i>: Defines the Local Hostname of the LAC. If the Remote Hostname field remains empty on the LNS, the related

Field	Description
	profile qualifies as the standard entry and is used for all incoming calls for which a profile with a matching remote hostname cannot be found.
Password	<p>Enter the password to be used for tunnel authentication. Authentication between LAC and LNS takes place in both directions, i.e. the LNS checks the Local Hostname and the Password contained in the SCCRQ of the LAC and compares them with those specified in the relevant profile. The LAC does the same with the fields of the SCCRP of the LNS.</p> <p>If this field remains empty, authentication data in the tunnel setup messages are not sent and are ignored.</p>

Fields in the LAC Mode Parameters menu

Field	Description
Remote IP Address	<p>Enter the fixed IP address of the LNS used as the destination address for connections based on this profile.</p> <p>The destination must be a device that can behave like an LNS.</p>
UDP Source Port	<p>Enter how the port number to be used as the source port for all outgoing L2TP connections based on this profile is to be determined.</p> <p>By default, the Fixed option is disabled, which means that ports are dynamically assigned to the connections that use this profile.</p> <p>If you want to enter a fixed port, enable the <i>Fixed</i> option. Select this option if you encounter problems with the firewall or NAT.</p> <p>The available values are <i>0</i> to <i>65535</i>.</p>
UDP Destination Port	<p>Enter the destination port number to be used for all calls based on this profile. The remote LNS that receives the call must monitor this port on L2TP connections.</p> <p>Possible values are <i>0</i> to <i>65535</i>.</p> <p>The default value is <i>1701</i> (RFC 2661).</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Local IP Address	<p>Enter the IP address to be used as the source address for all L2TP connections based on this profile.</p> <p>If this field is left empty, your device uses the IP address of the interface used to reach the remote IP Address by the L2TP tunnel.</p>
Hello Intervall	<p>Enter the interval (in seconds) between the sending of two L2TP HELLO messages. These messages are used to keep the tunnel open.</p> <p>The available values are <i>0</i> to <i>255</i>, the default value is <i>30</i>. The value <i>0</i> means that no L2TP HELLO messages are sent.</p>
Minimum Time between Retries	<p>Enter the minimum time (in seconds) that your device waits before resending a L2TP control packet for which it received no response.</p> <p>The wait time is dynamically extended until it reaches the Maximum Time between Retries. The available values are <i>1</i> to <i>255</i>, the default value is <i>1</i>.</p>
Maximum Time between Retries	<p>Enter the maximum time (in seconds) that your device waits before resending a L2TP control packet for which it received no response.</p> <p>The available values are <i>8</i> to <i>255</i>, the default value is <i>16</i>.</p>
Maximum Retries	<p>Enter the maximum number of times your device is to try to re-send the L2TP control packet for which is received no response.</p> <p>The available values are <i>8</i> to <i>255</i>, the default value is <i>5</i>.</p>
Data Packets Sequence Numbers	<p>Select whether your device is to use sequence numbers for data packets sent through a tunnel on the basis of this profile.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

13.2.2 Users

A list of all configured interface L2TP partners is displayed in the **VPN->L2TP->Users** menu.

13.2.2.1 New

Choose the **New** button to set up new L2TP partners.

The menu **VPN->L2TP->Users->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	<p>Enter a name for uniquely identifying the L2TP partner.</p> <p>The first character in this field must not be a number No special characters or umlauts must be used. The maximum length of the entry is 25 characters.</p>
Connection Type	<p>Select whether the L2TP partner is to take on the role of the L2TP network server (LNS) or the functions of a L2TP access concentrator client (LAC client).</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>LNS</i> (default value): If you select this option, the L2TP partner is configured so that it accepts L2TP tunnels and restores the encapsulated PPP traffic flow. • <i>LAC</i>: If you select this option, the L2TP partner is configured so that it encapsulates a PPP traffic flow in L2TP and sets up a L2TP tunnel to a remote LNS.
Tunnel Profile	<p>Only for Connection Type = <i>LAC</i></p> <p>Select a profile created in the Tunnel Profile menu for the connection to this L2TP partner.</p>
User Name	Enter the code of your device.
Password	Enter the password.
Always on	Select whether the interface should always be activated.

Field	Description
	<p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Connection Idle Timeout	<p>Only if Always on is disabled</p> <p>Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection.</p> <p>Possible values are <i>0</i> to <i>3600</i> (seconds). <i>0</i> deactivates the short hold. The default value is <i>300</i>.</p>

Fields in the IP Mode and Routes menu

Field	Description
IP Address Mode	<p>Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Static</i> (default value): You enter a static IP address. • <i>Provide IP Address</i>: Only for Connection Type = <i>LNS</i>. Your device dynamically assigns an IP address to the remote terminal. • <i>Get IP Address</i>: Only for Connection Type = <i>LAC</i>. Your device is dynamically assigned an IP address.
Default Route	<p>Only for IP Address Mode = <i>Get IP Address</i> and <i>Static</i></p> <p>Select whether the route to this connection partner is to be defined as the default route.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Create NAT Policy	<p>Only for IP Address Mode = <i>Get IP Address</i> and <i>Static</i></p>

Field	Description
	<p>Specify whether Network Address Translation (NAT) is to be activated for this connection.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
IP Assignment Pool (IPCP)	<p>Only for IP Address Mode = <i>Provide IP Address</i></p> <p>Select an IP pool configured in the WAN->Internet + Dialup->IP Pools menu.</p>
Local IP Address	<p>Only for IP Address Mode = <i>Static</i></p> <p>Enter the WAN IP address of your device.</p>
Route Entries	<p>Only for IP Address Mode = <i>Static</i></p> <p>Enter Remote IP Address and Netmask of the LANs for L2TP partners and the corresponding Metric. Add new entries with Add.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Block after connection failure for	<p>Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed.</p> <p>The default value is <i>300</i>.</p>
Authentication	<p>Select the authentication protocol for this L2TP partner.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>PAP/CHAP/MS-CHAP</i> (default value): Primarily run CHAP, on denial, the authentication protocol required by the PPTP partner. (MSCHAP version 1 or 2 possible.) • <i>PAP</i>: Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.

Field	Description
	<ul style="list-style-type: none"> • <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP. • <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only. • <i>None</i>: Some providers use no authentication. In this case, select this option.
Encryption	<p>If necessary, select the type of encryption that should be used for data traffic to the L2TP partner. This is only possible if STAC or MS-STAC compression is not activated for the connection. If Encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i>: MPP encryption is not used. • <i>Enabled</i> (default value): MPP encryption V2 with 128 bit is used to RFC 3078. • <i>Windows compatible</i>: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
LCP Alive Check	<p>Select whether the availability of the remote terminal is to be checked by sending LCP echo requests or replies. This is recommended for leased lines, PPTP and L2TP connections.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Prioritize TCP ACK Packets	<p>Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

Fields in the IP Options menu

Field	Description
OSPF Mode	Select whether and how routes are propagated via the interface and/or OSPF protocol packets are sent.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Passive</i> (default value): OSPF is not activated for this interface, i.e. no routes are propagated or OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces. • <i>Active</i>: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface. • <i>Inactive</i>: OSPF is disabled for this interface.
Proxy ARP Mode	<p>Select whether your device is to respond to ARP requests from its own LAN on behalf of the specific L2TP partner.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Inactive</i> (default value): Deactivates Proxy ARP for this L2TP partner. • <i>Up or Dormant</i>: Your device only responds to an ARP request if the status of the connection to the L2TP partner is <i>Up</i> (active) or <i>Dormant</i>. In the case of <i>Idle</i>, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • <i>Up only</i>: Your device responds to an ARP request only if the status of the connection to the L2TP partner is <i>Up</i> (active), i.e. a connection already exists to the L2TP partner.
DNS Negotiation	<p>Select whether your device receives IP addresses for Primary DNS Server und Secondary DNS Server and WINS Server Primary and Secondary from the L2TP partner or sends these to the L2TP partner.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

13.2.3 Options

The menu **VPN->L2TP->Options** consists of the following fields:

Fields in the Global Options menu

Field	Description
UDP Destination Port	<p>Enter the port to be monitored by the LNS on incoming L2TP tunnel connections.</p> <p>Available values are all whole numbers from 1 to 65535, the default value is 1701, as specified in RFC 2661.</p>
UDP Source Port Selection	<p>Select whether the LNS should only use the monitored port (UDP Destination Port) as the local source port for the L2TP connection.</p> <p>The function is enabled with <i>Fixed</i>.</p> <p>The function is disabled by default.</p>

13.3 PPTP

The Point-to-Point Tunneling Protocol (=PPTP) can be used to set up an encrypted PPTP tunnel to provide security for data traffic over an existing IP connection.

First a connection to an ISP (=Internet Service Provider) is set up at both sites. Once these connections are available, a tunnel is set up to the PPTP partner over the Internet using PPTP.

The PPTP subsystem sets up a control connection between the endpoints of the tunnel. This is used to send control data to set up, keep alive and terminate the connection between the two PPTP tunnel end-points. As soon as this control connection is set up, the PPTP transfers the traffic data packed in GRE packets (GRE = Generic Routing Encapsulation).

13.3.1 PPTP Tunnels

A list of all PPTP tunnels is displayed in the **PPTP Tunnels** menu.

13.3.1.1 New

Click on **New** to set up further PPTP partners.

The **VPN->PPTP->PPTP Tunnels->New** menu consists of the following fields:

Fields in the PPTP Partner Parameters menu

Field	Description
Description	<p>Enter a unique name for the tunnel.</p> <p>The first character in this field must not be a number No special characters or umlauts must be used.</p>
PPTP Mode	<p>Enter the role to be assigned to the PPTP interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>PNS</i> (default value): this assigns the PPTP interface the role of PPTP server. • <i>Windows Client Mode</i>: This assigns the PPTP interface the role of PPTP client.
User Name	Enter the user name.
Password	Enter the password.
Always on	<p>Select whether the interface should always be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Connection Idle Timeout	<p>Only if Always on is disabled.</p> <p>Enter the idle interval in seconds. This determines how many seconds should pass between sending the last traffic data packet and clearing the connection.</p> <p>Possible values are 0 to 3600 (seconds). 0 deactivates the timeout.</p> <p>The default value is 300.</p> <p>Example: 10 for FTP transmission, 20 for LAN-to-LAN transmission, 90 for Internet connections.</p>
Remote PPTP IP Address	<p>Only for PPTP Mode = <i>PNS</i></p> <p>Enter the IP address of the PPTP partner.</p>
Remote PPTP IP Address/Host Name	<p>Only for PPTP Mode = <i>Windows Client Mode</i></p> <p>Enter the IP address of the PPTP partner.</p>

Fields in the IP Mode and Routes menu

Field	Description
IP Address Mode	<p>Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Static</i> (default value): You enter a static IP address. • <i>Provide IP Address</i>: Only for PPTP Mode = PNS: Your device dynamically assigns an IP address to the remote terminal. • <i>Get IP Address</i>: Only for PPTP Mode = Windows Client Mode: Your device is dynamically assigned an IP address.
Default Route	<p>Only if IP Address Mode = Static</p> <p>Select whether the route to this connection partner is to be defined as the default route.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Create NAT Policy	<p>Only if IP Address Mode = Static</p> <p>When you configure an PPTP connection, specify whether Network Address Translation (NAT) is to be enabled.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Local IP Address	<p>Only for IP Address Mode = Static</p> <p>Assign the IP address from your LAN to the PPTP interface which is to be used as your device's internal source address.</p>
Route Entries	<p>Only if IP Address Mode = Static</p> <p>Define routing entries for this connection partner.</p> <ul style="list-style-type: none"> • <i>Remote IP Address</i>: IP address of the destination host or LAN. • <i>Netmask</i>: Netmask for Remote IP Address

Field	Description
	<ul style="list-style-type: none"> • <i>Metric</i>: The lower the value, the higher the priority of the route (possible values 0 . . . 15). The default value is 1.
IP Assignment Pool (IPCP)	<p>Only if PPTP Mode = <i>PNS</i>, IP Address Mode = <i>Provide IP Address</i></p> <p>Select a IP pool configured in the VPN->PPTP->IP Pools menu.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Block after connection failure for	<p>Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed.</p> <p>The default value is 300.</p>
Authentication	<p>Select the authentication protocol for this PPTP partner.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>PAP</i>: Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted. • <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP. • <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • <i>PAP/CHAP/MS-CHAP</i>: Give priority to CHAP, if refused use the authentication protocol requested by the PPTP partner. (MSCHAP version 1 or 2 possible.) • <i>MS-CHAPv2</i> (default value): Run MS-CHAP version 2 only. • <i>None</i>: Some providers use no authentication. In this case, select this option.
Encryption	<p>If necessary, select the type of encryption that should be used for data traffic to the connection partner. If Encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i>: MPP encryption is not used. • <i>Enabled</i> (default value): MPP encryption V2 with 128 bit is used to RFC 3078. • <i>Windows compatible</i>: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
Compression	<p>If necessary, select the type of encryption that should be used for data traffic to the connection partner. If encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i> (default value): Encryption is not used. • <i>STAC</i> • <i>MS-STAC</i> • <i>MPPC</i>: Microsoft Point-to-Point Compression
LCP Alive Check	<p>Select whether the availability of the remote terminal is to be checked by sending LCP echo requests or replies. This is recommended for leased lines, PPTP and L2TP connections.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

Fields in the IP Options menu

Field	Description
OSPF Mode	<p>Select whether and how routes are propagated via the interface and/or OSPF protocol packets are to be sent.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Passive</i> (default value): OSPF is not activated for this interface, i.e. no routes are propagated or OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces. • <i>Active</i>: OSPF is activated for this interface, i.e. routes are

Field	Description
	<p>propagated or OSPF protocol packets sent over this interface.</p> <ul style="list-style-type: none"> <i>Inactive</i>: OSPF is disabled for this interface.
Proxy ARP Mode	<p>Select whether your device is to answer APR requests from your LAN on behalf of the specific PPTP partner.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <i>Inactive</i> (default value): Disables Proxy-ARP (Address Resolution Protocol) for this PPTP partner. <i>Up or Dormant</i>: Your device only responds to an ARP request if the status of the connection to the PPTP partner is <i>Up</i> (active) or <i>Dormant</i>. In the case of <i>Idle</i>, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. <i>Up only</i>: Your device answers an APR request only if the status of the connection to the PPTP partner is <i>Active</i>, i.e. if a connection to the PPTP partner has already been established.
DNS Negotiation	<p>Select whether your device receives IP addresses for Primary DNS Server and Secondary DNS Server from the PPTP partner or sends these to the PPTP partner.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

Fields in the PPTP Callback menu

Field	Description
Callback	<p>Enables a PPTP tunnel through the Internet to be set up with a PPTP partner, even if the partner is currently inaccessible. As a rule, the PPTP partner will be requested by means of an ISDN call to go online and set up a PPTP connection.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>Note that you must activate the relevant option on the gateways of both partners. An ISDN connection is usually required</p>

Field	Description
	for this function. Without ISDN, callback is only to be activated in special applications.
Incoming ISDN Number	Only if Callback is enabled. Enter the ISDN number from which the remote device calls the local device (calling party number).
Outgoing ISDN Number	Only if Callback is enabled. Enter the ISDN number with which the local device calls the remote device calls (called party number).

Fields in the Dial Port Selection (only if callback = activated)

Field	Description
Selected Ports	Enter the ISDN port over which callback is carried out. Possible values: <ul style="list-style-type: none"> • <i>All Ports</i>: The callback is routed over an available ISDN port. • <i>Specify port</i>: In Specific Ports You can select the required ISDN port.
Specific Ports	Only for Selected Ports = <i>Specify port</i> , you can select additional ports with Add .

13.3.2 Options

In this menu, you can make general settings of the global PPTP profile.

The **VPN->PPTP->Options** menu consists of the following fields:

Fields in the Global Options menu

Field	Description
GRE Window Adaption	Select whether the GRE Window Adaptation is to be enabled. This adaptation only becomes necessary if you have installed service pack 1 from Microsoft Windows XP. Since, in SP 1, Microsoft has changed the confirmation algorithm in the GRE protocol, the automatic window adaptation for GRE must be turned off for bintec elmeg devices.

Field	Description
	<p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
GRE Window Size	<p>Enter the maximum number of GRE packets that can be sent without confirmation.</p> <p>Windows XP uses a higher initial reception window in the GRE, which is why the maximum send window size must be adjusted here by the GRE Window Size value. Possible values are <i>0</i> to <i>256</i>.</p> <p>The default value is <i>0</i>.</p>
Max. incoming control connections per remote IP Address	Enter the maximum number of control connections.

13.3.3 IP Pools


The **IP Pools** menu displays a list of all IP pools for PPTP connections.

Your device can operate as a dynamic IP address server for PPTP connections. You can use this function by providing one or more pools of IP addresses. These IP addresses can be assigned to dialling-in connection partners for the duration of the connection.

Any host routes entered always have priority over IP addresses from the address pools. This means if an incoming call has been authenticated, your device first checks whether a host route is entered in the routing table for this caller. If not, your device can allocate an IP address from an address pool (if available). If address pools have more than one IP address, you cannot specify which connection partner receives which address. The addresses are initially assigned in order. If a new dial-in takes place within an interval of one hour, an attempt is made to allocate the same IP address assigned to this partner the last time.

Choose the **Add** button to set up new IP pools.

13.3.3.1 Edit or New

Choose the **New** button to set up new IP address pools. Choose the  icon to edit existing entries.

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	<p>Primary: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool.</p> <p>Secondary: Optionally, enter the IP address of an alternative DNS server.</p>

13.4 GRE

Generic Routing Encapsulation (GRE) is a network protocol that encapsulates other protocols and transports them in the form of IP tunnels to the specified recipients.

The specification of the GRE protocol is available in two versions:

- GRE V.1 for use in PPTP connections (RFC 2637, configuration in the **PPTP** menu)
- GRE V.0 (RFC 2784) for general encapsulation using GRE

In this menu you can configure a virtual interface for using GRE V.0. The data traffic routed over this interface is then encapsulated using GRE and sent to the specified recipient.

13.4.1 GRE Tunnels

A list of all configured GRE tunnels is displayed in the **VPN->GRE->GRE Tunnels** menu.

13.4.1.1 New

Choose the **New** button to set up new GRE tunnels.

The **VPN->GRE->GRE Tunnels->New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter a description for the GRE tunnel.
Local GRE IP Address	Enter the source IP address of the GRE packets to the GRE

Field	Description
	<p>partner.</p> <p>If no IP address is given (this corresponds to IP address 0.0.0.0), the source IP address of the GRE packets is selected automatically from one of the addresses of the interface via which the GRE partner is reached.</p>
Remote GRE IP Address	Enter the target IP address of the GRE packets to the GRE partner.
Default Route	<p>If you enable the Default Route, all data is automatically routed to one connection.</p> <p>The function is disabled by default.</p>
Local IP Address	Here, enter the (LAN-side) IP address that is to be used as your device's source address for your own packets through the GRE tunnel.
Route Entries	<p>Define other routing entries for this connection partner.</p> <p>Add new entries with Add.</p> <ul style="list-style-type: none"> • <i>Remote IP Address</i>: IP address of the destination host or network. • <i>Netmask</i>: Netmask for Remote IP Address If no entry is made, your device uses a default netmask. • <i>Metric</i>: The lower the value, the higher the priority of the route (range of values 0... 15). The default value is 1.
MTU	<p>Enter the maximum packet size (Maximum Transfer Unit, MTU) in bytes that is allowed for the GRE connection between the partners.</p> <p>Possible values are 1 to 8192.</p> <p>The default value is 1500.</p>
Use key	<p>Enable the key input for the GRE connection, which makes it possible to distinguish between several parallel GRE connections between two GRE partners (see RFC 1701).</p> <p>The identification is enabled with <i>Enabled</i></p>

Field	Description
	The function is disabled by default.
Key Value	Only if Use key is enabled. Enter the GRE connection key. Possible values are 0 to 2147483647. The default value is 0.

Chapter 14 Firewall

The Stateful Inspection Firewall (SIF) provided for bintec elmeg gateways is a powerful security feature.

The SIF with dynamic packet filtering has a decisive advantage over static packet filtering: The decision whether or not to send a packet cannot be made solely on the basis of source and destination addresses or ports but also using dynamic packet filtering based on the state of the connection to a partner.

This means packets that belong to an already active connection can also be forwarded. The SIF also accepts packets that belong to an "affiliated connection". The negotiation of an FTP connection takes place over port 21, for example, but the actual data exchange can take place over a completely different port.

SIF and other security features

The Stateful Inspection Firewall fits into the existing security architecture of bintec elmeg. The configuration work for the SIF is comparatively straightforward with systems like Network Address Translation (NAT) and IP Access Lists (IPAL).

As SIF, NAT and IPAL are active in the system simultaneously, attention must be given to possible interaction: If any packet is rejected by one of the security instances, this is done immediately. This is irrelevant whether another instance would accept it or not. Your need for security features should therefore be accurately analysed.

The essential difference between SIF and NAT/IPAL is that the rules for the SIF are generally applied globally, i.e. not restricted to one interface.

In principle, the same filter criteria are applied to the data traffic as those used in NAT and IPAL:

- Source and destination address of the packet (with an associated netmask)
- Service (preconfigured, e.g. Echo, FTP, HTTP)
- Protocol
- Port number(s)

To illustrate the differences in packet filtering, a list of the individual security instances and their method of operation is given below.

NAT

One of the basic functions of NAT is the translation of the local IP addresses of your LAN into the global IP addresses you are assigned by your ISP and vice versa. All connections initiated externally are first blocked, i.e. every packet your device cannot assign to an existing connection is rejected. This means that a connection can only be set up from inside to outside. Without explicit permission, NAT rejects every access from the WAN to the LAN.

IP Access Lists

Here, packets are allowed or rejected exclusively on the basis of the criteria listed above, i.e. the state of the connection is not considered (except for **Services** = *TCP*).

SIF

The SIF sorts out all packets that are not explicitly or implicitly allowed. The result can be a "deny", in which case no error message is sent to the sender of the rejected packet, or a "reject", where the sender is informed of the packet rejection.

The incoming packets are processed as follows:

- The SIF first checks if an incoming packet can be assigned to an existing connection. If so, it is forwarded. If the packet cannot be assigned to an existing connection, a check is made to see if a suitable connection is expected (e.g. as affiliated connection of an existing connection). If so, the packet is also accepted.
- If the packet cannot be assigned to any existing or expected connection, the SIF filter rules are applied: If a deny rule matches the packet, the packet is rejected without sending an error message to the sender of the packet; if a reject rule matches, the packet is rejected and an ICMP Host Unreachable message sent to the sender of the packet. The packet is only forwarded if an accept rule matches.
- All packets without matching rules are rejected without sending an error message to the sender when all the existing rules have been checked (=default behaviour).


14.1 Policies


14.1.1 Filter Rules

The default behaviour with **Action** = *Access* consists of two implicit filter rules: If an incoming packet can be assigned to an existing connection and if a suitable connection is expected (e.g. such as an affiliated connection of an existing connection), the packet is allowed.

The sequence of filter rules in the list is relevant: The filter rules are applied to each packet in succession until a rule matches. If overlapping occurs, i.e. more than one filter rule matches a packet, only the first rule is executed. This means that if the first rule denies a packet, whereas a later rule allows it, the packet is rejected. A deny rule also has no effect if a relevant packet has previously been allowed by another filter rule.

A list of all configured filter rules is displayed in the **Firewall->Policies->Filter Rules** menu.

You can use the  button to insert another policy above the list entry. The configuration menu for creating a new policy opens.

You can use the  button to move the list entry. A dialog box opens, in which you can select the position to which the policy is to be moved.

14.1.1.1 New

Choose the **New** button to create additional parameters.

The menu **Firewall->Policies->Filter Rules->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Source	<p>Select one of the preconfigured aliases for the source of the packet.</p> <p>In the list, all WAN/LAN interfaces, interface groups (see Firewall->Interfaces->Groups), addresses (see Firewall->Addresses->Address List) and address groups (see Firewall->Addresses->Groups) are available.</p> <p>The value <i>Any</i> means that neither the source interface nor the source address is checked.</p>
Destination	<p>Select one of the preconfigured aliases for the destination of the packet.</p> <p>In the list, all WAN/LAN interfaces, interface groups (see Firewall->Interfaces->Groups), addresses (see Firewall->Addresses->Address List) and address groups (see Firewall->Addresses->Groups).</p> <p>The value <i>Any</i> means that neither the destination interface nor the destination address is checked.</p>

Field	Description
Service	<p>Select one of the preconfigured services to which the packet to be filtered must be assigned.</p> <p>The extensive range of services configured ex works includes the following:</p> <ul style="list-style-type: none"> • <i>ftp</i> • <i>telnet</i> • <i>smtp</i> • <i>dns</i> • <i>http</i> • <i>nntp</i> • <i>Internet</i> • <i>Netmeeting</i> <p>Additional services are created in Firewall->Services->Service List.</p> <p>In addition, the service groups configured in Firewall->Services->Groups can be selected.</p>
Action	<p>Select the action to be applied to a filtered packet.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Access</i> (default value): The packets are forwarded on the basis of the entries. • <i>Deny</i>: The packets are rejected. • <i>Reject</i>: The packets are rejected. An error message is issued to the sender of the packet.
Apply QoS	<p>Only for Action = <i>Access</i></p> <p>Select whether you want to enable QoS for this policy with the priority selected in Priority.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The option is deactivated by default.</p> <p>If QoS is not activated for this policy, bear in mind that the data cannot be prioritised on the sender side either.</p>

Field	Description
	A policy for which QoS has been enabled is also set for the firewall. Make sure therefore that data traffic that has not been expressly authorised if blocked by the firewall!
Priority	<p>Only for Action = <i>Access</i> and Apply QoS = <i>Enabled</i></p> <p>Select the priority with which the data specified by the policy is handled on the send side.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i> (default value): No priority. • <i>Low Latency</i>: Low Latency Transmission (LTT), i.e. handling of data with the lowest possible latency, e.g. suitable for VoIP data. • <i>High</i> • <i>Medium</i> • <i>Low</i>

14.1.2 QoS

More and more applications need increasingly larger bandwidths, which are not always available. Quality of Service (QoS) makes it possible to distribute the available bandwidths effectively and intelligently. Certain applications can be given preference and bandwidth reserved for them.

A list of all QoS rules is displayed in the **Firewall->Policies->QoS** menu.

14.1.2.1 New

Choose the **New** button to set up new QoS rules.

The **Firewall->Policies->QoS->New** menu consists of the following fields:

Fields in the Configure QoS Interface menu

Field	Description
Interface	Select the interface on which bandwidth management is to be carried out.
Traffic Shaping	Select whether you want to activate bandwidth management

Field	Description
	<p>for the selected interface.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Specify bandwidth	<p>Only for Traffic Shaping = <i>Enabled</i></p> <p>Enter the maximum available bandwidth in kbps for the selected interface.</p>
Filter Rules	<p>This field contains a list of all configured firewall policies for which QoS was activated (Apply QoS = <i>Enabled</i>). The following options are available for each list entry:</p> <ul style="list-style-type: none"> • Use: Select whether this entry should be assigned to the QoS interface. The option is deactivated by default. • Bandwidth: Enter the maximum available bandwidth in Bit/s for the service specified under Service. <i>0</i> is entered by default. • Bounded: Select whether the bandwidth defined in Bandwidth can be exceeded in the longer term. By activating this field, you specify that it cannot be exceeded. If the option is deactivated, the bandwidth can be exceeded and the excess data rate is handled in accordance with the priority defined in the firewall policy. The option is deactivated by default.

14.1.3 Options

In this menu, you can disable or enable the firewall and can log its activities. In addition, you can define after how many seconds of inactivity a session shall be ended.

The menu **Firewall->Policies->Options** consists of the following fields:

Fields in the Global Firewall Options menu

Field	Description
Firewall Status	<p>Enable or disable the firewall function.</p> <p>The function is enabled with <i>Enabled</i></p> <p>The function is enabled by default.</p>

Field	Description
Logged Actions	<p>Select the firewall syslog level.</p> <p>The messages are output together with messages from other subsystems.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>All</i> (default value): All firewall activities are displayed. • <i>Deny</i>: Only reject and deny events are shown, see "Action". • <i>Accept</i>: Only accept events are shown. • <i>None</i>: Syslog messages are not generated.
Full Filtering	<p>Here you define whether packets are only to be filtered if they are sent to an interface other than the interface that created the connection.</p> <p>With <i>Enable</i>, all the packets are filtered (default value).</p>

Fields in the Session Timer menu

Field	Description
UDP Inactivity	<p>Enter the inactivity time after which a UDP session is to be regarded as expired (in seconds).</p> <p>Possible values are <i>30</i> to <i>86400</i>.</p> <p>The default value is <i>180</i>.</p>
TCP Inactivity	<p>Enter the inactivity time after which a TCP session is to be regarded as expired (in seconds).</p> <p>Possible values are <i>30</i> to <i>86400</i>.</p> <p>The default value is <i>3600</i>.</p>
PPTP Inactivity	<p>Enter the inactivity time after which a PPTP session is to be regarded as expired (in seconds).</p> <p>Possible values are <i>30</i> to <i>86400</i>.</p> <p>The default value is <i>86400</i>.</p>
Other Inactivity	<p>Enter the inactivity time after which a session of another type is to be regarded as expired (in seconds).</p>

Field	Description
	Possible values are <i>30 to 86400</i> .
	The default value is <i>30</i> .

14.2 Interfaces

14.2.1 Groups

A list of all configured interface routes is displayed in the **Firewall->Interfaces->Groups** menu.

You can group together the interfaces of your device. This makes it easier to configure firewall rules.

14.2.1.1 New

Choose the **New** button to set up new interface groups.

The menu **Firewall->Interfaces->Groups->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the interface group.
Members	Select the members of the group from the available interfaces. To do this, activate the field in the Selection column.

14.3 Addresses

14.3.1 Address List

A list of all configured addresses is displayed in the **Firewall->Addresses->Address List** menu.

14.3.1.1 New

Choose the **New** button to create additional addresses.

The menu **Firewall->Addresses->Address List->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter the desired description of the address.
Address Type	Select the type of address you want to specify. Possible values: <ul style="list-style-type: none"> • <i>Address / Subnet</i> (default value): Enter an IP address with subnet mask. • <i>Address Range</i>: Enter an IP address range with a start and end address.
Address / Subnet	Only for Address Type = <i>Address / Subnet</i> Enter the IP address of the host or a network address and the related netmask. The default value is <i>0.0.0.0</i> .
Address Range	Only for Address Type = <i>Address Range</i> Enter the start and end IP address of the range.

14.3.2 Groups

A list of all configured address groups is displayed in the **Firewall->Addresses->Groups** menu.

You can group together addresses. This makes it easier to configure firewall rules.

14.3.2.1 New

Choose the **New** button to set up additional address groups.

The menu **Firewall->Addresses->Groups->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter the desired description of the address group.
Selection	Select the members of the group from the available Addresses . To do this, activate the Fields in the Selection column.

14.4 Services

14.4.1 Service List

In the **Firewall->Services->Service List** menu, a list of all available services is displayed.

14.4.1.1 New

Choose the **New** button to set up additional services.

The menu **Firewall->Services->Service List->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter an alias for the service you want to configure.
Protocol	Select the protocol on which the service is to be based. The most important protocols are available for selection.
Destination Port Range	<p>Only for Protocol = <i>TCP, UDP/TCP</i> or <i>UDP</i></p> <p>In the first field, enter the destination port via which the service is to run.</p> <p>If a port number range is specified, in the second field enter the last port of the port range. By default the field does not contain an entry. If a value is displayed, this means that the previously specified port number is verified. If a port range is to be checked, enter the upper limit here.</p> <p>Possible values are <i>1 to 65535</i>.</p>
Source Port Range	Only for Protocol = <i>TCP, UDP/TCP</i> or <i>UDP</i>

Field	Description
	<p>In the first field, enter the source port to be checked, if applicable.</p> <p>If a port number range is specified, in the second field enter the last port of the port range. By default the field does not contain an entry. If a value is displayed, this means that the previously specified port number is verified. If a port range is to be checked, enter the upper limit here.</p> <p>Possible values are <i>1</i> to <i>65535</i>.</p>
Type	<p>Only for Protocol = <i>ICMP</i></p> <p>The Type field shows the class of ICMP messages, the Code field specifies the type of message in greater detail.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Any</i> (default value) • <i>Echo Reply</i> • <i>Destination unreachable</i> • <i>Source Quench</i> • <i>Redirect</i> • <i>Echo</i> • <i>Time Exceeded</i> • <i>Parameter Problem</i> • <i>Timestamp</i> • <i>Timestamp Reply</i> • <i>Information Request</i> • <i>Information Reply</i> • <i>Address Mask Request</i> • <i>Address Mask Reply</i>
Code	<p>Selection options for the ICMP codes are only available for Type = <i>Destination unreachable</i></p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Any</i> (default value) • <i>Net Unreachable</i>

Field	Description
	<ul style="list-style-type: none"> • <i>Host Unreachable</i> • <i>Protocol Unreachable</i> • <i>Port Unreachable</i> • <i>Fragmentation Needed</i> • <i>Communication with Destination Network is Administratively Prohibited</i> • <i>Communication with Destination Host is Administratively Prohibited</i>

14.4.2 Groups

A list of all configured service groups is displayed in the **Firewall->Services->Groups** menu.

You can group together services. This makes it easier to configure firewall rules.

14.4.2.1 New

Choose the **New** button to set up additional service groups.

The menu **Firewall->Services->Groups->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter the desired description of the service group.
Members	Select the members of the group from the available service aliases. To do this, activate the Fields in the Selection column.

Chapter 15 Local Services

This menu offers services for the following application areas:

- Name resolution (DNS)
- Configuration via web browser (HTTPS)
- Locating of dynamic IP addresses using a DynDNS provider
- Configuration of gateway as a DHCP server (assignment of IP addresses)
- Access restriction on the Internet (web filter)
- Assignment of incoming and outgoing data and voice calls to authorised users (CAPI server)
- Automation of tasks according to schedule (scheduling)
- Alive checks for hosts or interfaces, ping tests
- User LAN protection (theft protection)
- Realtime video/audio conferences (Messenger services, universal plug & play)
- Provision of public Internet accesses (hotspot).
- Use of a redundant gateway (BRRP).

15.1 DNS

Each device in a TCP/IP network is usually located by its IP address. Because host names are often used in networks to reach different devices, it is necessary for the associated IP address to be known. This task can be performed by a DNS server, which resolves the host names into IP addresses. Alternatively, name resolution can also take place over the HOSTS file, which is available on all PCs.

Your device offers the following options for name resolution:

- DNS Proxy, for forwarding DNS requests sent to your device to a suitable DNS server. This also includes specific forwarding of defined domains (Forwarded Domains).
- DNS cache, for saving the positive and negative results of DNS requests.
- Static entries (static hosts), to manually define or prevent assignments of IP addresses to names.
- DNS monitoring (statistics), to provide an overview of DNS requests on your device.

Name server

Under **Local Services->DNS->Global Settings->Basic Parameters** you enter the IP addresses of name servers that are queried if your device cannot answer requests itself or by forwarding entries. Global name servers and name servers that are attached to an interface can both be entered.

Your device can also receive the global name servers dynamically via PPP or DHCP and transfer them dynamically if necessary.

Strategy for name resolution on your device

A DNS request is handled by your device as follows:

- (1) If possible, the request is answered directly from the static or dynamic cache with IP address or negative response.
- (2) Otherwise, if a suitable forwarding entry exists, the relevant DNS server is asked, depending on the configuration of the Internet or dialin connections, if necessary by setting up a WAN connection at extra cost. If the DNS server can resolve the name, the information is forwarded and a dynamic entry created in the cache.
- (3) Otherwise, if name servers have been entered, taking into account the priority configured and if the relevant interface status is "up", the primary DNS server is queried and then the secondary DNS server. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.
- (4) Otherwise, if a suitable Internet or dialin connection is selected as the standard interface, the relevant DNS server is asked, depending on the configuration of the Internet or dialin connections, if necessary by setting up a WAN connection at extra cost. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.
- (5) Otherwise, if overwriting the addresses of the global name servers is allowed in the **WAN->Internet + Dialup** menu (**Interface Mode** = *Dynamic*), a connection is set up – if necessary at extra cost – to the first Internet or dialin connection configured to enable DNS server addresses to be requested from DNS servers (**DNS Negotiation** = *Enabled*), if this has not been already attempted. When the name servers have been negotiated successfully, these name servers are then available for more queries.
- (6) Otherwise the initial request is answered with a server error.

If one of the DNS servers answers with `non-existent domain`, the initial request is immediately answered accordingly and a corresponding negative entry is made in the DNS cache of your device.

15.1.1 Global Settings

The menu **Local Services->DNS->Global Settings** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Domain Name	Enter the standard domain name of your device.
WINS Server Primary Secondary	Enter the IP address of the first and, if necessary, alternative global Windows Internet Name Server (=WINS) or NetBIOS Name Server (=NBNS).

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Positive Cache	Select whether the positive dynamic cache is to be activated, i.e. successfully resolved names and IP addresses are to be stored in the cache. The function is activated by selecting <i>Enabled</i> . The function is enabled by default.
Negative Cache	Select whether the negative dynamic cache is to be activated, i.e. whether queried names for which a DNS server has sent a negative response are stored as negative entries in the cache. The function is activated by selecting <i>Enabled</i> . The function is enabled by default.
Cache Size	Enter the maximum total number of static and dynamic entries. Once this value is reached, the dynamic entry not requested for the longest period of time is deleted when a new entry is added. Cache Size is reduced by the user, dynamic entries are deleted if necessary. Statistical entries are not deleted. Cache Size cannot be set to lower than the current number of static entries.

Field	Description
	<p>Possible values: <i>0.. 1000</i>.</p> <p>The default value is <i>100</i>.</p>
Maximum TTL for Positive Cache Entries	<p>Enter the value to which the TTL is to be set for a positive dynamic DNS entry in the cache if its TTL is <i>0</i> or its TTL exceeds the value for Maximum TTL for Positive Cache Entries.</p> <p>The default value is <i>86400</i>.</p>
Maximum TTL for Negative Cache Entries	<p>Enter the value set to which the TTL is to be set in the case of a negative dynamic entry in the cache.</p> <p>The default value is <i>86400</i>.</p>
Fallback interface to get DNS server	<p>Select the interface to which a connection is set up for name server negotiation if other name resolution attempts were not successful.</p> <p>The default value is <i>Automatic</i>, i.e. a one-time connection is set up to the first suitable connection partner configured in the system.</p>

Fields in the IP address to use for DNS/WINS server assignment menu


Field	Description
As DHCP Server	<p>Select which name server addresses are sent to the DHCP client if your device is used as DHCP server.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i>: No name server address is sent. • <i>Own IP Address</i> (default value): The address of your device is transferred as the name server address. • <i>DNS Setting</i>: The addresses of the global name servers entered on your device are sent.
As IPCP Server	<p>Select which name server addresses are to be transmitted by your device in the event of dynamic server name negotiation if your device is used as the IPCP server for PPP connections.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i>: No name server address is sent.

Field	Description
	<ul style="list-style-type: none"> • <i>Own IP Address</i>: The address of your device is transferred as the name server address. • <i>DNS Setting</i> (default value): The addresses of the global name servers entered on your device are sent.

15.1.2 DNS Servers

A list of all configured DNS servers is displayed in the **Local Services->DNS->DNS Servers** menu.

15.1.2.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to set up additional DNS servers.

Here you can configure both global DNS servers and DNS servers that are to be assigned to a particular interface.

Configuring a DNS server for a particular interface can be useful, for example, if accounts with different providers have been set up via different interfaces and load balancing is being used.

The **Local Services->DNS->DNS Servers->New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Admin Status	<p>Select whether the DNS server should be enabled.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Description	Enter a description for DNS server.
Priority	<p>Assign a priority to the DNS server.</p> <p>You can assign more than one pair of DNS servers (Primary DNS Server and Secondary DNS Server) to an interface (i. e. for example, to an Ethernet port or a PPPoE WAN partner). The pair with the highest priority is used if the interface is "up".</p> <p>Possible values from 0 (highest priority) to 9 (lowest priority).</p>

Field	Description
	The default value is <i>5</i> .
Interface Mode	<p>Select whether the IP addresses of name servers for resolving the names of Internet addresses are to be obtained automatically or whether up to two fixed DNS server addresses are to be entered, depending on the priority.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Static</i> • <i>Dynamic</i> (default value)
Interface	<p>Select the interface to which the DNS server pair is to be assigned.</p> <p>For Interface Mode = <i>Dynamic</i></p> <p>A global DNS server is created with the setting <i>None</i>.</p> <p>For Interface Mode = <i>Static</i></p> <p>A DNS server is configured for all interfaces with the <i>Any</i> setting.</p>
Primary DNS Server	<p>Only if Interface Mode = <i>Manual</i></p> <p>Enter the IP address of the first name server for Internet address name resolution.</p>
Secondary DNS Server	<p>Only if Interface Mode = <i>Manual</i></p> <p>Optionally, enter the IP address of an alternative name server.</p>

15.1.3 Static Hosts

A list of all configured static hosts is displayed in the **Local Services->DNS->Static Hosts** menu.

15.1.3.1 New

Choose the **New** button to set up new static hosts.

The menu **Local Services->DNS->Static Hosts->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
DNS Hostname	<p>Enter the host name to which the IP Address defined in this menu is to be assigned if a positive response is received to a DNS request. If a negative response is received to a DNS request, no address is specified.</p> <p>The entry can also start with the wildcard *, e.g. *.bintec-elmeg.com.</p> <p>If a name is entered without a dot, this is completed with OK "<Name.>" after confirmation.</p> <p>Entries with spaces are not allowed.</p>
Response	<p>In this entry, select the type of response to DNS requests.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Negative</i>: A DNS request for DNS Hostname gets a negative response. • <i>Positive</i> (default value): A DNS request for DNS Hostname is answered with the related IP Address. • <i>None</i>: A DNS request is ignored; no answer is given.
IP Address	<p>Only if Response = <i>Positive</i></p> <p>Enter the IP address assigned to DNS Hostname.</p>
TTL	<p>Enter the validity period of the assignment from DNS Hostname to IP Address in seconds (only relevant for Response = <i>Positive</i>) transmitted to requesting hosts.</p> <p>The default value is <i>86400</i> (= 24 h).</p>

15.1.4 Domain Forwarding

In the **Local Services->DNS->Domain Forwarding** menu, a list of all configured forwardings for defined domains is displayed.

15.1.4.1 New

Choose the **New** button to set up additional forwardings.

The menu **Local Services->DNS->Domain Forwarding->New** consists of the following fields:

Fields in the Forwarding Parameters menu

Field	Description
Forward	<p>Select whether a host or domain is to be forwarded.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Host</i> (default value) • <i>Domain</i>
Host	<p>Only for Forwarding = <i>Host</i></p> <p>Enter the name of the host to be forwarded.</p> <p>The entry can also start with the wildcard *, e.g. *.bintec-elmeg.com. If a name is entered without a full stop, you complete with OK " <Default Domain>. " " is added.</p>
Domain	<p>Only for Forwarding = <i>Domain</i></p> <p>Enter the name of the domain to be forwarded.</p> <p>The entry can also start with the wildcard *, e.g. *.bintec-elmeg.com. If a name is entered without a full stop, you complete with OK " <Default Domain>. " " is added.</p>
Forward to	<p>Select the forwarding destination requests to the name defined in Host or Domain.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Interface</i> (default value): The request is forwarded to the defined Interface. • <i>DNS Server</i>: The request is forwarded to the defined DNS Server.
Interface	<p>Only for Forward to = <i>Interface</i></p> <p>Select the interface via which the requests for the defined Domain are to be received and forwarded to the DNS server.</p>
DNS Server	<p>Only for Forward to = <i>DNS Server</i></p>

Field	Description
	Enter the IP address of the primary and secondary DNS server.

15.1.5 Cache

In the **Local Services->DNS->Cache** menu, a list of all available cache entries is displayed.

You can select individual entries using the checkbox in the corresponding line, or select them all using the **Select all** button.

A dynamic entry can be converted to a static entry by marking the entry and confirming with **Make static**. This corresponding entry disappears from the list and is displayed in the list in the **Static Hosts** menu. The TTL is transferred.

15.1.6 Statistics

In the **Local Services->DNS->Statistics** menu, the following statistical values are displayed:

Fields in the DNS Statistics menu

Field	Description
Received DNS Packets	Shows the number of received DNS packets addressed direct to your device, including the response packets for forwarded requests.
Invalid DNS Packets	Shows the number of invalid DNS packets received and addressed direct to your device.
DNS Requests	Shows the number of valid DNS requests received and addressed direct to your device.
Cache Hits	Shows the number of requests that were answered with static or dynamic entries from the cache.
Forwarded Requests	Shows the number of requests forwarded to other name servers.
Cache Hitrate (%)	Indicates the number of Cache Hits pro DNS request in percentage.
Successfully Answered Queries	Shows the number of successfully answered requests (positive and negative).
Server Failures	Shows the number of requests that were not answered by any

Field	Description
	name server (either positively or negatively).

15.2 HTTPS

You can operate the user interface of your device from any PC with an up-to-date Web browser via an HTTPS connection.

HTTPS (HyperText Transfer Protocol Secure) is the procedure used to establish an encrypted and authenticated connection by SSL between the browser used for configuration and the device.

15.2.1 HTTPS Server

In the **Local Services->HTTPS->HTTPS Server** menu, configure the parameters of the backed up configuration connection via HTTPS.

The **Local Services->HTTPS->HTTPS Server** menu consists of the following fields:

Fields in the HTTPS Parameters menu

Field	Description
HTTPS TCP Port	<p>Enter the port via which the HTTPS connection is to be established.</p> <p>Possible values are <i>0</i> to <i>65535</i>.</p> <p>The default value is <i>443</i>.</p>
Local Certificate	<p>Select a certificate that you want to use for the HTTPS connection.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <i>Internal</i> (default value): Select this option if you want to use the certificate built into the device. <<i>Certificate name</i>>: Under System Management->Certificates->Certificate List select entered certificate.

15.3 DynDNS Client

The use of dynamic IP addresses has the disadvantage that a host in the network can no longer be found once its IP address has changed. DynDNS ensures that your device can still be reached after a change to the IP address.

The following configuration steps are necessary:

- Registration of a host name at a DynDNS provider
- Configuration of your device

Registration

The registration of a host name means that you define an individual user name for the DynDNS service, e.g. *dyn_client*. The service providers offer various domain names for this, so that a unique host name results for your device, e.g. *dyn_client.provider.com*. The DynDNS provider relieves you of the task of answering all DNS requests concerning the host *dyn_client.provider.com* with the dynamic IP address of your device.

To ensure that the provider always knows the current IP address of your device, your device contacts the provider when setting up a new connection and propagates its present IP address.

15.3.1 DynDNS Update

In the **Local Services->DynDNS Client->DynDNS Update** menu, a list of all configured DynDNS registrations for updating is displayed

15.3.1.1 New

Choose the **New** button to set up further DynDNS registrations to be updated.

The menu **Local Services->DynDNS Client->DynDNS Update->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Host Name	Enter the complete host name as registered with the DynDNS provider.

Field	Description
Interface	Select the WAN interface whose IP address is to be propagated over the DynDNS service (e.g. the interface of the Internet Service Provider).
User Name	Enter the user name as registered with the DynDNS provider.
Password	Enter the password as registered with the DynDNS provider.
Provider	<p>Select the DynDNS provider with which the above data is registered.</p> <p>A choice of DynDNS providers is already available in the unconfigured state and their protocols are supported.</p> <p>Other DynDNS providers can be configured in the Local Services->DynDNS Client->DynDNS Provider menu.</p> <p>The default value is <i>DynDNS</i>.</p>
Enable update	<p>Select whether the DynDNS entry configured here is to be activated.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu

Field	Description
Mail Exchanger (MX)	<p>Enter the full host name of a mail server to which e-mails are to be forwarded if the host currently configured is not to receive mail.</p> <p>Ask your provider about this forwarding service and make sure e-mails can be received from the host entered as MX.</p>
Wildcard	<p>Select whether forwarding of all subdomains of the Host Name is to be enabled for the current IP address of the Interface (advanced name resolution).</p> <p>The function is activated by selecting <i>Enabled</i>.</p>

Field	Description
	The function is disabled by default.

15.3.2 DynDNS Provider

A list of all configured DynDNS providers is displayed in the **Local Services->DynDNS Client->DynDNS Provider** menu.

15.3.2.1 New

Choose the **New** button to set up new DynDNS providers.

The menu **Local Services->DynDNS Client->DynDNS Provider->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Provider Name	Enter a name for this entry.
Server	Enter the host name or IP address of the server on which the provider's DynDNS service runs.
Update Path	Enter the path on the provider's server that contains the script for managing the IP address of your device. Ask your provider for the path to be used.
Port	Enter the port at which your device is to reach your provider's server. Ask your provider for the relevant port. The default value is <i>80</i> .
Protocol	Select one of the protocols implemented. Possible values: <ul style="list-style-type: none"> • <i>DynDNS</i> (default value) • <i>Static DynDNS</i> • <i>ODS</i>

Field	Description
	<ul style="list-style-type: none"> • <i>HN</i> • <i>DYNS</i> • <i>GnuDIP-HTML</i> • <i>GnuDIP-TCP</i> • <i>Custom DynDNS</i> • <i>DnsExit</i>
Update Interval	<p>Enter the minimum time (in seconds) that your device must wait before it is allowed to propagate its current IP address to the DynDNS provider again.</p> <p>The default value is <i>300</i> seconds.</p>

15.4 DHCP Server

You can configure your device as a DHCP (Dynamic Host Configuration Protocol) server.

Your device and each PC in your LAN requires its own IP address. One option for allocating IP addresses in your LAN is the Dynamic Host Configuration Protocol (DHCP). If you configure your device as a DHCP server, the device automatically assigns IP addresses to requesting PCs in the LAN from a predefined IP address pool.


If a client requires an IP address for the first time, it sends a DHCP request (with its MAC address) to the available DHCP server as a network broadcast.* The client then receives its IP address from bintec elmeg (as part of a brief exchange).

You therefore do not need to allocate fixed IP addresses to PCs, which reduces the amount of configuration work in your network. To do this, you set up a pool of IP addresses, from which your device assigns IP addresses to hosts in the LAN for a defined period of time. A DHCP server also transfers the addresses of the domain name server entered statically or by PPP negotiation (DNS), NetBIOS name server (WINS) and default gateway.

15.4.1 IP Pool Configuration

The **Local Services->DHCP Server->IP Pool Configuration** menu displays a list of all the configured IP pools. This list is global and also displays pools configured in other menus.

15.4.1.1 Edit or New

Choose the **New** button to set up new IP address pools. Choose the  icon to edit existing entries.

The **Local Services->DHCP Server->IP Pool Configuration->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	<p>Primary: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool.</p> <p>Secondary: Optionally, enter the IP address of an alternative DNS server.</p>

15.4.2 DHCP Configuration

To activate your device as a DHCP server, you must first define IP address pools from which the IP addresses are distributed to the requesting clients.


A list of all configured IP address pools is displayed in the **Local Services->DHCP Server->DHCP Configuration** menu.

In the list, for each entry, you have the possibility under **Status** of enabling or disabling the configured DHCP pools.

Note

In the ex works state the DHCP pool is preconfigured with the IP addresses 192.168.0.10 to 192.168.0.49 and is used if there is no other DHCP server available in the network.

15.4.2.1 Edit or New

Choose the **New** button to set up new IP address pools. Choose the  icon to edit existing entries.

The **Local Services->DHCP Server->DHCP Configuration->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Select the interface over which the addresses defined in IP Address Range are to be assigned to DHCP clients. When a DHCP request is received over this Interface , one of the addresses from the address pool is assigned.
IP Pool Name	Enter any description to uniquely identify the IP pool.
Pool Usage	Specify whether the IP pool is used for DHCP requests in the same subnet or for DHCP requests that have been forwarded to your device from another subnet. In this case it is possible to define IP addresses from another network. Possible values: <ul style="list-style-type: none"> • <i>Local</i> (default value): The DHCP pool is only used for DHCP requests in the same subnet. • <i>Relay</i>: The DHCP pool is only used for DHCP requests forwarded from other subnets. • <i>Local/Relay</i>: The DHCP pool is used for DHCP requests in the same subnet and from other subnets.

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Advanced Settings


Field	Description
Gateway	Select which IP address is to be transferred to the DHCP client as gateway. Possible values: <ul style="list-style-type: none"> • <i>Use router as gateway</i> (default value): Here, the IP ad-

Field	Description
	<p>dress defined for the Interface is transferred.</p> <ul style="list-style-type: none"> • <i>No gateway</i>: No IP address is sent. • <i>Specify</i>: Enter the corresponding IP address.
Lease Time	<p>Enter the length of time (in minutes) for which an address from the pool is to be assigned to a host.</p> <p>After the Lease Time expires, the address can be reassigned by the server.</p> <p>The default value is <i>120</i>.</p>
DHCP Options	<p>Specify which additional data is forwarded to the DHCP client.</p> <p>Possible values for Option:</p> <ul style="list-style-type: none"> • <i>Time Server</i> (default value): Enter the IP address of the time server to be sent to the client. • <i>DNS Server</i>: Enter the IP address of the DNS server to be sent to the client. • <i>DNS Domain Name</i>: Enter the DNS domain to be sent to the client. • <i>WINS/NBNS Server</i>: Enter the IP address of the WINS/NBNS server to be sent to the client. • <i>WINS/NBT Node Type</i>: Select the type of the WINS/NBT node to be sent to the client. • <i>TFTP Server</i>: Enter the IP address of the TFTP server to be sent to the client. • <i>CAPWAP Controller</i>: Enter the IP address of the CAPWAP controller to be sent to the client. • <i>URL (provisioning server)</i>: This option enables you to send a client any URL. <p>Use this option to send querying IP1x0 telephones the URL of the provisioning server if the telephones are to be provisioned automatically. The URL then needs to take the form <i>http://<IP address of the provisioning server>/eg_prov</i>.</p> <ul style="list-style-type: none"> • <i>Vendor Group</i> (Vendor Specific Information): This enables you to send the client any manufacturer-specific information in any text string.

Field	Description
	Several entries are possible. Add additional entries with the Add button.

Edit

In the **Local Services->DHCP Server ->DHCP Configuration->Advanced Settings** menu you can edit an entry in the **DHCP Options** field, if **Option = Vendor Group** is selected.

Choose the  icon to edit an existing entry. In popup menu, you configure manufacture-specific settings in the DHCP server for specific telephones.

Fields in the Basic Parameters menu

Field	Description
Select vendor	<p>Your device does not currently use this parameter.</p> <p>Here, you can select for which manufacturer specific values shall be transmitted for the DHCP server.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Siemens</i> (default value) • <i>Other</i>
Provisioning Server (code 3)	<p>Your device does not currently use this parameter.</p> <p>Enter which manufacturer value shall be transmitted.</p> <p>For the setting Select vendor = <i>Siemens</i>, the default value <i>sdlp</i> is displayed.</p> <p>You can complete the IP address of the desired server.</p>

15.4.3 IP/MAC Binding

The **Local Services->DHCP Server->IP/MAC Binding** menu displays a list of all clients that received an IP address from your device via DHCP.

You can allocate an IP address from a defined IP address pool to specific MAC addresses. You can do this by selecting the **Static Binding** option in the list to convert a list entry as a fixed binding, or you manually create a fixed IP/MAC binding by configuring this in the **New** sub-menu.

**Note**

You can only create new static IP/MAC bindings if IP address ranges were configured in **Local Services->DHCP Server->DHCP Pool**.

15.4.3.1 New

Choose the **New** button to set up new IP/MAC bindings.

The menu **Local Services->DHCP Server->IP/MAC Binding->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter the name of the host to which the MAC Address the IP Address is to be bound. A character string of up to 256 characters is possible.
IP Address	Enter the IP address to be assigned to the MAC address specified in MAC Address is to be assigned.
MAC Address	Enter the MAC address to which the IP address specified in IP Address is to be assigned.

15.4.4 DHCP Relay Settings

If your device for the local network does not distribute any IP addresses to the clients by DHCP, it can still forward the DHCP requests on behalf of the local network to a remote DHCP server. The DHCP server then assigns the your device an IP address from its pool, which in turn sends this to the client in the local network.

The menu **Local Services->DHCP Server->DHCP Relay Settings** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Primary DHCP Server	Enter the IP address of a server to which BootP or DHCP requests are to be forwarded.

Field	Description
Secondary DHCP Server	Enter the IP address of an alternative BootP or DHCP server.

15.5 CAPI Server

You can use the CAPI Server function to assign user names and passwords to users of the CAPI applications on your device. This makes sure that only authorised users can receive incoming calls and make outgoing calls via CAPI.

The CAPI service allows connection of incoming and outgoing data and voice calls to communications applications on hosts in the LAN that access the Remote CAPI interface of your device. This enables, for example, hosts connected to your device to receive and send faxes.



Note

All incoming calls to the CAPI are offered to all registered and "eavesdropping" CAPI applications in the LAN.

In the ex works state, a user with the user name *default* and no password is entered for the CAPI subsystem.

Once you've created your intended users with password, you should delete the *default* user without password.

15.5.1 User

A list of all configured CAPI users is displayed in the **Local Services->CAPI Server->User** menu.

15.5.1.1 New

Choose the **New** button to set up new CAPI users.

The menu **Local Services->CAPI Server->User->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
User Name	Enter the user name for which access to the CAPI service is to

Field	Description
	be allowed or denied.
Password	Enter the password which the user User Name shall use for identification to gain access to the CAPI service.
Access	Select whether access to the CAPI service is to be permitted or denied for the user. The function is activated by selecting <i>Enabled</i> . The function is enabled by default.

15.5.2 Options

The menu **Local Services->CAPI Server->Options** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Enable server	Select whether your device is to be enabled as a CAPI server. The function is activated by selecting <i>Enabled</i> . The function is enabled by default.
Faxheader	Select whether the fax header should be printed at the top of outgoing faxes. The function is activated by selecting <i>Enabled</i> . The function is disabled by default.
CAPI Server TCP Port	The field can only be edited if Enable server is enabled. Enter the TCP port number for remote CAPI connections. The default value is <i>2662</i> .

15.6 Scheduling

Your device has a event scheduler, which enables certain standard actions (for example, activating and deactivating interfaces) to be carried out. Moreover, every existing MIB variable can be configured with any value.

You specify the **Actions** you want and define the **Trigger** that control when and under which conditions the **Actions** are to be carried out. A **Trigger** may be a single event or a sequence of events which are combined into an **Event List**. You also create an event list for a single event, but it only contains one event.

Actions can be initiated on a time-controlled basis. Moreover, the status or accessibility of interfaces or their data traffic may lead to execution of the configured actions, or also the validity of licences. Here also, it is possible to set up every MIB variable as initiator with any value.

To take the event scheduler live, enable the **Schedule Interval** under **Options**. This interval species the time gap in which the system checks whether at least one event has occurred. This event is used as the initiator for a configured action.



Caution

The configuration of actions that are not available as defaults requires extensive knowledge of the method of operation of **bintec elmeg** gateways. An incorrect configuration can cause considerable disruption during operation. If applicable, save the original configuration on your PC.



Note

To run the event scheduler, the date configured on your device must be 1.1.2000 or later.

15.6.1 Trigger

The **Local Services->Scheduling->Trigger** menu displays all the event lists that have been configured. Every event list contains at least one event which is intended to be the initiator for an action.

15.6.1.1 New

Choose the **New** button to create more event lists.

The menu **Local Services->Scheduling->Trigger->New** consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Event List	<p>You can create a new event list with <i>New</i> (default value). You give this list a name with Description. You use the remaining parameters to create the first event in the list.</p> <p>If you want to add to an existing event list, select the event list you want and add at least one more event to it.</p> <p>You can use event lists to create complex conditions for initiating an action. The events are processed in the same order in which they are created in the list.</p>
Description	<p>Only for Event List = <i>New</i></p> <p>Enter your chosen designation for the event list.</p>
Event Type	<p>Select the type of event.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Time</i> (default value): The operations configured and assigned in Actions are initiated at specific points in time. • <i>MIB/SNMP</i>: The actions configured and assigned in Actions are initiated when the defined MIB variables assumes the assigned values. • <i>Interface Status</i>: Operations configured and assigned in Actions are initiated, when the defined interfaces take on a specified status. • <i>Interface Traffic</i>: The operations configured and assigned in Actions are triggered if the data traffic on the specified interfaces falls below or exceed the defined value. • <i>Ping Test</i>: the operations configured and assigned in Actions are triggered if the defined IP address is accessible or not accessible. • <i>Certificate Lifetime</i>: Operations configured and as-

Field	Description
	signed in Actions are initiated when the defined period of validity is reached.
Monitored Variable	<p>Only for Event Type <i>MIB/SNMP</i></p> <p>Select the MIB variable whose defined value is to be configured as initiator. First, select the System in which the MIB variable is saved, then the MIB Table and finally the MIB Variable itself. Only the MIB tables and MIB variables present in the respective area are displayed.</p>
Compare Condition	<p>Only for Event Type <i>MIB/SNMP</i></p> <p>Select whether the MIB variable <i>Greater</i> (default value), <i>Equal</i>, <i>Less</i>, <i>Not Equal</i>, must have the value given in <i>Compare Value</i> or must lie within <i>Range</i> to initiate the operation.</p>
Compare Value	<p>Only for Event Type <i>MIB/SNMP</i></p> <p>Enter the value of the MIB variable.</p>
Index Variables	<p>Only for Event Type <i>MIB/SNMP</i></p> <p>Where required, select MIB variables to uniquely identify a specific data set in the MIB Table, e.g. <i>ConnIfIndex</i>. The unique identification of a particular table entry is derived from the combination of Index Variable (usually an index variable which is flagged with *) and Index Value.</p> <p>Use Index Variables to create more entries with Add.</p>
Monitored Interface	<p>Only for Event Type <i>Interface Status</i> and <i>Interface Traffic</i></p> <p>Select the interface whose defined status shall trigger an operation.</p>
Interface Status	<p>Only for Event Type <i>Interface Status</i></p> <p>Select the status that the interface must have in order to initiate the intended operation.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Up</i> (default value): The function is enabled.

Field	Description
	<ul style="list-style-type: none"> <i>Down</i>: The interface is disabled.
Traffic Direction	<p>Only for Event Type <i>Interface Traffic</i></p> <p>Select the direction of the data traffic whose values should be monitored as initiating an operation.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <i>RX</i> (default value): Incoming data traffic is monitored. <i>TX</i>: Outgoing data traffic is monitored.
Interface Traffic Condition	<p>Only for Event Type <i>Interface Traffic</i></p> <p>Select whether the value for data traffic must be <i>Greater</i> (default value) or <i>Less</i> the value specified in <i>Transferred Traffic</i> in order to initiate the operation.</p>
Transferred Traffic	<p>Only for Event Type <i>Interface Traffic</i></p> <p>Enter the desired value in kBytes for the data traffic to serve as comparison.</p> <p>The default value is <i>0</i>.</p>
Destination IP Address	<p>Only for Event Type <i>Ping Test</i></p> <p>Enter the IP address whose accessibility is to be checked.</p>
Source IP Address	<p>Only for Event Type <i>Ping Test</i></p> <p>Enter an IP address to be used as sender address for the ping test.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <i>Automatic</i> (default value): The IP address of the interface over which the ping is sent is automatically entered as sender address. <i>Specific</i>: Enter the desired IP address in the input field.
Status	<p>Only for Event Type <i>Ping Test</i></p> <p>Select whether Destination IP Address <i>Reacheable</i> must be (default value) or <i>Unreacheable</i> in order to initiate the opera-</p>

Field	Description
	tion.
Interval	<p>Only for Event Type <i>Ping Test</i></p> <p>Enter the time in Seconds after which a ping must be resent.</p> <p>The default value is <i>60</i> seconds.</p>
Trials	<p>Only for Event Type <i>Ping Test</i></p> <p>Enter the number of ping tests to be performed until Destination IP Address as <i>Unreachable</i> applies.</p> <p>The default value is <i>3</i>.</p>
Monitored Certificate	<p>Only for Event Type <i>Certificate Lifetime</i></p> <p>Select the certificate whose validity should be checked.</p>
Remaining Validity	<p>Only for Event Type <i>Certificate Lifetime</i></p> <p>Enter the desired value for the remaining validity of the certificate in percentage.</p>

Fields in the menu **Select time interval**

Field	Description
Time Condition	<p>For Event Type <i>Time</i> only</p> <p>First select the type of time entry in Condition Type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Weekday</i>: Select a weekday in Condition Settings. • <i>Periods</i> (default value): In Condition Settings, select a particular period. • <i>Day of Month</i>: Select a specific day of the month in Condition Settings. <p>Possible values for Condition Settings in Condition Type = <i>Weekday</i>:</p> <p><i>Monday</i> (default value) ... <i>Sunday</i>.</p> <p>Possible values for Condition Settings in Condition Type =</p>

Field	Description
	<p><i>Periods:</i></p> <ul style="list-style-type: none"> • <i>Daily</i>: The initiator becomes active daily (default value). • <i>Monday-Friday</i>: The initiator becomes active daily from Monday to Friday. • <i>Monday - Saturday</i>: The initiator becomes active daily from Monday to Saturday. • <i>Saturday - Sunday</i>: The initiator becomes active on Saturdays and Sundays. <p>Possible values for Condition Settings in Condition Type = <i>Day of Month</i>:</p> <p>1... 31.</p>
Start Time	Enter the time from which the initiator is to be activated. Activation is carried on the next scheduling interval. the default value of this interval is 55 seconds.
Stop Time	Enter the time from which the initiator is to be deactivated. Deactivation is carried on the next scheduling interval. If you do not enter a Stop Time or set a Stop Time = Start Time , the initiator is activated, and deactivated after 10 seconds.

15.6.2 Actions

In the **Local Services->Scheduling->Actions** menu is displayed a list of all operations to be initiated by events or event chains configured in **Local Services->Scheduling->Trigger**.

15.6.2.1 New

Choose the **New** button to configure additional operations.

The menu **Local Services->Scheduling->Actions->New** consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter your chosen designation for the action.

Field	Description
Command Type	<p>Select the desired action.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Reboot</i> (default value): Your device is rebooted. • <i>MIB/SNMP</i>: The desired value is entered for a MIB variable. • <i>Interface Status</i>: The status of an interface is modified. • <i>Wlan Status</i>: Only for devices with a wireless LAN. The status of a WLAN-SSID is modified. • <i>Software Update</i>: A software update is initiated. • <i>Configuration Management</i>: A configuration file is loaded onto your device or backed up by your device. • <i>Ping Test</i>: Accessibility of an IP address is checked. • <i>Certificate Management</i>: A certificate is to be renewed, deleted or entered.
Event List	<p>Select the event list you want which has been created in Local Services->Scheduling->Trigger.</p>
Event List Condition	<p>For the selected chains of events, select how many of the configured events must occur for the operation to be initiated.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>All</i> (default value): The operation is initiated if all events occur. • <i>One</i>: The operation is initiated if a single event occurs. • <i>None</i>: The operation is triggered if no event occurs. • <i>One not</i>: The operation is triggered if one of the events does not occur.
Reboot device after	<p>Only if Command Type = <i>Reboot</i></p> <p>Enter the timespan in seconds that must elapse after occurrence of the event until the device is restarted.</p> <p>The default value is <i>60</i> seconds.</p>
MIB/SNMP Variable to add/edit	<p>Only if Command Type = <i>MIB/SNMP</i></p> <p>Select the MIB table in which the MIB variable whose value</p>

Field	Description
	<p>shall be changed is saved. First, select the System, then the MIB Table. Only the MIB tables present in the respective area are displayed.</p>
Command Mode	<p>Only if Command Type = <i>MIB/SNMP</i></p> <p>Select how the MIB entry is to be manipulated.</p> <p>Possible settings:</p> <ul style="list-style-type: none"> • <i>Change existing entry</i> (default value): An existing entry shall be modified. • <i>Create new MIB entry</i>: A new entry shall be created.
Index Variables	<p>Only if Command Type = <i>MIB/SNMP</i></p> <p>Where required, select MIB variables to uniquely identify a specific data set in MIB Table, e.g. <i>ConnIfIndex</i>. The unique identification of a particular table entry is derived from the combination of Index Variable (usually an index variable which is flagged with *) and Index Value.</p> <p>Use Index Variables to create more entries with Add.</p>
Trigger Status	<p>Only if Command Type = <i>MIB/SNMP</i></p> <p>Select what status the event must have in order to modify the MIB variable as defined.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Active</i> (default value): The value of the MIB variable is modified if the initiator is active. • <i>Inactive</i>: The value of the MIB variable is modified if the initiator is inactive. • <i>Both</i>: The value of the MIB variable is differentially modified if the initiator status changes.
MIB Variables	<p>Only if Command Type = <i>MIB/SNMP</i></p> <p>Select the MIB variable whose value is to be configured as dependent upon initiator status.</p> <p>If the initiator is active (Trigger Status <i>Active</i>), the MIB vari-</p>

Field	Description
	<p>able is described with the value entered in Active Value.</p> <p>If the initiator is inactive (Trigger Status <i>Inactive</i>), the MIB variable is described with the value entered in Inactive Value.</p> <p>If the MIB variable is to be modified, depending on whether the initiator is active or inactive (Trigger Status <i>Both</i>), it is described with an active initiator with the value entered in Active Value and with an inactive initiator with the value in Inactive Value.</p> <p>Use Add to create more entries.</p>
Interface	<p>Only if Command Type = <i>Interface Status</i></p> <p>Select the interface whose status should be changed.</p>
Set interface status	<p>Only if Command Type = <i>Interface Status</i></p> <p>Select the status to be set for the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Up</i> (default value) • <i>Down</i> • <i>Reset</i>
Source Location	<p>Only if Command Type = <i>Software Update</i></p> <p>Select the source for the software update.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Current Software from Update Server</i> (default value): The latest software will be downloaded from the update server. • <i>HTTP Server</i>: The latest software will be downloaded from an HTTP server that you define in <i>Server URL</i>. • <i>HTTPS Server</i>: The latest software will be downloaded from an HTTPS server that you define in <i>Server URL</i>. • <i>TFTP Server</i>: The latest software will be downloaded from an TFTP server that you define in <i>Server URL</i>.
Server URL	<p>Where Command Type = <i>Software Update</i> if Source Loc-</p>

Field	Description
	<p>action not <i>Current Software from Update Server</i></p> <p>Enter the URL of the server from which the desired software version is to be retrieved.</p> <p>Where Command Type = <i>Configuration Management</i> with Action = <i>Import configuration</i> or <i>Export configuration</i></p> <p>Enter the URL of the server from which a configuration file is to be retrieved, or on which the configuration file is to be backed up.</p>
File Name	<p>For Command Type = <i>Software Update</i></p> <p>Enter the file name of the software version.</p> <p>Where Command Type = <i>Certificate Management</i> with Action = <i>Import certificate</i></p> <p>Enter the file name of the certificate file.</p>
Action	<p>For Command Type = <i>Configuration Management</i></p> <p>Select which operation is to be performed on a configuration file.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Import configuration</i> (default value) • <i>Export configuration</i> • <i>Rename configuration</i> • <i>Delete configuration</i> • <i>Copy configuration</i> <p>For Command Type = <i>Certificate Management</i></p> <p>Select which operation you wish to perform on a certificate file.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Import certificate</i> (default value) • <i>Delete certificate</i> • <i>SCEP</i>

Field	Description
Protocol	<p>Only for Command Type = <i>Certificate Management</i> and <i>Configuration Management</i> if Action = <i>Import configuration</i></p> <p>Select the protocol for the data transfer.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>HTTP</i> (default value) • <i>HTTPS</i> • <i>TFTP</i>
CSV File Format	<p>Only where Command Type = <i>Configuration Management</i> and Action = <i>Import configuration</i> or <i>Export configuration</i></p> <p>Select whether the file is to be sent in the CSV format.</p> <p>The CSV format can easily be read and modified. In addition, you can view the corresponding file clearly using Microsoft Excel for example.</p> <p>The function is enabled by default.</p>
Remote File Name	<p>Only if Command Type = <i>Configuration Management</i></p> <p>For Action = <i>Import configuration</i></p> <p>Enter the name of the file under which it is saved on the server from which it is to be retrieved.</p> <p>For Action = <i>Export configuration</i></p> <p>Enter the file name under which it should be saved on the server.</p>
Local File Name	<p>Only where Command Type = <i>Configuration Management</i> and Action = <i>Import configuration</i>, <i>Rename configuration</i> or <i>Copy configuration</i></p> <p>At import, renaming or copying enter a name for the configuration file under which to save it locally on the device.</p>
File Name in Flash	<p>Where Command Type = <i>Configuration Management</i> and Action = <i>Export configuration</i></p>

Field	Description
	<p>Select the file to be exported.</p> <p>Where Command Type = <i>Configuration Management</i> and Action = <i>Rename configuration</i></p> <p>Select the file to be renamed.</p> <p>Where Command Type = <i>Configuration Management</i> and Action = <i>Delete configuration</i></p> <p>Select the file to be deleted.</p> <p>Where Command Type = <i>Configuration Management</i> and Action = <i>Copy configuration</i></p> <p>Select the file to be copied.</p>
Configuration contains certificates/keys	<p>Only where Command Type = <i>Configuration Management</i> and Action = <i>Import configuration</i> or <i>Export configuration</i></p> <p>Select whether the certificates and keys contained in the configuration are to be imported or exported.</p> <p>The function is disabled by default.</p>
Encrypt configuration	<p>Only where Command Type = <i>Configuration Management</i> and Action = <i>Import configuration</i> or <i>Export configuration</i></p> <p>Define whether the data of the selected Action are to be encrypted..</p> <p>The function is disabled by default.</p>
Reboot after execution	<p>Only if Command Type = <i>Configuration Management</i></p> <p>Select whether your device should restart after the intended Action.</p> <p>The function is disabled by default.</p>
Version Check	<p>Only where Command Type = <i>Configuration Management</i> and Action = <i>Import configuration</i></p> <p>Select whether, when importing a configuration file, to check on</p>

Field	Description
	<p>the server for the presence of a more current version of the already loaded configuration. If not, the file import is interrupted.</p> <p>The function is disabled by default.</p>
Destination IP Address	<p>Only if Command Type = <i>Ping Test</i></p> <p>Enter the IP address whose accessibility is to be checked.</p>
Source IP Address	<p>Only if Command Type = <i>Ping Test</i></p> <p>Enter an IP address to be used as sender address for the ping test.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Automatic</i> (default value): The IP address of the interface over which the ping is sent is automatically entered as sender address. • <i>Specific</i>: Enter the desired IP address in the input field.
Interval	<p>Only if Command Type = <i>Ping Test</i></p> <p>Enter the time in Seconds after which a ping must be resent.</p> <p>The default value is 1 second.</p>
Count	<p>Only if Command Type = <i>Ping Test</i></p> <p>Enter the number of ping tests to be performed until Destination IP Address is considered unreachable.</p> <p>The default value is 3.</p>
Server Address	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>Import certificate</i></p> <p>Enter the URL of the server from which a certificate file is to be retrieved.</p>
Local Certificate Description	<p>Where Command Type = <i>Certificate Management</i> and Action = <i>Import certificate</i></p> <p>Enter a description for the certificate under which to save it on</p>

Field	Description
	<p>the device.</p> <p>Where Command Type = <i>Certificate Management</i> and Action = <i>Delete certificate</i></p> <p>Select the certificate to be deleted.</p>
Password for protected Certificate	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>Import certificate</i></p> <p>Select whether to use a secure certificate requiring a password and enter it into the entry field.</p> <p>The function is disabled by default.</p>
Overwrite similar certificate	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>Import certificate</i></p> <p>Select whether to overwrite a certificate already present on the your device with the new one.</p> <p>The function is disabled by default.</p>
Write certificate in configuration	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>Import certificate</i></p> <p>Select whether to integrate the certificate in a configuration file; and if so, select the desired configuration file.</p> <p>The function is disabled by default.</p>
Certificate Request Description	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>Enter a description under which the SCEP certificate on your device is to be saved.</p>
URL SCEP Server URL	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>Enter the URL of the SCEP server, e.g. <i>http://scep.bintec-elmeg.com:8080/scep/scep.dll</i></p> <p>Your CA administrator can provide you with the necessary data.</p>

Field	Description
Subject Name	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>Enter a subject name with attributes.</p> <p>Example: "CN=VPNServer, DC=mydomain, DC=com, c=DE"</p>
CA Name	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>Enter the name of the CA certificate of the certification authority (CA) from which you wish to request your certificate, e.g. <i>cawindows</i>. Your CA administrator can provide you with the necessary data.</p>
Password	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>To obtain certificates, you may need a password from the certification authority. Enter the password you received from the certification authority here.</p>
Key Size	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>Select the length of the key to be created. Possible values are 1024 (default value), 2048 and 4096.</p>
Autosave Mode	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>Select whether your device automatically stores the various steps of the enrolment internally. This is an advantage if enrolment cannot be concluded immediately. If the status has not been saved, the incomplete registration cannot be completed. As soon as the enrolment is completed and the certificate has been downloaded from the CA server, it is automatically saved in the device configuration.</p> <p>The function is enabled by default.</p>
Use CRL	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p>

Field	Description
	<p>Define the extent to which certificate revocation lists (CRLs) are to be included in the validation of certificates issued by the owner of this certificate.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Auto</i> (default value): In case there is an entry for a CDP, CRL distribution point this should be evaluated in addition to the CRLs globally configured in the device. • <i>Yes</i>: CRLs are always checked. • <i>No</i>: No checking of CRLs.

15.6.3 Options

You configure the schedule interval in the **Local Services->Scheduling->Options**.

The **Local Services->Scheduling->Options** menu consists of the following fields:

Fields in the Scheduling Options menu

Field	Description
Schedule Interval	<p>Select whether the schedule interval is to be enabled for the interface.</p> <p>Enter the period of time in seconds after which the system checks whether configured events have occurred.</p> <p>Possible values are <i>0</i> to <i>65535</i>.</p> <p>The value <i>300</i> is recommended (5 minute accuracy).</p>

15.7 Surveillance

In this menu, you can configure an automatic availability check for hosts or interfaces and automatic ping tests.




Note

This function cannot be configured on your device for connections that are authenticated via a RADIUS server.

15.7.1 Hosts

A list of all monitored hosts is displayed in the **Local Services->Surveillance->Hosts** menu.

15.7.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create additional monitoring tasks.

The menu **Local Services->Surveillance->Hosts->New** consists of the following fields:

Fields in the Host Parameters menu

Field	Description
Group ID	<p>If the availability of a group of hosts or the default gateway is to be monitored by your device, select an ID for the group or the default gateway.</p> <p>The group IDs are automatically created from <i>0</i> to <i>255</i>. If an entry has not yet been created, a new group is created using the <i>New ID</i> option. If entries have been created, you can select one from the list of created groups.</p> <p>Each host to be monitored must be assigned to a group.</p> <p>The operation configured in Interface is only executed if no group member can be reached.</p>

Fields in the Trigger menu

Field	Description
Monitored IP Address	<p>Enter the IP address of the host to be monitored.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Default Gateway</i> (default value): The default gateway is monitored. • <i>Specific</i>: Enter the IP address of the host to be monitored manually in the adjacent input field.
Source IP Address	<p>Select how the IP address is to be determined that your device uses as the source address of the packet sent to the host to be</p>


Field	Description
	<p>monitored.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Automatic</i> (default value): The IP address is determined automatically. • <i>Specific</i>; Enter the IP address in the adjacent input field.
Interval	<p>Enter the time interval (in seconds) to be used for checking the availability of hosts.</p> <p>Possible values are 1 to 65536.</p> <p>The default value is 10.</p> <p>Within a group, the smallest Interval of the group members is used.</p>
Successful Trials	<p>Specify how many pings need to be answered for the host to be regarded as accessible.</p> <p>You can use this setting to specify, for example, when a host is deemed to be accessible once more, and used again, instead of a backup device.</p> <p>Possible values are 1 to 65536.</p> <p>The default value is 3.</p>
Unsuccessful Trials	<p>Specify how many pings need to be unanswered for the host to be regarded as inaccessible.</p> <p>You can use this setting to specify, for example, when a host is deemed to be inaccessible, and that a backup device should be used.</p> <p>Possible values are 1 to 65536.</p> <p>The default value is 3.</p>
Action to be performed	<p>Select which Action should be run. For most actions, you select an Interface to which the Action relates.</p> <p>All physical and virtual interfaces can be selected.</p>

Field	Description
	<p>For each interface, select whether it is to be enabled (<i>Enable</i>), disabled (<i>Disable</i> default value), reset (<i>Reset</i>), or the connection reestablished (<i>Redial</i>).</p> <p>With Action = <i>Monitor</i> you can monitor the IP address that is specified under Monitored IP Address. This information can be used for other functions, such as the Tracking IP Address.</p>

15.7.2 Interfaces

A list of all monitored hosts is displayed in the **Local Services->Surveillance->Interfaces** menu.

15.7.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to set up monitoring for other interfaces.

The menu **Local Services->Surveillance->Interfaces->New** consists of the following fields:

Fields in the Basic Parameters menu


Field	Description
Monitored Interface	Select the interface on your device that is to be monitored.
Trigger	<p>Select the state or state transition of Monitored Interface that is to trigger a particular Interface Action.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Interface goes up</i> (default value) • <i>Interface goes down</i>
Interface Action	<p>Select the action that is to follow the state or state transition defined in Trigger.</p> <p>The action is applied to the Interface(s) selected in Interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Enable</i> (default value): Activation of interface(s)

Field	Description
	<ul style="list-style-type: none"> • <i>Disable</i>: Deactivation of interface(s)
Interface	<p>Select the interface(s) for which the action defined in Interface is to be performed.</p> <p>You can choose all physical and virtual interfaces as well as options <i>All PPP Interfaces</i> and <i>All IPSec Interfaces</i>.</p>

15.7.3 Ping Generator

In the **Local Services->Surveillance->Ping Generator** menu, a list of all configured, automatically generated pings is displayed.

15.7.3.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create additional pings.

The menu **Local Services->Surveillance->Ping Generator->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Destination IP Address	Enter the IP address to which the ping is automatically sent.
Source IP Address	<p>Enter the source IP address of the outgoing ICMP echo request packets.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Automatic</i>: The IP address is determined automatically. • <i>Specific</i> (default value): Enter the IP address in the adjacent input field e.g. to test a particular extended route.
Interval	<p>Enter the interval in seconds during which the ping is sent to the address specified in Remote IP Address.</p> <p>Possible values are <i>1</i> to <i>65536</i>.</p> <p>The default value is <i>10</i>.</p>

Field	Description
Trials	<p>Enter the number of ping tests to be performed until Destination IP Address as <i>Unreachable</i> applies.</p> <p>The default value is <i>3</i>.</p>

15.8 UPnP

Universal Plug and Play (UPnP) makes it possible to use current messenger services (e.g. real time video/audio conferencing) as peer-to-peer communication where one of the peers lies behind a NAT-enabled gateway.

UPnP enables (mostly) Windows-based operating systems to take control of other devices with UPnP functionality on the local network. These include gateways, access points and print servers. No special device drivers are needed as known common protocols are used, such as TCP/IP, HTTP and XML.

Your gateway makes it possible to use the subsystem of the Internet Gateway Device (IGD) from the UPnP function range.

In a network behind a NAT-enabled gateway, the UPnP-configured computers act as LAN UPnP clients. To do this, the UPnP function on the PC must be enabled.

The pre-configured port used for UPnP communication between LAN UPnP clients and the gateway is *5678*. The LAN UPnP client acts as a so-called service control point, i.e. it recognizes and controls the UPnP devices on the network.

The ports assigned dynamically by, for example, MSN Messenger, lie in the range from *5004* to *65535*. The ports are released internally to the gateway on demand, i.e. when an audio/video transfer is started in Messenger. When the application is closed, the ports are immediately closed again.

The peer-to-peer-communication is initiated via public SIP servers with only the information from the two clients being forwarded. The clients then communicate directly with one another.

For further information about UPnP, see www.upnp.org.

15.8.1 Interfaces

In this menu, you configure the UPnP settings individually for each interface of your gateway.

You can determine whether UPnP requests from clients are accepted by each interface

(for requests from the local network) and/or whether the interface can be controlled via UPnP requests.

The menu **Local Services->UPnP->Interfaces** consists of the following fields:

Fields in the Interfaces menu

Field	Description
Interface	Shows the name of the interface for which the UPnP settings are to be made. The entry cannot be changed.
Answer to client request	Determine whether UPnP requests from clients are to be answered via the particular interface (from the local network). The function is enabled with <i>Enabled</i> . The function is disabled by default.
Interface is UPnP controlled	Determine whether the NAT configuration of this interface is controlled by UPnP. The function is enabled with <i>Enabled</i> . The function is disabled by default.

15.8.2 General

In this menu, you make the basic UPnP settings.

The **Local Services->UPnP->General** menu consists of the following fields:

Fields in the General menu

Field	Description
UPnP Status	Decide how the gateway processes UPnP requests from the LAN. The function is enabled with <i>Enabled</i> . The gateway proceeds with UPnP releases in accordance with the parameters contained in the request from the LAN UPnP client, independently of the IP address of the requesting LAN UPnP client. The function is disabled by default. The gateway rejects UPnP requests, NAT releases are not made.

Field	Description
UPnP TCP Port	<p>Enter the number of the port on which the gateway listens for UPnP requests.</p> <p>The possible values are 1 to 65535, the default value is 5678.</p>

15.9 HotSpot Gateway

The **HotSpot Solution** allows provision of public Internet accesses (using WLAN or wired Ethernet). The solution is adapted to setup of smaller and larger Hotspot solutions for cafes, hotels, companies, communal residences, campgrounds, etc.

The **HotSpot Solution** consists of a **bintec elmeg** gateway installed onsite (with its own WLAN access point or additional connected WLAN device or wired LAN) and of the Hotspot server, centrally located at a computing centre. The operator account is administered on the server via an administration terminal (e.g., a hotel reception PC); this includes functions such as registration entry, generating tickets, statistical analysis, etc.

Login sequence at the Hotspot server

- When a new user connects with the Hotspot, he/she is automatically assigned an IP address via DHCP.
- As soon as he attempts to access any Internet site with a browser, the user is redirected to the home/login page.
- After the user has entered the registration data (user/password), these are sent to the central RADIUS server (Hotspot server) as RADIUS registration.
- Following successful registration, the gateway opens Internet access.
- For each user, the gateway sends regular additional information to the RADIUS server for recording accounting data.
- When the ticket expires, the user is automatically logged off and again redirected to the home/login page.

Requirements

To operate a Hotspot, the customer requires:

- a **bintec elmeg** device as hotspot gateway with active Internet access and configured hotspot server entries for login and accounting (see menu **System Management->Remote Authentication->RADIUS->New** with **Group Description** *default group 0*)
- **bintec elmeg** Hotspot hosting (article number 5510000198)

- Access data
- Documentation
- Software licensing

Please note that you must first activate the licence.

Go to www.bintec-elmeg.com then **Service/Support -> Services -> Online Services**.

- Enter the required data (please note the relevant explanations on the license sheet), and follow the instructions of the online licensing.

- You then receive the Hotspot server's login data.



Note

Activation may require 2-3 business days.

Access data for gateway configuration

RADIUS Server IP	62.245.165.180
RADIUS Server Password	Set by Gigaset Communications GmbH
Domain	Individually set for customers by customer/dealer
Walled Garden Network	Individually set for customers by customer/dealer
Walled Garden Server URL	Individually set for customers by customer/dealer
Terms & Conditions URL	Individually set for customers by customer/dealer

Access data for configuration of the Hotspot server

Admin URL	https://hotspot.bintec-elmeg.com/
Username	Individually set by bintec elmeg
Password	Individually set by bintec elmeg


15.9.1 HotSpot Gateway

In the **HotSpot Gateway** menu, you can configure the bintec elmeg gateway installed onsite for the **Hotspot Solution**.

A list of all configured hotspot networks is displayed in the **Local Services->HotSpot Gateway->HotSpot Gateway** menu.


You can use the **Enabled** option to enable or disable the corresponding entry.

15.9.1.1 Edit or New

You configure the hotspot networks in the **Local Services->HotSpot Gateway->HotSpot Gateway->** menu. Choose the **New** button to set up additional Hotspot networks.

The **Local Services->HotSpot Gateway->HotSpot Gateway->** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	<p>Choose the interface to which the Hotspot LAN or WLAN is connected. When operating over LAN, enter the Ethernet interface here (e. g. en1-0). If operating over WLAN, the WLAN interface to which the access point is connected must be selected.</p> <p> Caution</p> <p>For security reasons you cannot configure your device over an interface that is configured for the Hotspot. Therefore take care when selecting the interface you want to use for the Hotspot.</p> <p>If you select the interface over which the current configuration session is running, the current connection will be lost. You must then log in again over a reachable interface that is not configured for the Hotspot to configure your device.</p>
Domain at the HotSpot Server	Enter the domain name that you used when setting up the HotSpot server for this customer. The domain name is required so that the Hotspot server can distinguish between the different clients (customers).
Walled Garden	<p>Enable this function if you want to define a limited and free area of websites (intranet).</p> <p>The function is not activated by default.</p>

Field	Description
Walled Network / Netmask	<p>Only if Walled Garden is enabled.</p> <p>Enter the network address of the Walled Network and the corresponding Netmask of the intranet server.</p> <p>For the address range resulting from Walled Network / Netmask, clients require no authentication.</p> <p>Example: Enter 192.168.0.0 / 255.255.255.0, if all IP addresses from 192.168.0.0 to 19.168.0.255 are free. Enter 192.168.0.1 / 255.255.255.255, if only the IP address 192.168.0.1 is free.</p>
Walled Garden URL	<p>Only if Walled Garden is enabled.</p> <p>Enter the Walled Garden URL of the intranet server. Freely accessible websites must be reachable over this address.</p>
Terms & Conditions	<p>Only if Walled Garden is enabled.</p> <p>In the Terms & Conditions input field, enter the address of the general terms and conditions on the intranet server, or public server, e.g., http://www.webserver.de/agb.htm. The page must lie within the address range of the walled garden network.</p>
Additional freely accessible Domain Names	<p>Only if Walled Garden is enabled.</p> <p>Add further URLs or IP addresses with Add. The web pages can be accessed via these additional freely accessible addresses.</p>
Language for login window	<p>Here you can choose the language for the start/login page.</p> <p>The following languages are supported: <i>English, Deutsch, Italiano, Français, Español, Português</i> and <i>Nederlands</i>.</p> <p>The language can be changed on the start/login page at any time.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the menu **Advanced Settings**

Field	Description
Ticket Type	<p>Select the ticket type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Voucher</i>: Only the user name must be entered. Define a default password in the input field. • <i>Username/Password</i> (default value): User name and password must be entered.
Allowed HotSpot Client	<p>Here you can define which type of users can log in to the Hot-spot.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>All</i>: All clients are approved. • <i>DHCP Client</i>: Prevents users who have not received an IP address from DHCP from logging in.
Login Frameset	<p>Enable or disable the login window.</p> <p>The login window on the HTML homepage consists of two frames.</p> <p>When the function is enabled, the login form displays on the left-hand side.</p> <p>When the function is disabled, only the website with information, advertising and/or links to freely accessible websites is displayed.</p> <p>The function is enabled by default.</p>
Pop-Up window for status indication	<p>Specify whether the device uses pop-up windows to display the status.</p> <p>The function is enabled by default.</p>
Default Idle Timeout	<p>Enable or disable the Default Idle Timeout. If a hotspot user does not trigger any data traffic for a configurable length of time, they are logged out of the hotspot.</p> <p>The function is enabled by default.</p> <p>The default value is 600 seconds.</p>

15.9.2 Options

In the **Local Services->HotSpot Gateway->Options** menu, general settings are performed for the hotspot.

The **Local Services->HotSpot Gateway->Options** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Host for multiple locations	If several locations (branches) are set up on the Hotspot server, enter the value of the NAS identifier (RADIUS server parameter) that has been registered for this location on the Hotspot server.


15.10 Wake-On-LAN

With the function **Wake-On-LAN (WOL)** you can start network devices that are switched off via an integrated network card. The network card also needs a power supply, even when the computer is switched off. You can use filters and rule chains to define the conditions that need to be met to send the so-called magic packet, and select the interfaces that are to be monitored for the defined rule chains. Configuring the filters and rule chains is largely like configuring filters and rule chains in the menu **Access Rules**.

15.10.1 Wake-On-LAN Filter

The menu **Local Services->Wake-On-LAN->Wake-On-LAN Filter** displays a list of all the WOL filters that have been configured.

15.10.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to enter additional filters.

The **Local Services->Wake-On-LAN->Wake-On-LAN Filter->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter the name of the filter.

Field	Description
Service	<p>Select one of the preconfigured services. The extensive range of services configured ex works includes the following:</p> <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i> • <i>charge</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>The default value is <i>Any</i>.</p>
Protocol	<p>Select a protocol.</p> <p>The option <i>Any</i> (default value) matches any protocol.</p>
Type	<p>Only for Protocol = <i>ICMP</i></p> <p>Select the type.</p> <p>Possible values: <i>Any, Echo reply, Destination unreachable, Source quench, Redirect, Echo, Time exceeded, Timestamp, Timestamp reply</i>.</p> <p>See RFC 792.</p> <p>The default value is <i>Any</i>.</p>
Connection State	<p>With Protocol = <i>TCP</i>, you can define a filter that takes the status of the TCP connections into account.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Established</i>: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter. • <i>Any</i> (default value): All TCP packets match the filter.
Destination IP Address/Netmask	<p>Enter the destination IP address of the data packets and the corresponding netmask.</p>


Field	Description
Destination Port/ Range	<p>Only for Protocol = <i>TCP</i> or <i>UDP</i></p> <p>Enter a destination port number or a range of destination port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>-All-</i> (default value): The destination port is not specified. • <i>Specify port</i>: Enter a destination port. • <i>Specify port range</i>: Enter a destination port range.
Source IP Address/ Netmask	<p>Enter the source IP address of the data packets and the corresponding netmask.</p>
Source Port/Range	<p>Only for Protocol = <i>TCP</i> or <i>UDP</i></p> <p>Enter a source port number or a range of source port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>-All-</i> (default value): The destination port is not specified. • <i>Specify port</i>: Enter a destination port. • <i>Specify port range</i>: Enter a destination port range.
DSCP/TOS Filter (Layer 3)	<p>Select the Type of Service (TOS).</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Ignore</i> (default value): The type of service is ignored. • <i>DSCP Binary Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). • <i>DSCP Decimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • <i>DSCP Hexadecimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111. • <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63.

Field	Description
	<ul style="list-style-type: none"> • <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.
COS Filter (802.1p/Layer 2)	<p>Enter the service class of the IP packets (Class of Service, CoS).</p> <p>Possible values are whole numbers between 0 and 7. Value range 0 to 7.</p> <p>The default value is <i>Ignore</i>.</p>

15.10.2 WOL Rules

The menu **Local Services->Wake-On-LAN->WOL Rules** displays a list of all the WOL rules that have been configured.

15.10.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to enter additional rules.

The **Local Services->Wake-On-LAN->WOL Rules->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Wake-On-LAN Rule Chain	<p>Select whether to create a new rule chain or to edit an existing one.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>New</i> (default value): You can create a new rule chain with this setting. • <i><Name of the rule chain></i>: Shows a rule chain that has already been created, which you can select and edit.
Description	<p>Only where Wake-On-LAN Rule Chain = <i>New</i></p> <p>Enter the name of the rule chain.</p>
Wake-On-LAN Filter	Select a WOL filter.


Field	Description
	<p>If the rule chain is new, select the filter to be set at the first point of the rule chain.</p> <p>If the rule chain already exists, select the filter to be attached to the rule chain.</p> <p>To select a filter, at least one filter must be configured in the Wake-On-LAN->WOL Rules menu.</p>
Action	<p>Define the action to be taken for a filtered data packet.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Invoke WOL if filter matches</i>: Run WOL if the filter matches. • <i>Invoke if filter does not match</i>: Run WOL if the filter does not match. • <i>Deny WOL if filter matches</i>: Do not run WOL if the filter matches. • <i>Deny WOL if filter does not match</i>: Do not run WOL if the filter does not match. • <i>Ignore rule and skip to next rule</i>: This rule is ignored and the next one in the chain is examined.
Type	<p>Select whether the Wake on LAN magic packet is to be sent as a UDP packet or as an Ethernet frame via the interface specified in Send WOL packet via interface.</p>
Send WOL packet via interface	<p>Select the interface which is to be used to send the Wake on LAN magic packet.</p>
Target MAC-Address	<p>Only where Action = <i>Invoke WOL if filter matches</i> and <i>Invoke if filter does not match</i></p> <p>Enter the MAC address of the network device that is to be enabled using WOL.</p>
Password	<p>Only where Action = <i>Invoke WOL if filter matches</i> and <i>Invoke if filter does not match</i></p> <p>If the network device that is to be enabled supports the "SecureOn" function, enter the corresponding password for this device here. The device is only enabled if the MAC address and password are correct.</p>

15.10.3 Interface Assignment

In this menu, the configured rule chains are assigned to individual interfaces which are then monitored for these rule chains.

A list of all configured interface assignments is displayed in the **Local Services->Wake-On-LAN->Interface Assignment** menu.

15.10.3.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create other entries.

The **Local Services->Wake-On-LAN->Interface Assignment->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Select the interface for which a configured rule chain is to be assigned.
Rule Chain	Select a rule chain.

Chapter 16 Maintenance

This menu provides you with numerous functions for maintaining your device. It firstly provides a menu for testing availability within the network. You can manage your system configuration files. If more recent system software is available, you can use this menu to install it. If you need other languages for the configuration interface, you can import these. You can also trigger a system reboot in this menu.

16.1 Diagnostics

In the **Maintenance->Diagnostics** menu, you can test the availability of individual hosts, the resolution of domain names and certain routes.

16.1.1 Ping Test

You can use the ping test to check whether a certain host in the LAN or an internet address can be reached. The **Output** field displays the ping test messages. The ping test is launched by entering the IP address to be tested in **Test Ping Address** and clicking the **Go** button.

16.1.2 DNS Test

The DNS test is used to check whether the domain name of a particular host is correctly resolved. The **Output** field displays the DSN test messages. The ping test is launched by entering the domain name to be tested in **DNS Address** and clicking the **Go** button.

16.1.3 Traceroute Test

You use the traceroute test to display the route to a particular address (IP address or domain name), if this can be reached. The **Output** field displays the traceroute test messages. The ping test is launched by entering the IP address to be tested in **Traceroute Address** and clicking the **Go** button.

16.2 Software & Configuration

You can use this menu to manage the software version of your device, your configuration files and the language of the **GUI**.

16.2.1 Options

Your device contains the version of the system software available at the time of production. More recent versions may have since been released. You may therefore need to carry out a software update.

Every new system software includes new features, better performance and any necessary bugfixes from the previous version. You can find the current system software at www.gigasetpro.com. The current documentation is also available here.



Important

If you want to update your software, make sure you consider the corresponding release notes. These describe the changes implemented in the new system software.

The result of an interrupted update (e.g. power failure during the update) could be that your gateway no longer boots. Do not turn your device off during the update.

An update of BOOTmonitor and/or Logic is recommended in a few cases. In this case, the release notes refer expressly to this fact. Only update BOOTmonitor or Logic if bintec elmeg GmbH explicitly recommends this.

Flash

Your device saves its configuration in configuration files in the flash EEPROM (Electrically Erasable Programmable Read Only Memory). The data even remains stored in the flash when your device is switched off.

RAM

The current configuration and all changes you set on your device during operation are stored in the working memory (RAM). The contents of the RAM are lost if the device is switched off. So if you modify your configuration and want to keep these changes for the next time you start your device, you must save the modified configuration in the flash

memory before switching off: The **Save configuration** button over the navigation area of the **GUI**. This configuration is then saved in the flash in a file with the name *boot*. When you start your device, the *boot* configuration file is used by default.

Actions

The files in the flash memory can be copied, moved, erased and newly created. It is also possible to transfer configuration files between your device and a host via HTTP.

Configuration file format

The file format of the configuration file allows encryption and ensures compatibility when restoring the configuration on the gateway in various system software versions. This is a CSV format, which can be read and modified easily. In addition, you can view the corresponding file clearly using Microsoft Excel for example. The administrator can store encrypted backup files for the configuration. When the configuration is sent by e-mail (e.g for support purposes) confidential configuration data can be protected fully if required. You can save or import files with the actions "Export configuration", "Export configuration with status information" and "Load configuration". If you want to save a configuration file with the action ""Export configuration" or "Export configuration with status information", you can choose whether the configuration file is saved encrypted or without encryption.



Caution

If you have saved a configuration file in an old format via the SNMP shell with the `put` command, there is no guarantee that it can be reloaded to the device. As a result, the old format is no longer recommended.

The **Maintenance->Software & Configuration ->Options** menu consists of the following fields:

Fields in the Currently Installed Software menu

Field	Description
BOSS	Shows the current software version loaded on your device.
System Logic	Shows the current system logic loaded on your device.
ADSL Logic	Shows the current version of the ADSL logic loaded on your device.

Fields in the Software and Configuration Options menu

Field	Description
Action	<p>Select the action you wish to execute.</p> <p>After each task, a window is displayed showing the other steps that are required.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>No Action</i> (default value): • <i>Export configuration</i>: The configuration file Current File Name in Flash is transferred to your local host. If you click the Go button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name. • <i>Import configuration</i>: Under Filename select a configuration file you want to import. Please note: Click Go to first load the file under the name <i>boot</i> in the flash memory for the device. You must restart the device to enable it. <p>Please note: The files to be imported must be in CSV format!</p> <ul style="list-style-type: none"> • <i>Copy configuration</i>: The configuration file in the Source File Name field is saved as Destination File Name. • <i>Delete configuration</i>: The configuration in the Select file field is deleted. • <i>Rename configuration</i>: The configuration file in the Select file field is renamed to New File Name. • <i>Restore backup configuration</i>: Only if, under Save configuration with the setting <i>Save configuration and back up previous boot configuration</i> the current configuration was saved as boot configuration and the previous boot configuration was also archived. <p>You can load back the archived boot configuration.</p> <ul style="list-style-type: none"> • <i>Delete software/firmware</i>: The file in the Select file field is deleted. • <i>Import language</i>: You can import additional language versions of the GUI into your device. You can download the files to your PC from the download area at www.gigasetpro.com and from there import them to your device • <i>Update system software</i>: You can launch an update of the system software, the ADSL logic and the BOOTmonitor.

Field	Description
	<ul style="list-style-type: none"> • <i>Import Voice Mail Wave Files</i>: (Only displayed if an SD card is inserted.) In file name, select the <i>vms_wavfiles.zip</i> file that you wish to import. • <i>Export configuration with state information</i>: The active configuration from the RAM is transferred to your local host. If you click the Go button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name.
Action	<p>Select the action you wish to execute.</p> <p>After each task, a window is displayed showing the other steps that are required.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>No Action</i> (default value): • <i>Import configuration</i>: Under Filename select a configuration file you want to import. Please note: Click Go to first load the file under the name <i>boot</i> in the flash memory for the device. You must restart the device to enable it. <p>Please note: The files to be imported must be in CSV format!</p> <ul style="list-style-type: none"> • <i>Import language</i>: You can import additional language versions of the GUI into your device. You can download the files to your PC from the download area at www.gigasetpro.com and from there import them to your device. • <i>Update system software</i>: You can launch an update of the system software, the ADSL logic and the BOOTmonitor. • <i>Export configuration</i>: The configuration file Current File Name in Flash is transferred to your local host. If you click the Go button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name. • <i>Export configuration with state information</i>: The active configuration from the RAM is transferred to your local host. If you click the Go button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name. • <i>Restore backup</i>: Only if, under Save configuration with the setting <i>Save configuration and back up previ-</i>

Field	Description
	<p><i>ous boot configuration</i> the current configuration was saved as boot configuration and the previous boot configuration was also archived.</p> <p>You can load back the archived boot configuration.</p> <ul style="list-style-type: none"> • <i>Copy configuration</i>: The configuration file in the Source File Name field is saved as Destination File Name. • <i>Rename configuration</i>: The configuration file in the Select file field is renamed to New File Name. • <i>Delete configuration</i>: The configuration in the Select file field is deleted. • <i>Delete software/firmware</i>: The file in the Select file field is deleted.
Configuration Encryption	<p>Only for Action = <i>Import configuration, Export configuration, Export configuration with state information</i>. Define whether the data of the selected Action are to be encrypted..</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>If the function is enabled, you can enter the Password in the text field.</p>
Filename	<p>Only for Action = <i>Import configuration, Import language Update system software</i>.</p> <p>Enter the path and name of the file or select the file with Browse... via the explorer/finder.</p>
Source Location	<p>Only for Action = <i>Update system software</i></p> <p>Select the source of the update.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Local File</i> (default value): The system software file is stored locally on your PC. • <i>HTTP Server</i>: The file is stored on a remote server specified in the URL. • <i>Current Software from Update Server</i>: The file is

Field	Description
	on the official update server.
URL	Only for Source Location = <i>HTTP Server</i> Enter the URL of the update server from which the system software file is loaded.
Current File Name in Flash	For Action = <i>Export configuration</i> Select the configuration file to be exported.
Include certificates and keys	For Action = <i>Export configuration, Export configuration with state information</i> Define whether the selected Action should also be applied for certificates and keys. The function is activated by selecting <i>Enabled</i> . The function is enabled by default.
Source File Name	Only for Action = <i>Copy configuration</i> Select the source file to be copied.
Destination File Name	Only for Action = <i>Copy configuration</i> Enter the name of the copy.
Select file	Only for Action = <i>Rename configuration, Delete configuration or Delete software/firmware</i> Select the file or configuration to be renamed or deleted.
New File Name	Only for Action = <i>Rename configuration</i> Enter the new name of the configuration file.

16.3 Phone Update

In the **Maintenance->Phone Update** menu, you can update your system telephone software.

**Note**

Before beginning with the software update of your system telephone, you must load the software in the **Maintenance->Phone Update->Firmware Files** menu on your SD card.

16.3.1 Gigaset Phones


In the **Maintenance->Phone Update->Gigaset Phones** menu, you will see a list of the connected Gigaset telephones or base stations. This view displays both Gigaset telephones and Gigaset DECT base stations, if there are any. You can select devices to have their software updated immediately or allow them to download completely new software from the system.


In the case of immediate updating, there is no version control.

**Note**

Note that immediate software updates for DECT multi-cell systems are only available via the system's web configurator and that they cannot be initiated by the **elmeg hybrid** GUI.

Values in the list Gigaset Phones

Field	Description
Description	Displays the description entered for the system telephone.
Phone Type	Displays the system telephone type.
MAC Address	Shows the system telephone's MAC address.
Phone Version	Displays the software version of the telephone.
SD Card Vers.	Displays the inserted SD card version.
Status/Update Status	<p>Displays the system telephone status, or a progress bar during the update progress.</p> <p> identifies a connected system telephone whose system software is supported by your hybird.</p>

Field	Description
	<p> identifies a system telephone that is either not connected, or whose system software is not supported by your hybird.</p> <p>For IP telephone, there is no restriction on simultaneous updating of system software.</p> <p>If the system telephone system software is not supported by your hybird, there is still a way to update the system software.</p> <p>During system software updating, you see a progress bar.</p>
Update enabled	<p>Shows whether connected telephones can independently download new software from the system.</p> <p>You can select individual entries using the checkbox in the corresponding line, or select them all using the Select all button or the Deselect all button.</p>
Update immediately	<p>Displays whether the system telephone software should be updated immediately.</p> <p>This function is enabled on an individual device by setting a checkmark. The function is disabled by default.</p> <p>You can use the Select all and Deselect all buttons for all the devices displayed.</p>

16.3.2 Firmware Files

In the **Maintenance->Phone Update->Firmware Files** menu, you see the system software files that are currently available on your SD card. You can load additional files on the SD card.




Note

For DECT systems there is a ZIP file available which contains the system software files and, for **Gigaset N510 IP PRO**, language files too.

**Note**

One version of the system software file per telephone type can be saved on the SD card.

Values in the list Firmware Files

Field	Description
Load firmware	Save the system software files on your SD card.
No.	Displays the serial number of the system software file on your SD card.
Phone Type	Displays the system telephone type.
Version	Displays the version of the system software.
Status	 indicates that a system software file is saved on the SD card in the correct directory.

16.3.3 Settings

In the **Maintenance->Phone Update->Settings** menu, you can set a period for the time-dependent updating of the system software. You can save a telephone number that may be used in case a system software update has failed. You can dial this number with the telephone in order to update the system software once the telephone is in boot mode following a failed update.

The **Maintenance->Phone Update->Settings** menu consists of the following fields:

Fields in the menu Time Settings for System Phone Firmware Update

Field	Description
Internal Number	<p>For ISDN system telephones only</p> <p>Enter the number of the hybird update server that you wish to call from the telephone if the system software update fails. In this case, you can perform the update from the telephone.</p> <p>This number is automatically sent to the system telephone when the telephone logs into the hybird.</p>

Field	Description
	When it has been sent, the number is displayed on the telephone under Menu->Service->Software Update . If you press the OK button, the number is available in redial.
Firmware Update	Set a period for updating the system software. To do this, select the Start Time and the Stop Time .

16.4 Reboot

16.4.1 System Reboot

In this menu, you can trigger an immediate reboot of your device. Once your system has restarted, you must call the **GUI** again and log in.

Pay attention to the LEDs on your device. For information on the meaning of the LEDs, see the **Technical Data** chapter of the manual.



Note

Before a reboot, make sure you confirm your configuration changes by clicking the **Save configuration** button, so that these are not lost when you reboot.

If you wish to restart your device, click the **OK** button. The device will reboot.

Chapter 17 External Reporting

In this system menu, you define what system protocol messages are saved on which computers, and whether the system administrator should receive an e-mail for certain events. Information on IP data traffic can also be saved--depending on the individual interfaces. In addition, SNMP traps can be sent to specific hosts in case of error. Moreover, you can prepare your device for monitoring with the activity monitor.

17.1 Syslog

Events in various subsystems of your device (e.g. PPP) are logged in the form of syslog messages (system logging messages). The number of messages visible depends on the level set (eight steps from *Emergency over Information to Debug*).

In addition to the data logged internally on your device, all information can and should be transmitted to one or more external PCs for storage and processing, e.g. to the system administrator's PC. The syslog messages saved internally on your device are lost when you reboot.



Warning

Make sure you only pass syslog messages to a safe computer. Check the data regularly and ensure that there is always enough spare capacity available on the hard disk of your PC.

Syslog Daemon

All Unix operating systems support the recording of syslog messages. For Windows PCs, the Syslog Demon included in the **DIME Tools** can record the data and distribute to various files depending on the contents (can be called in the download area at www.bintec-elmeg.com).

17.1.1 Syslog Servers

Configure your device as a syslog server so that defined system messages can be sent to suitable hosts in the LAN.

In this menu, you define which messages are sent to which hosts and with which conditions.

A list of all configured system log servers displayed in the **External Reporting->Syslog->Syslog Servers** menu.

17.1.1.1 New

Select the **New** button to set up additional syslog servers.

The menu **External Reporting->Syslog->Syslog Servers->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
IP Address	Enter the IP address of the host to which syslog messages are passed.
Level	<p>Select the priority of the syslog messages that are to be sent to the host.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Emergency</i> (highest priority) • <i>Alert</i> • <i>Critical</i> • <i>Error</i> • <i>Warning</i> • <i>Notice</i> • <i>Information</i> (default value) • <i>Debug</i> (lowest priority) <p>Syslog messages are only sent to the host if they have a higher or identical priority to that indicated, i.e. at syslog level <i>Debug</i> all messages generated are forwarded to the host.</p>
Facility	<p>Enter the syslog facility on the host.</p> <p>This is only required if the Log Host is a Unix computer.</p> <p>Possible values: <i>local0</i> - 7</p> <p>.</p> <p>The default value is <i>local0</i>.</p>

Field	Description
Timestamp	<p>Select the format of the time stamp in the syslog.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i> (default value): No system time indicated. • <i>Time</i>: System time without date. • <i>Date &Time</i>: System time with date.
Protocol	<p>Select the protocol for the transfer of syslog messages. Note that the syslog server must support the protocol.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>UDP</i> (default value) • <i>TCP</i>
Type of Messages	<p>Select the message type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>System &Accounting</i> (default value) • <i>System</i> • <i>Accounting</i>

17.2 IP Accounting

In modern networks, information about the type and number of data packets sent and received over the network connections is often collected for commercial reasons. This information is extremely important for Internet Service Providers that bill their customers by data volume.

However, there are also non-commercial reasons for detailed network accounting. If, for example, you manage a server that provides different kinds of network services, it is useful for you to know how much data is generated by the individual services.

Your device contains the IP Accounting function, which enables you to collect a lot of useful information about the IP network traffic (each individual IP session).

17.2.1 Interfaces

In this menu, you can configure the IP Accounting function individually for each interface.

In the **External Reporting->IP Accounting->Interfaces** menu, a list of all interfaces configured on your device is shown. For each entry, you can activate IP Accounting by setting the checkmark. In the **IP Accounting** column, you do not need to click each entry individually. Using the options **Select all** or **Deselect all** you can enable or disable the IP accounting function for all interfaces simultaneously.

17.2.2 Options

In this menu, you configure general settings for IP Accounting.

In the **External Reporting->IP Accounting->Options** menu, you can define the **Log Format** of the IP accounting messages. The messages can contain character strings in any order, sequences separated by a slash, e.g. `\t` or `\n` or defined tags.

Possible format tags:

Format tags for IP Accounting messages

Field	Description
%d	Date of the session start in the format DD.MM.YY
%t	Time of the session start in the format HH:MM:SS
%a	Duration of the session in seconds
%c	Protocol
%i	Source IP Address
%r	Source Port
%f	Source interface index
%l	Destination IP Address
%R	Destination Port
%F	Destination interface index
%p	Packets sent
%o	Octets sent
%P	Packets received
%O	Octets received
%s	Serial number for accounting message
%%	%

By default, the following format instructions are entered in the **Log Format** field: `INET:`

```
%d%t%a%c%i:%r/%f -> %I:%R/%F%p%o%P%O[%s]
```

17.3 Alert Service

It was previously possible to send syslog messages from the router to any syslog host. Depending on the configuration, e-mail alerts are sent to the administrator as soon as relevant syslog messages appear.

17.3.1 Alert Recipient

A list of Syslog messages is displayed in the **Alert Recipient** menu.

17.3.1.1 New

Select the **New** to create additional alert recipients.

The menu **External Reporting->Alert Service->Alert Recipient->New** consists of the following fields:

Fields in the Add / Edit Alert Recipient menu

Field	Description
Alert Service	Displays the alert service.
Recipient	Enter the recipient's e-mail address. The entry is limited to 40 characters.
Message Compression	Select whether the text in the alert E-mail is to be shortened. The e-mail then contains the syslog message only once plus the number of relevant events. Enable or disable the field. The function is enabled by default.
Subject	You can enter a subject.
Matching String	You must enter a "Matching String". This must occur in a syslog message as a necessary condition for triggering an alert. The entry is limited to 55 characters. Bear in mind that without the use of wildcards (e.g. "*"), only those strings that correspond exactly to the entry fulfil the condition. The "Matching String" entered therefore usually contains wildcards. To be informed of all syslog messages of the selected level, just enter

Field	Description

Severity	<p>Select the severity level which the string configured in the Matching String field must reach to trigger an e-mail alert.</p> <p>Possible values:</p> <p><i>Emergency (default value), Alert, Critical, Error, Warning, Notice, Information, Debug</i></p>
Monitored Subsystems	<p>Select the subsystems to be monitored.</p> <p>Add new subsystems with Add.</p>
Message Timeout	<p>Enter how long the router must wait after a relevant event before it is forced to send the alert mail.</p> <p>Possible values are 0 to 86400. The value 0 disables the timeout. The default value is 60.</p>
Number of Messages	<p>Enter the number of syslog messages that must be reached before an E-mail can be sent for this case. If timeout is configured, the mail is sent when this expires, even if the number of messages has not been reached.</p> <p>Possible values are 0 to 99; the default value is 1.</p>

17.3.2 Alert Settings

The menu **External Reporting->Alert Service->Alert Settings** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Alert Service	<p>Select whether the alert service is to be enabled for the interface.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Maximum E-mails per	Limit the number of outgoing mails per minute. Possible values

Field	Description
Minute	are 1 to 15, the default value is 6.

Fields in the E-mail Parameters menu

Field	Description
Sender E-mail Address	Enter the mail address to be entered in the sender field of the E-mail.
SMTP Server	Enter the address (IP address or valid DNS name) of the mail server to be used for sending the mails. The entry is limited to 40 characters.
SMTP Authentication	Authentication expected by the SMTP server. Possible values: <ul style="list-style-type: none"> • <i>None</i> (default value): The server accepts and send emails without further authentication. • <i>ESMTP</i>: The server only accepts e-mails if the router logs in with the correct user name and password. • <i>SMTP after POP</i>: The server requires that e-mails are called via POP3 by the sending IP with the correct POP3 user name and password before sending an e-mail.
User Name	Only if SMTP Authentication = <i>ESMTP</i> or <i>SMTP after POP</i> Enter the user name for the POP3 or SMTP server.
Password	Only if SMTP Authentication = <i>ESMTP</i> or <i>SMTP after POP</i> Enter the password of this user.
POP3 Server	Only if SMTP Authentication = <i>SMTP after POP</i> Enter the address of the server from which the e-mails are to be retrieved.
POP3 Timeout	Only if SMTP Authentication = <i>SMTP after POP</i> Enter how long the router must wait after the POP3 call before it is forced to send the alert mail. The default value is 600 seconds.

17.4 SNMP

SNMP (Simple Network Management Protocol) is a protocol from the IP protocol family for transporting management information about network components.

Every SNMP management system contains an MIB. SNMP can be used to configure, control and administrate various network components from one system. Such an SNMP tool is included on your device: the Configuration Manager. As SNMP is a standard protocol, you can use any other SNMP managers, e.g. HPOpenView.

For more information on the SNMP versions, see the relevant RFCs and drafts:

- SNMP V. 1: RFC 1157
- SNMP V. 2c: RFC 1901 - 1908
- SNMP V. 3: RFC 3410 - 3418

17.4.1 SNMP Trap Options

In the event of errors, a message - known as a trap packet - is sent unrequested to monitor the system.

In the **External Reporting->SNMP->SNMP Trap Options** menu, you can configure the sending of traps.

The menu **External Reporting->SNMP->SNMP Trap Options** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
SNMP Trap Broadcasting	<p>Select whether the transfer of SNMP traps is to be activated.</p> <p>Your device then sends SNMP traps to the LAN's broadcast address.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
SNMP Trap UDP Port	<p>Only if SNMP Trap Broadcasting is enabled.</p> <p>Enter the number of the UDP port to which your device is to send SNMP traps.</p>

Field	Description
	Any whole number is possible. The default value is <i>162</i> .
SNMP Trap Community	Only if SNMP Trap Broadcasting is enabled. Enter a new SNMP code. This must be sent by the SNMP Manager with every SNMP request so that this is accepted by your device. A character string of between <i>0</i> and <i>255</i> characters is possible. The default value is <i>SNMP Trap</i> .

17.4.2 SNMP Trap Hosts

In this menu, you specify the IP addresses to which your device is to send the SNMP traps.

In the **External Reporting->SNMP->SNMP Trap Hosts** menu, a list of all configured SNMP trap hosts is displayed.

17.4.2.1 New

Select the **New** button to create additional SNMP trap hosts.

The menu **External Reporting->SNMP->SNMP Trap Hosts->New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
IP Address	Enter the IP address of the SNMP trap host.

Chapter 18 Monitoring


This menu contains information that enable you to locate problems in your network and monitor activities, e.g. at your device's WAN interface.

18.1 Status Information

This menu displays current settings for terminals and team subscribers. This data is continuously read out.

18.1.1 Users

In the **Monitoring->Status Information->Users** menu, current settings for a user's internal number (MSN) are displayed.

By pressing the  button, you display detailed statistics on the respective user.

Values in the Extension Status list

Field	Description
Number	Displays the user's internal number.
Name	Displays the name assigned to the user. If a voicemail system is active, <i>Voice Mail System</i> is displayed.
Current Class of Service	Displays the all of the authorisation classes assigned to the user. The currently enabled authorisation class is marked appropriately with a green arrow (➔).
Terminal	Displays the interface assigned to this subscriber.
Charges	Displays calculated charges for accrued connection units.
Status	Displays the status of the interface to which the subscriber is connected.


Values in the System Settings list

Field	Description
Parallel Ringing	Displays whether parallel call is set up for the user.
Call Forwarding	Displays current call forwarding for this user.

Field	Description
Do not Disturb	Displays whether call waiting protection is set up for the user. (Only for system telephones)
Call Waiting	Displays whether call waiting is allowed for internal and/or external calls.
Direct Call	Displays whether direct call on receiver pickup is configured for the user.
Room Monitoring	Displays whether room monitoring is enabled for the user.
Receive Announcement Calls	Displays whether the announcement is allowed for the user.
Receive Intercom Calls	Displays whether simplex operation is allowed for the user.
Automatic Call Pick-up	Displays whether automatic call acceptance is configured for the user.

18.1.2 Teams

In the **Monitoring->Status Information->Teams** menu, current team settings are displayed.

By pressing the  button, you display detailed statistics for the respective team.

Values in the Team Status list

Field	Description
Name	Displays the name assigned to the team.
Number	Displays the team's internal number.
Users assigned/Users logged on	Displays the users assigned to the team, and how many of these users are logged in.
Call Forwarding	Displays current call forwarding for this team.

Values in the System Settings list

Field	Description
Active Variant (Day)	Displays the currently enabled call option for this team.
Switch call signalling	Displays whether the call option can be switched manually, over the calendar or manually and over the calendar.
Signalling	Displays the type of call signalling in the team.
Busy on busy	Displays whether busy on busy is configured for the team.
Automatic Call Pick-up	Displays whether automatic call acceptance is configured, and which melody is played.

Field	Description
Rerouting on no response	Displays whether redirect on no reply is enabled and, if so, the time period after which it occurs and the destination team.
Further Rerouting	Displays which of the redirect functions are enabled and which subscriber is the redirect destination.

The menu **Advanced Settings** consists of the following fields:

Values in the Advanced Settings list

Field	Description
Assigned Users	Displays all logged-in and logged-out subscribers in the team.

18.2 Internal Log

18.2.1 System Messages

In the **Monitoring->Internal Log->System Messages** menu, a list of all internally stored system messages is displayed. Above the table you will find the configured values for the **Maximum Number of Syslog Entries** and **Maximum Message Level of Syslog Entries** fields. These values can be changed in the **System Management->Global Settings->System** menu.

Values in the System Messages list

Field	Description
No.	Displays the serial number of the system message.
Date	Displays the date of the record.
Time	Displays the time of the record.
Level	Displays the hierarchy level of the message.
Subsystem	Displays which subsystem of the device generated the message.
Message	Displays the message text.



18.3 IPSec


18.3.1 IPSec Tunnels

A list of all configured IPSec tunnel providers is displayed in the **Monitoring->IPSec->IPSec Tunnels** menu.

Values in the IPSec Tunnels list

Field	Description
Description	Displays the name of the IPSec tunnel.
Remote IP	Displays the IP address of the remote IPSec Peers.
Remote Networks	Displays the currently negotiated subnets of the remote terminal.
Security Algorithm	Displays the encryption algorithm of the IPSec tunnel.
Status	Displays the operating status of the IPSec tunnel.
Action	Enables you to change the status of the IPSec tunnel as displayed.
Details	Opens a detailed statistics window.

You change the status of the IPSec tunnel by clicking the  button or the  button in the **Action** column.

By clicking the  button, you display detailed statistics on the IPSec connection.

Values in the IPSec Tunnels list

Field	Description
Description	Shows the description of the peer.
Local IP Address	Shows the WAN IP address of your device.
Remote IP Address	Shows the WAN IP address of the connection partner.
Local ID	Shows the ID of your device for this IPSec tunnel.
Remote ID	Shows the ID of the peer.
Negotiation Type	Shows the exchange type.
Authentication Method	Shows the authentication method.
MTU	Shows the current MTU (Maximum Transfer Unit).
Alive Check	Shows the method for checking that the peer is reachable.
NAT Detection	Displays the NAT detection method.
Local Port	Shows the local port.

Field	Description
Remote Port	Shows the remote port.
Packets	Shows the total number of incoming and outgoing packets.
Bytes	Shows the total number of incoming and outgoing bytes.
Errors	Shows the total number of errors.
IKE (Phase-1) SAs (x) Role / Algorithm / Lifetime remaining / Status	The parameters of the IKE (Phase 1) SAs are displayed here.
IPSec (Phase-2) SAs (x) Role / Algorithm / Lifetime remaining / Status	Shows the parameters of the IPSec (Phase 2) SAs.
Messages	The system messages for this IPSec tunnel are displayed here.

18.3.2 IPSec Statistics

In the **Monitoring->IPSec->IPSec Statistics** menu, statistical values for all IPSec connections are displayed.

The **Monitoring->IPSec->IPSec Statistics** menu consists of the following fields:

Fields in the Licences menu

Field	Description
IPSec Tunnels	Shows the IPSec licences currently in use (In Use) and the maximum number of licenses usable (Maximum).

Fields in the Peers menu

Field	Description
Status	Displays the number of IPSec tunnels by their current status. <ul style="list-style-type: none"> • Up: Currently active IPSec tunnels. • Going up: IPSec tunnels currently in the tunnel setup phase. • Blocked: IPSec tunnels that are blocked. • Dormant: Currently inactive IPSec tunnels.

Field	Description
	<ul style="list-style-type: none"> • Configured: Configured IPsec tunnels.

Fields in the SAs menu

Field	Description
IKE (Phase-1)	Shows the number of active phase 1 SAs (Established) from the total number of phase 1 SAs (Total).
IPsec (Phase-2)	Shows the number of active phase 2 SAs (Established) from the total number of phase 2 SAs (Total).

Fields in the Packet Statistics menu



Field	Description
Total	Shows the number of all processed incoming (In) or outgoing (Out) packets.
Passed	Shows the number of incoming (In) or outgoing (Out) packets forwarded in plain text.
Dropped	Shows the number of all rejected incoming (In) or outgoing (Out) packets.
Encrypted	Shows the number of all incoming (In) or outgoing (Out) packets protected by IPsec.
Errors	Shows the number of incoming (In) or outgoing (Out) packets for which processing led to errors.

18.4 Interfaces

18.4.1 Statistics

In the **Monitoring->Interfaces->Statistics** menu, current values and activities of all device interfaces are displayed.

With the filter bar, you can select whether to display **Transfer Totals** or **Transfer Throughput**. The values per second are shown on the **Transfer Throughput** display.

Change the status of the interface by clicking the  or the  button in the **Action** column.

Values in the Statistics list

Field	Description
No.	Shows the serial number of the interface.

Field	Description
Description	Displays the name of the interface.
Type	Displays the interface text.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Tx Errors	Shows the total number of errors sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.
Rx Errors	Shows the total number of errors received.
Status	Shows the operating status of the selected interface.
Unchanged for	Shows the length of time for which the operating status of the interface has not changed.
Action	Enables you to change the status of the interface as displayed.

Press the  button to display the statistical data for the individual interfaces in detail.

Values in the Statistics list

Field	Description
Description	Displays the name of the interface.
MAC Address	Displays the interface text.
IP Address / Netmask	Shows the IP address and the netmask.
NAT	Indicates if NAT is activated for this interface.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.

Fields in the TCP Connections menu

Field	Description
Status	Displays the status of an active TCP connection.
Local Address	Displays the local IP address of the interface for an active TCP connection.
Local Port	Displays the local port of the IP address for an active TCP connection.
Remote Address	Displays the IP address to which an active TCP connection exists.

Field	Description
Remote Port	Displays the port to which an active TCP connection exists.

18.5 HotSpot Gateway

18.5.1 HotSpot Gateway

A list of all linked hotspot users is displayed in the **Monitoring->HotSpot Gateway->HotSpot Gateway** menu.

Values in the HotSpot Gateway list

Field	Description
User Name	Displays the user's name.
IP Address	Shows the IP address of the user.
Physical Address	Shows the physical address of the user.
Logon	Displays the time of the notification.
Interface	Shows the interface used.

18.6 QoS

In the **Monitoring->QoS** menu, statistics are displayed for interfaces on which QoS has been configured.

18.6.1 QoS

A list of all interfaces for which QoS was configured is displayed in the **Monitoring->QoS->QoS** menu.

Values in the QoS list

Field	Description
Interface	Shows the interface for which QoS has been configured.
QoS Queue	Shows the QoS queue, which has been configured for this interface.
Send	Shows the number of sent packets with the corresponding

Field	Description
	packet class.
Dropped	Shows the number of rejected packets with the corresponding packet class in case of overloading.
Queued	Shows the number of waiting packets with the corresponding packet class in case of overloading.

Index

- Description 58
- ISDN Timeserver 14
- System Admin Password 10
- Gigaset DECT 119

- #

- #1 #2, #3 47

- A**

- Access 333
- Access Configuration 61
- Access Filter 218
- Access Level 40
- Access Type 54 , 76
- Access Filter 214
- Access Profiles 38
- Access Codes 19
- Access Rules 213
- ACCESS_ACCEPT 30
- ACCESS_REJECT 30
- ACCESS_REQUEST 30
- ACCOUNTING_START 30
- ACCOUNTING_STOP 30
- Action 57 , 154 , 218 , 304 , 340 ,
365 , 370 , 391 , 393
- Action to be performed 351
- Actions 340
- Active Variant 161 , 169
- Active Calls 160
- Active Variant 173
- Active Doorcom Variant 166
- Active IPsec Tunnels 3
- Active Sessions (SIF, RTP, etc...) 3
- Active Variant (Day) 88 , 106 , 113
- Active Variant (Day) 389
- Add 24
- Additional Traffic Filter 256 , 258
- Additional freely accessible Domain
Names 359
- Additional Info for Extern Call 93

- Address Mode 180
- Address Range 310
- Address Type 310
- Address List 309
- Address / Subnet 310
- Addresses 69 , 309
- Admin Password 118 , 122
- Administration 185
- Administrative Status 253 , 318
- Administrative Access 24
- ADSL Logic 370
- Agents 163
- Agents assigned 160
- Agents in Wrap-up 160
- Agents logged on 160
- Alarm Signalling Period 170
- Alarm Calls 169
- Alarm Input 9
- Alert Service 383
- Alert Service 384
- Alert Recipient 383
- Alert Settings 384
- Alert Service 383
- Alive Check 32 , 270 , 275
- Alive Check 391
- All Multicast Groups 229
- Allow manual trunk group selection
91
- Allowed HotSpot Client 360
- Always on 233 , 237 , 241 , 286 , 291
- Analogue 127
- Analogue Ports 57
- Announcement 146
- Answer to client request 356
- Answered of Calls Today 160
- Application 142
- Applications 103 , 141
- Apply QoS 304
- ARP Lifetime 220
- ARS 137
- As DHCP Server 317
- As IPCP Server 317
- Assign project codes 20
- Assigned Users 390

- Assignment 108 , 113 , 150 , 167
- Assistants 1
- Authentication 235 , 239 , 244 , 288 , 294
- Authentication ID 61
- Authentication Method 253 , 266
- Authentication Type 31 , 35
- Authentication Method 391
- Authentication for PPP Dialin 37
- Authorization 114
- Authorizations 89
- Auto Attendant with DISA 148
- Automatic Call Pick-up with 110 , 162
- Automatic Call Pick-up 388 , 389
- Automatic Outside Line 91
- Automatic Route Selection (ARS) 93
- Automatic Route Selection 137
- Autosave Mode 48 , 340

- B**
- Back Route Verify 260
- Back Route Verify 192
- Back-up of configuration on SD card 2
- Based on Ethernet Interface 180
- Basic Settings 90
- Bell ID 166
- Bell Name 166
- Block after connection failure for 235 , 239 , 244 , 288 , 294
- Block Time 36 , 270
- BOSS 370
- BOSS Version 2
- Burst size 209
- Busy on busy 85 , 110
- Busy on busy 389
- Busy starting with 111
- Busy Tone Detection 59
- Busy when 162
- Bytes 391

- C**
- CA Certificate 44
- CA Certificates 270
- CA Name 340
- Cache 322
- Cache Hitrate (%) 322
- Cache Hits 322
- Cache Size 316
- Calendar 141
- Calendar for status "Out of Office" 173
- Call Forwarding extern (SIP 302) 65
- Call Number 247
- Call Switching 148
- Call Through 90 , 96 , 153
- Call Waiting 96 , 128
- Call Forwarding 388 , 389
- Call Waiting 388
- Call Forwarding 133
- Call Distribution 112
- Call Center Description 161
- Call Data Records 156
- Call Forwarding (CFNR) 16
- Call Forwarding to External Numbers 106
- Call Hold inside the PBX system 65 , 78
- Call Routing 132
- Call Signalisation Timer 167
- Call-prefix 138
- Callback 296
- Callback Mode 244
- Called Number 157
- CAPI 130
- CAPI Server 333
- CAPI Server TCP Port 334
- Certificate Request 44
- Certificate List 42
- Certificate Servers 50
- Certificate is CA Certificate 42
- Certificate Request Description 44 , 340
- Certificate Revocation List (CRL) Checking 42
- Certificates 41
- Channel Bundling 246

- Charge Information (S0 / Upn Extension) 8
 - Charge Rate Factor 8
 - Charges 388
 - Check PIN 175
 - Class ID 203 , 209
 - Class map 203
 - Class of Services 90
 - Client Registration Timer 74
 - CLIP 58
 - Code 311
 - Code for Doorcom Call Acceptance 165
 - Codec Profile 118 , 121 , 125
 - Codec Profiles 65
 - Codec Profiles 71
 - Codec Proposal Sequence 72
 - Command Mode 340
 - Command Type 340
 - Common Name 46
 - Compare Condition 336
 - Compare Value 336
 - Compression 27 , 294
 - Config Mode 255
 - Configuration Encryption 370
 - Configuration Access 37
 - Configuration contains
 - certificates/keys 340
 - Configuration Interface 23
 - Configured Speed / Mode 52
 - Confirm Admin Password 10
 - Congestion Avoidance (RED) 212
 - Connection State 201 , 214 , 362
 - Connection Type 241 , 286
 - Connection Idle Timeout 233 , 237 , 241 , 286 , 291
 - Connections Nr. 118
 - Consider public holidays 143
 - Contact 4
 - Control Mode 206 , 250
 - Controlled Interfaces 249
 - COS Filter (802.1p/Layer 2) 201 , 214 , 362
 - Costs 157
 - Count 340
 - Country 46
 - Country Profile 7
 - CPU Usage 3
 - Create NAT Policy 234 , 238 , 242 , 287 , 293
 - CRLs 49
 - CSV File Format 340
 - Currency 8
 - Current Class of Service 388
 - Current File Name in Flash 370
 - Current Local Time 13
 - Current Speed / Mode 52
 - Custom 46
- D**
- D Channel Mode 264
 - Data Packets Sequence Numbers 285
 - Date 12 , 157 , 157 , 390
 - Date (DD - MM) 144
 - Deactivate number suppression 65
 - Default MSN 56
 - Default Route 234 , 238 , 242 , 255 , 287 , 293 , 299
 - Default Behavior 69
 - Default MSN 56
 - Default Idle Timeout 360
 - Default User Password 31
 - Delete 192
 - Delete SIP bindings after Restart 65
 - Delete Phonebook 156
 - Delete call data records 159
 - Delete complete IPSec configuration 279
 - Description 38 , 42 , 50 , 54 , 57 , 61 , 69 , 72 , 76 , 81 , 83 , 91 , 106 , 116 , 120 , 123 , 126 , 127 , 130 , 131 , 133 , 136 , 138 , 139 , 142 , 144 , 145 , 149 , 151 , 153 , 161 , 166 , 169 , 177 , 189 , 195 , 201 , 203 , 209 , 214 , 218 , 233 , 237 , 241 , 253 , 258 , 266 , 273 , 277 , 283 , 286 , 291 , 299 , 309 , 310 ,

- 310 , 311 , 313 , 318 , 332 , 336 ,
340 , 362 , 365 , 375 , 391 , 391 ,
393 , 394
- Description - Connection Information -
Link 4
- Destination 304
- Destination Interface 229
- Destination Port 189 , 258
- Destination Port/Range 196 , 201 ,
214 , 362
- Destination File Name 370
- Destination IP Address 336 , 340 ,
354
- Destination IP Address/Netmask 188
, 196 , 201 , 214 , 258 , 362
- Destination IP Address 192
- Destination Port Range 311
- Details 391
- DH Group 266
- DHCP Hostname 181
- DHCP Options 329
- DHCP Configuration 328
- DHCP Broadcast Flag 181
- DHCP Client on Interface 220
- DHCP MAC Address 181
- DHCP Relay Settings 332
- DHCP Server 327
- Diagnostics 368
- Dial Control 93
- Dial Control 135
- Dial End Monitoring Time 65
- Dial Tone Detection 59
- Dial Tone Pause 59
- Dialling Authorization 91
- Dialling Method 58
- Dialling Method 57
- Direct Call 16 , 388
- Direct Call 132
- Direct Call Number 133
- Direction 203
- Display Language 7
- Displayed Description 86 , 88 , 118 ,
122
- Displayed Name 79
- DNS 314
- DNS Hostname 320
- DNS Negotiation 235 , 239 , 247 ,
289 , 295
- DNS Server 249 , 279 , 298 , 321 ,
328
- DNS Requests 322
- DNS Servers 318
- DNS Test 368
- Do not Disturb 128
- Do not Disturb 388
- Domain 61 , 321
- Domain Forwarding 320
- Domain at the HotSpot Server 359
- Domain Name 316
- Doorcom Access 103
- Doorcom Signalling 9
- Doorcom Signalling 166
- Doorcom Units 164
- Doorcom Signalling Variant 1 and 2
167
- Downstream Bandwidth Limitation 69
- Drop non-members 184
- Drop In 220
- Drop In Groups 220
- Drop untagged frames 184
- Dropped 393 , 395
- Dropping Algorithm 212
- DSA Key Status 26
- DSCP / TOS Value 189
- DSCP Settings for rtp Traffic 71
- DSCP Settings for sip Traffic 74
- DSCP/TOS Filter (Layer 3) 201 , 214
, 362
- DSP Module 3
- DTMF 72
- Duration 157 , 157
- Dynamic RADIUS Authentication 280
- DynDNS Provider 326
- DynDNS Update 324
- DynDNS Client 324

E

E-mail 46

- E-mail Address 84
 - E-Mail Notification 173
 - E-Mail Address (from User Settings) 173
 - Early media support 65
 - Enable update 324
 - Enable IPSec 279
 - Enable server 334
 - Enable VLAN 185
 - Enabled 299
 - Enabled number 136
 - Encrypt configuration 340
 - Encrypted 393
 - Encryption 36 , 244 , 288 , 294
 - Encryption Algorithms 26
 - End-of-Selection Signal 59
 - Entries 153 , 247
 - Entry active 31 , 35
 - Errors 391 , 393
 - Ethernet Ports 51
 - Ethernet Interface Selection 52
 - Event Type 336
 - Event List 336 , 340
 - Event List Condition 340
 - Exclude from NAT (DMZ) 220
 - Explicit Call Transfer 17
 - Export call data records 159
 - Extended Route 192
 - Extension Rerouting 9
 - External Assignment 108 , 167
 - External Connection Timer 170
 - External Filename 48 , 49
 - External Number 105 , 161
 - External Number 157
 - External Reporting 379
 - External Door Connections 16
- F**
- Facility 380
 - Fallback interface to get DNS server 316
 - Faxheader 334
 - Features 94
 - File Encoding 48 , 49
 - File Name 340
 - File Name in Flash 340
 - Filename 370
 - Filter 203
 - Filter Rules 306
 - Filter Rules 303
 - Firewall 302
 - Firewall Status 307
 - Firmware Update 377
 - Firmware Files 376
 - First Timeserver 14
 - First External Number 171
 - Flash Time for DTMF Dialling 129
 - Force certificate to be trusted 42
 - Forward 321
 - Forward to 321
 - Forwarded Requests 322
 - Forwarding 228
 - From Domain 65
 - Full Filtering 307
 - Further Rerouting 111 , 162
 - Further Rerouting 389
 - FXO 57
 - FXS 59
 - FXS Ringing Frequency 129
- G**
- G.711 aLaw 72
 - G.711 uLaw 72
 - G.722 72
 - G.726 (16 kbit/s) 72
 - G.726 (24 kbit/s) 72
 - G.726 (32 kbit/s) 72
 - G.726 (40 kbit/s) 72
 - G.726 Codec settings 72
 - G.729 72
 - Gateway 192 , 329
 - Gateway IP Address 188
 - General 106 , 116 , 120 , 137 , 149 , 156 , 158 , 160 , 164 , 166 , 177 , 224 , 356
 - Generate international phone number 65
 - Generate national subscriber number

- 65
- Generate Private Key 44
- Gigaset Phones 116 , 375
- Gigaset Phones 116
- Global Rerouting 9 , 9
- Global Settings 316
- Global Settings 4
- Global CLIP no Screening Number
62 , 77
- GRE 299
- GRE Tunnels 299
- GRE Window Adaption 297
- GRE Window Size 297
- Group Description 31 , 220
- Group ID 351
- Groups 105 , 309 , 310 , 313

- H**

- Hashing Algorithms 26
- Hello Intervall 285
- High Priority Class 203
- Home Number 84
- Host 321
- Host for multiple locations 362
- Host Name 324
- Hosts 351
- HotSpot Gateway 358
- HotSpot Gateway 357 , 395
- HTTP 24
- HTTPS 24 , 323
- HTTPS Server 323
- HTTPS TCP Port 323

- I**

- IGMP 225
- IGMP Proxy 227
- IGMP State Limit 226
- IGMP State Limit 227
- IGMP Status 227
- Ignore Certificate Request Payloads
281
- IKE (Phase-1) 393
- IKE (Phase-1) SAs 391

- Immediately 111
- Import / Export 154
- Include certificates and keys 370
- Incoming Distribution 112
- Incoming ISDN Number 296
- Incoming Phone Number 264
- Index Variables 336 , 340
- Info Message (UUS1) 170
- Inhibited number 136
- Int. No. 157 , 157
- Interconnect external calls 6
- Interface 24 , 24 , 126 , 127 , 157 ,
157 , 165 , 169 , 184 , 186 , 192 ,
192 , 195 , 206 , 219 , 226 , 250 ,
306 , 318 , 321 , 324 , 329 , 340 ,
353 , 356 , 359 , 367 , 395 , 395
- Interface Action 353
- Interface Mode 180 , 318
- Interface Status 336
- Interface Traffic Condition 336
- Interface Description 23
- Interface Assignment 219 , 367
- Interface - Connection Information -
Link 3
- Interface / Location 131
- Interface is UPnP controlled 356
- Interface Mode / Bridge Groups 21
- Interface Selection 220
- Interfaces 23 , 51 , 69 , 179 , 203 ,
309 , 353 , 355 , 381 , 393
- Interfaces / Provider 138
- Internal Assignment 82 , 108 , 167 ,
171
- Internal Number 86 , 88 , 105 , 106 ,
113 , 118 , 122 , 127 , 134 , 161 ,
163 , 165 , 169 , 173
- Internal Numbers 86 , 124 , 126 , 131
- Internal Number 173 , 177 , 377
- Internal Numbers 131
- Internal Log 390
- Internal Number and Rerouting
Settings 114
- Internal Time Server 14
- International Prefix / Country Code 7

- Internet + Dialup 230
 - Internet Key Exchange 253
 - Interval 336 , 340 , 351 , 354
 - Invalid DNS Packets 322
 - IP Compression 275
 - IP Accounting 381
 - IP Configuration 179
 - IP Address 320 , 332 , 380 , 387 , 395
 - IP Address Assignment 255
 - IP Address Mode 234 , 238 , 242 , 287 , 293
 - IP Address Range 249 , 279 , 293 , 298 , 328
 - IP Address / Netmask 180
 - IP Address / Netmask 394
 - IP Assignment Pool 242 , 255
 - IP Assignment Pool (IPCP) 287 , 293
 - IP Pool Name 249 , 279 , 298 , 328 , 329
 - IP Pool Configuration 327
 - IP Pools 248 , 278 , 298
 - IP/MAC Binding 120
 - IP/MAC Binding 331
 - IPSec 251 , 390
 - IPSec (Phase-2) 393
 - IPSec Tunnels 392
 - IPSec Statistics 392
 - IPSec Tunnels 391
 - IPSec (Phase-2) SAs 391
 - IPSec Debug Level 279
 - IPSec over TCP 280
 - IPSec Peers 252
 - IPv4 Route Configuration 186
 - IPv4 Routing Table 191
 - ISDN 126 , 241
 - ISDN Synchronisation 55
 - ISDN External 54
 - ISDN Internal 55
 - ISDN Login 24
 - ISDN Ports 53
- K**
- Key Size 340
 - Key Value 299
- L**
- L2TP 282
 - LAN 179
 - Language 173 , 177
 - Language for login window 359
 - Last configuration stored 2
 - Last Member Query Interval 226
 - Layer 4 Protocol 189
 - LCP Alive Check 235 , 239 , 288 , 294
 - LDAP URL Path 50
 - Lease Time 329
 - Level 380 , 390
 - Level No. 38
 - Licence Key 19
 - Licence Serial Number 19
 - License Allocation 173
 - Lifetime 178 , 266 , 273
 - Line 160
 - Line Access Digit 20
 - Lines 160
 - Load firmware 377
 - Local Certificate 266
 - Local Hostname 283
 - Local Address 394
 - Local Certificate 323
 - Local Services 314
 - Local Certificate Description 48 , 49 , 340
 - Local File Name 340
 - Local GRE IP Address 299
 - Local ID 253 , 391
 - Local ID Type 253 , 266
 - Local ID Value 266
 - Local IP Address 188 , 220 , 234 , 238 , 242 , 255 , 285 , 287 , 293 , 299
 - Local IP Address 391
 - Local Port 391 , 394
 - Local PPTP IP Address 239
 - Locality 46
 - Location 4 , 65 , 116 , 120 , 123

- Log Format 382
- Log on / Log off 112 , 163
- Logged Actions 307
- Logging Level 27
- Login Frameset 360
- Login Grace Time 27
- Ligon 395
- Loopback active 193
- Lost Calls Today 160

- M**

- MAC Address 116 , 120 , 180 , 332
- MAC Address 375 , 394
- Mail Exchanger (MX) 325
- Maintenance 368
- Management VID 185
- Matching String 383
- Max Recording Time 173
- Max waiting time in the queue 146
- Max. incoming control connections per remote IP Address 297
- Max. queue size 212
- Maximum Downstream Bandwidth 69
- Maximum Number of Dialup Retries 235 , 239 , 244
- Maximum Retries 285
- Maximum Upstream Bandwidth 69
- Maximum Groups 227
- Maximum Message Level of Syslog Entries 4
- Maximum Number of Accounting Log Entries 4
- Maximum Sources 227
- Maximum E-mails per Minute 384
- Maximum Number of Syslog Entries 4
- Maximum number of concurrent connections 25
- Maximum Response Time 226
- Maximum Time between Retries 285
- Maximum TTL for Negative Cache Entries 316
- Maximum TTL for Positive Cache Entries 316

- Maximum Upload Speed 206 , 209 , 250
- Members 309 , 313
- Memory Usage 3
- Memory Card 3
- Message 390
- Message Compression 383
- Message Timeout 383
- Messages 391
- Metric 188 , 192 , 255
- MIB Variables 340
- MIB/SNMP Variable to add/edit 340
- Min. queue size 212
- Mini Call Center 159
- Minimum Time between Retries 285
- Misdial Routing 115
- MobiKE 260
- Mobile Number 84 , 122
- Mode 44 , 189 , 192 , 220 , 226 , 227 , 247 , 264 , 266 , 277
- Mode / Bridge Group 23
- Mode for status "In the Office" 175
- Mode for status "Out of Office" 175
- Monitored Certificate 336
- Monitored Interface 336 , 353
- Monitored Subsystems 383
- Monitored Variable 336
- Monitored IP Address 351
- Monitoring 388
- MTU 299 , 391
- Multicast 223
- Multicast Routing 225
- Multicast Group Address 229
- Multiple SIP Connections (Sub-Exchange) 125
- Music on Hold 103

- N**

- Name 54 , 56 , 57 , 58 , 59 , 83 , 155 , 277 , 388 , 389
- NAT 193 , 394
- NAT method 195
- NAT Traversal 270
- NAT Detection 391

- NAT Configuration 194
 - NAT active 193
 - NAT Interfaces 193
 - National Prefix / City Code 7
 - Negative Cache 316
 - Negotiation Type 391
 - Net Direct (Keypad) 102
 - Netmask 192 , 220 , 287
 - Network Address 220
 - Network Configuration 220
 - Networking 186
 - New Calls 176
 - New Destination Port 199
 - New Destination IP
 - Address/Netmask 199
 - New File Name 370
 - New Source Port 199
 - New Source IP Address/Netmask
 - 199
 - Night 84
 - Night Mode Status 2
 - No Hold and Retrieve 117 , 121 , 125
 - No. 192 , 377 , 390 , 393
 - Notification 173
 - Number 176 , 388 , 389
 - Number of Messages 383
 - Number of playbacks 148 , 170
 - Number of repeats 170
 - Number of Admitted Connections
 - 258
 - Number of allowed simultaneous
 - Calls 65
 - Number of B Channels 246
 - Number of Used Ports 247
 - Numbering 76
 - Numbers 86 , 112 , 118 , 122 , 163
- O**
- Old Calls 176
 - On Busy 111
 - Optional 84
 - Optional Rerouting 88
 - Options 37 , 192 , 227 , 279 , 290 ,
297 , 307 , 334 , 350 , 362 , 369 ,
382
 - Organization 46
 - Organizational Unit 46
 - OSPF Mode 247 , 289 , 295
 - Other Inactivity 308
 - Other phones 123
 - Outbound Interface 209
 - Outgoing 156
 - Outgoing Signalisation 62 , 77 , 86
 - Outgoing Signalisation 86
 - Outgoing Services 132
 - Outgoing ISDN Number 296
 - Outgoing Phone Number 264
 - Overbooking allowed 209
 - Overview 131
 - Overwrite similar certificate 340
- P**
- P-P Additional MSN 79
 - P-P Base Number 79
 - P-P DDI Exception 79
 - Packets 391
 - Parallel Ringing 105
 - Parallel Ringing 388
 - Parallel Ringing 104
 - Parent Location 69
 - Passed 393
 - Password 40 , 44 , 48 , 49 , 61 , 89 ,
233 , 237 , 241 , 277 , 283 , 286 ,
291 , 324 , 333 , 340 , 365 , 370 ,
385
 - Password for protected Certificate
 - 340
 - Password for IP Phone Registration
 - 89
 - Passwords 10
 - PBX coupling 65
 - Peer Address 253
 - Peer ID 253
 - Permanent Layer 2 Activation 55
 - Permit Call Forwarding 106
 - Personal Access 89
 - Phase-1 Profile 258
 - Phase-1 Profiles 266

- Phase-2 Profile 258
 - Phase-2 Profiles 273
 - Phone Number 153
 - Phone Number 155
 - Phone Version 375
 - Phone Type 116 , 120 , 131 , 375 , 377
 - Phone Update 374
 - Physical Address 395
 - Physical Interfaces 51
 - Pick-up Group 96
 - Pick-up (Extension) 20
 - Pick-up Group 20
 - PIN (6 Digit Numeric) 114
 - PIN for Phone Access 89
 - PIN1 11
 - PIN2 11
 - Ping 24
 - Ping Generator 354
 - Ping Test 368
 - Policies 303
 - Policy 32 , 36
 - Pool Usage 329
 - Pop-Up window for status indication 360
 - POP3 Server 385
 - POP3 Timeout 385
 - Port 76 , 193 , 326
 - Port Number 124
 - Port Configuration 52 , 184
 - Port STUN server 64
 - Ports 76
 - Positive Cache 316
 - PPPoE 232
 - PPPoE Mode 233
 - PPPoE Ethernet Interface 233
 - PPPoE Interfaces for Multilink 233
 - PPTP 237 , 291
 - PPTP Inactivity 308
 - PPTP Passthrough 193
 - PPTP Tunnels 291
 - PPTP Address Mode 239
 - PPTP Ethernet Interface 237
 - PPTP Mode 291
 - Preshared Key 253
 - Primary DHCP Server 332
 - Primary DNS Server 318
 - Prioritisation Algorithm 206
 - Prioritize TCP ACK Packets 235 , 239 , 288 , 294
 - Priority 31 , 35 , 209 , 304 , 318
 - Priority Number 136
 - Priority Numbers 136
 - Priority Queueing 209
 - Privacy Number Truncation 158
 - Project Code 157 , 157
 - Propagate PMTU 275
 - Proposals 266 , 273
 - Protocol 196 , 201 , 214 , 258 , 311 , 326 , 340 , 362 , 380
 - Protocol Header Size below Layer 3 206
 - Provider 324
 - Provider Name 326
 - Provider Status 61
 - Provider without Registration 65
 - Provisioning Server (code 3) 331
 - Proxy 64
 - Proxy Interface 227
 - Proxy Port 64
 - Proxy ARP 181 , 260
 - Proxy ARP Mode 247 , 289 , 295
 - Public Source IP Address 260
 - PVID 184
- ## Q
- QoS 200 , 306 , 395
 - QoS Classification 203
 - QoS Interfaces/Policies 206
 - QoS Filter 200
 - QoS Queue 395
 - Query Interval 226
 - Queued 395
 - Queues/Policies 206
- ## R
- RA Encrypt Certificate 44

- RA Sign Certificate 44
 - RADIUS 29
 - RADIUS Dialout 32
 - RADIUS Secret 31
 - RADIUS Server Group ID 277
 - Real Time Jitter Control 206
 - Real Time Jitter Control 249
 - Reboot 378
 - Reboot after execution 340
 - Reboot device after 340
 - Receive Announcement Calls 102
 - Receive charges 58
 - Receive Announcement Calls 388
 - Receive Intercom Calls 388
 - Receive MWI Information 102
 - Receive System Intercom Call 102
 - Received DNS Packets 322
 - Recipient 383
 - Registrar 63
 - Registrar Port 63
 - Registration Timer 64
 - Relay Contact 170
 - Remaining Validity 336
 - Remote Hostname 283
 - Remote Address 394
 - Remote Networks 391
 - Remote Port 391 , 394
 - Remote Authentication 29
 - Remote Access (e.g. Follow me, Room Monitoring) 11
 - Remote File Name 340
 - Remote GRE IP Address 299
 - Remote ID 391
 - Remote IP 391
 - Remote IP Address 284
 - Remote IP Address 391
 - Remote PPTP IP Address 239 , 291
 - Remote PPTP IP AddressHost Name 291
 - Remote User (for Dialin only) 241
 - Repeat after 170
 - Reporting Method 219
 - Rerouting 145
 - Rerouting Application 88 , 113
 - Rerouting Function 162
 - Rerouting Applications 149
 - Rerouting Functions 145
 - Rerouting of Incoming Distribution 9
 - Rerouting on no response 111 , 162
 - Rerouting on no response 389
 - Rerouting to Number 115
 - Rerouting to Number 6
 - Response 320
 - Restore Default Settings 24
 - Retries 32
 - Return Address 178
 - Robustness 226
 - Role 277
 - Room Monitoring 388
 - Route 138
 - Route Class 186
 - Route Entries 234 , 238 , 242 , 255 , 287 , 293 , 299
 - Route and Charge Assignment 108
 - Route Type 186 , 192
 - Routes 186
 - Routing 139
 - Routing Mode 138
 - Routing Stage 137
 - Routing Stage 1 140
 - Routing Stage 2 140
 - RSA Key Status 26
 - RTP Port 74
 - RTT Mode (Realtime Traffic Mode) 209
 - Rule Chain 218 , 219 , 367
 - Rule Chains 217
 - Rx Bytes 393 , 394
 - Rx Errors 393
 - Rx Packets 393 , 394
- S**
- Save configuration 38
 - Save call data records 103
 - Save incoming calls 158
 - Save outgoing calls 158
 - SCEP URL 44
 - Schedule Interval 350

- Scheduling 335
- SD Card Vers. 375
- Second Timeserver 14
- Second External Number 171
- Secondary DHCP Server 332
- Secondary DNS Server 318
- Security Algorithm 391
- Select file 151
- Select Interface 82
- Select lines 164
- Select vendor 331
- Select file 154
- Select file 370
- Selected Ports 297
- Selection 310
- Send 395
- Send Certificate Chains 281
- Send Certificate Request Payloads 281
- Send CRLs 281
- Send Initial Contact Message 280
- Send Key Hash Payloads 281
- Sender E-mail Address 385
- Separator 154
- Sequence of Trunk Lines in Group 81
- Serial Number 2
- Server 326
- Server Address 340
- Server Timeout 32
- Server URL 340
- Server Failures 322
- Server IP Address 31 , 35
- Service 196 , 201 , 214 , 304 , 362
- Set Time 13
- Set COS value (802.1p/Layer 2) 203
- Set Date 13
- Set DSCP/TOS value (Layer 3) 203
- Set interface status 340
- Settings 61 , 118 , 122 , 377
- Severity 383
- Show Connected Number (COLP) 93
- Show Date and Time 128
- Show incoming Name (CNIP) 128
- Show incoming Number (CLIP) 128
- Show incoming waiting Number (CLIP off Hook) 128
- Show new Messages (MWI) 129
- Show Outgoing Number (CLIP) 93
- Show passwords and keys in clear text 12
- Signal remote caller number 62 , 77
- Signal fixed out number 62 , 77
- Signalling 110 , 167 , 389
- Silent Deny 219
- Silent Deny 193
- Simultaneous on no response 107 , 167
- Single Number (MSN) 79
- SIP Provider 61
- SIP Client Mode 124
- SIP Client IP Address 124
- SIP Header Field for User Name 65
- SIP Header Field(s) for Caller Address 65
- Size of Queue 146
- SMTP Authentication 385
- SMTP Password 178
- SMTP Server 178 , 385
- SMTP Server Port 178
- SMTP User Name 178
- SNMP 24 , 28 , 386
- SNMP Version 28
- SNMP Listen UDP Port 28
- SNMP Read Community 12
- SNMP Trap Broadcasting 386
- SNMP Trap Community 386
- SNMP Trap Hosts 387
- SNMP Trap Options 386
- SNMP Trap UDP Port 386
- SNMP Write Community 12
- Software & Configuration 369
- Source 304
- Source Interface 189 , 229
- Source Location 340
- Source Port 189 , 196 , 258
- Source Port/Range 196 , 201 , 214 , 362

- Source Location 370
 - Source File Name 370
 - Source IP Address 336 , 340 , 351 , 354
 - Source IP Address/Netmask 189 , 196 , 201 , 214 , 258 , 362
 - Source Port Range 311
 - Specific Ports 297
 - Specify bandwidth 306
 - Speed Dial 20
 - Speed Dial Number 153
 - SSH 24 , 25
 - SSH Port 25
 - SSH service active 25
 - Standard 84
 - Start Mode 258
 - Start Time 339
 - State/Province 46
 - Static Hosts 319
 - Statistics 322 , 393
 - Status 2 , 56 , 57 , 59 , 112 , 163 , 169 , 171 , 176 , 336 , 377 , 388 , 391 , 392 , 393 , 394
 - Status Information 388
 - Status of Mail Box Owner 175
 - Status/Update Status 375
 - Stop Time 339
 - STUN server 64
 - Subject 383
 - Subject Name 340
 - Substitution of Incoming Number Prefix 65
 - Substitution of International Prefix with "+" 65
 - Subsystem 390
 - Successful Trials 351
 - Successfully Answered Queries 322
 - Summary 46
 - Surveillance 350
 - Switch signalling 166 , 169
 - Switch Port 52
 - Switch call signalling 106 , 149 , 161
 - Switch call signalling 389
 - Switch signalling variants manually 96
 - Switch to SNMP Browser 38
 - Switching Points 142 , 143
 - Sync SAs with ISP interface state 280
 - Syslog 379
 - Syslog Servers 379
 - System 4
 - System Logic 370
 - System Name 4
 - System Licences 19
 - System Messages 390
 - System Reboot 378
 - System Management 2
 - System Date 2
 - System Parked Enquiry 17
 - System Parking (Open Enquiry) 20
 - System Phonebook 152
 - System Phonebook Authorization 103
- ## T
- T.38 FAX support 65
 - TACACS+ 34
 - TACACS+ Secret 35
 - Take Waiting Calls witht 146
 - TAPI 103
 - Target Number 146
 - Target MAC-Address 365
 - Target Number "Immediate" 134
 - Target Number "On busy" 134
 - Target Number "On no reply" 134
 - TCP Inactivity 308
 - TCP Keepalives 27
 - TCP Port 36
 - TCP-MSS Clamping 181
 - Team Signalling 9
 - Team Speed Timer 107 , 161 , 167
 - Teams 105 , 389
 - Telnet 24
 - Terminal 388
 - Terminal Type 126 , 127
 - Terminal Endpoint Identifier (TEI) 82
 - Terminals 116

Terms & Conditions 359
 Third Timeserver 14
 Ticket Type 360
 Time 12, 157, 157, 390
 Time Condition 339
 Time for Rerouting on No Reply 146
 Time Update Interval 14
 Time Update Policy 14
 Time Zone 13
 Timeout 36
 Timer 16
 Timestamp 380
 Total 393
 Traceroute Test 368
 Traffic Direction 336
 Traffic shaping 206, 209, 306
 Transfer Mode 264
 Transfer with 146
 Transfer Signalling 6
 Transfer call data records via Serial 2
 158
 Transfer own IP address over ISDN/
 GSM 264
 Transfer to busy extension 6, 17
 Transferred Traffic 336
 Transmit charge information 103
 Transmit Charges Pulses 129
 Transport Protocol 63, 64, 124
 Trials 336, 354
 Trigger 335, 353
 Trigger Status 340
 Trunk 79, 113, 115
 Trunk Numbers 78
 Trunk Settings 76
 Trunk Group Selection 20
 Trunk Groups 81
 Trunk Line Selection with Line Access
 Number 91
 Trunks 76
 TTL 320
 Tunnel Profile 286
 Tunnel Profiles 283
 Tx Bytes 393, 394
 Tx Errors 393

Tx Packets 393, 394
 Type 69, 201, 214, 311, 362, 393
 Type of Messages 380
 Type of Number 78, 79
 Type of Rerouting Application 149
 Type of traffic 195
 Type of Call Forwarding 134
 Type of Rerouting Function 145

U

UDP Inactivity 308
 UDP Destination Port 284
 UDP Destination Port 291
 UDP Port 32
 UDP Source Port 284
 UDP Source Port Selection 291
 Unchanged for 393
 Unsuccessful Trials 351
 Update Interval 326
 Update Path 326
 Update enabled 375
 Update immediately 375
 UPnP 355
 UPnP Status 356
 UPnP TCP Port 356
 Upstream Bandwidth Limitation 69
 Upstreaming Device with NAT 65
 Uptime 2
 URL 370
 URL SCEP Server URL 340
 Usage 56, 59
 Usage Type 244
 Use CRL 340
 Use global rerouting 96
 Use PFS Group 273
 Use settings from 142, 143
 Use Zero Cookies 280
 User 40, 118, 122, 157, 157, 163,
 173, 176, 333
 User Settings 83
 User must change password 40
 User Name 61, 89, 233, 237, 241,
 286, 291, 324, 333, 385, 395
 Users 40, 83, 277, 286, 388

Users assigned/Users logged on 389

V

Variant 107, 149, 171

Variant 1 - 4 161

Vendor Mode 31

Version 377

Version Check 340

View 160

VLAN 183, 233

VLAN Identifier 183

VLAN Members 183

VLAN ID 180, 233

VLAN Name 183

VLANs 183

Voice Applications 150

Voice Mail Language 173

Voice Mail System 177

Voice Mail Boxes 172

Voice Mail System 172

VoIP 61, 123

Volume 151

VPN 251

W

Waiting Calls 160

Wake-On-LAN 362

Wake-On-LAN Filter 362

Wake-On-LAN Filter 365

Wake-On-LAN Rule Chain 365

Walled Garden 359

Walled Garden URL 359

Walled Network / Netmask 359

WAN 230

Wave Files 151

Wave-File 170

Web Access Password 156, 158, 164

Web Access Username 156, 158, 164

Weight 209

Wildcard 325

WINS Server 316

WOL Rules 365

Wrap-up Time 164

Wrap-up Timer 107

Write certificate in configuration 340

X

X.31 82

XAUTH Profile 258

XAUTH Profiles 277

Z

Zero Cookie Size 280

Zones 139, 139