Explosion proof and weatherproof VoIP-telephones

ResistTel IP2/IP154
ResistTel IP2/IP152

Operating instructions

FUNKE+HUSTER·FERNSIG

FHF BA 9710-6 03/13 V9

BA 9710-6 03/13 V9
Manual
ResistTel IP2 / IP152
ExResistTel IP2 / IP154

☞	**Note** Please read the operating manual carefully before installing the telephone. Please check the contents of the box for completeness.	☞

FHF Funke + Huster Fernsig GmbH
Gewerbeallee 15 – 19
45478 Mülheim an der Ruhr
Tel +49 (208) 8268 - 0
Fax +49 (208) 8268 - 377
http://www.fhf.de

Table of Contents

1 About this Manual

This manual describes the operation and administration of the weatherproof VoIP telephone **ResistTel IP2 / IP152** and the explosion proof VoIP telephone **ExResistTel IP2 / IP154**. In order to create a VoIP gateway or a VoIP PBX, please contact the gateway or PBX manufacturer for more information. All advice and instructions for the operation of the VoIP telephone must be followed carefully and the telephone should only be used as specified.

This manual is updated regularly.

1.1 Tips for Reading

Symbols can be found together with a box at various chapters of this manual. They are intended to refer you to chapters of particular significance, as shown below.

Note

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

Tip

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

Caution

Make sure that you pay attention to these fields, to prevent damage to the equipment and to ensure your own safety.

1.2 Overview of the Chapters

This manual offers extensive information about the VoIP telephones ResistTel IP2 / IP152 and ExResistTel IP2 / IP154. Apart from the general basics, it also offers detailed operating instructions as well as administrator instructions.

General information on the phone is provided in chapter 2. It contains the setup of the phone and descriptions of the available keys and the structure of the display.

Chapter 3 is particularly interesting for the user of the phone. Here it is shown in detail, which possibilities are available.

Chapter 4 is intended for the administrator of the system. This chapter is not exhaustive. Instead, in this chapter, the basic administrative settings are explained that are of interest to the user, but cannot be performed directly on the phone.

The Web interface allows for comfortable administrative setup of the VoIP telephones. Refer to chapter 4.1 General beginning on page 173.

Note

This configuration can be accessed after password entry only. Refer to chapter 4.1.2 **User Name** and **Password** beginning on page 174.

Follow the safety instructions in the manual at all times!

Note

Parameters that are transmitted to the telephone per DHCP cannot be overwritten by a local configuration.

2 VoIP Telephones ResistTel IP2 / IP152 and ExResistTel IP2 / IP154

2.1 Keypad

2.1.1 Assignment

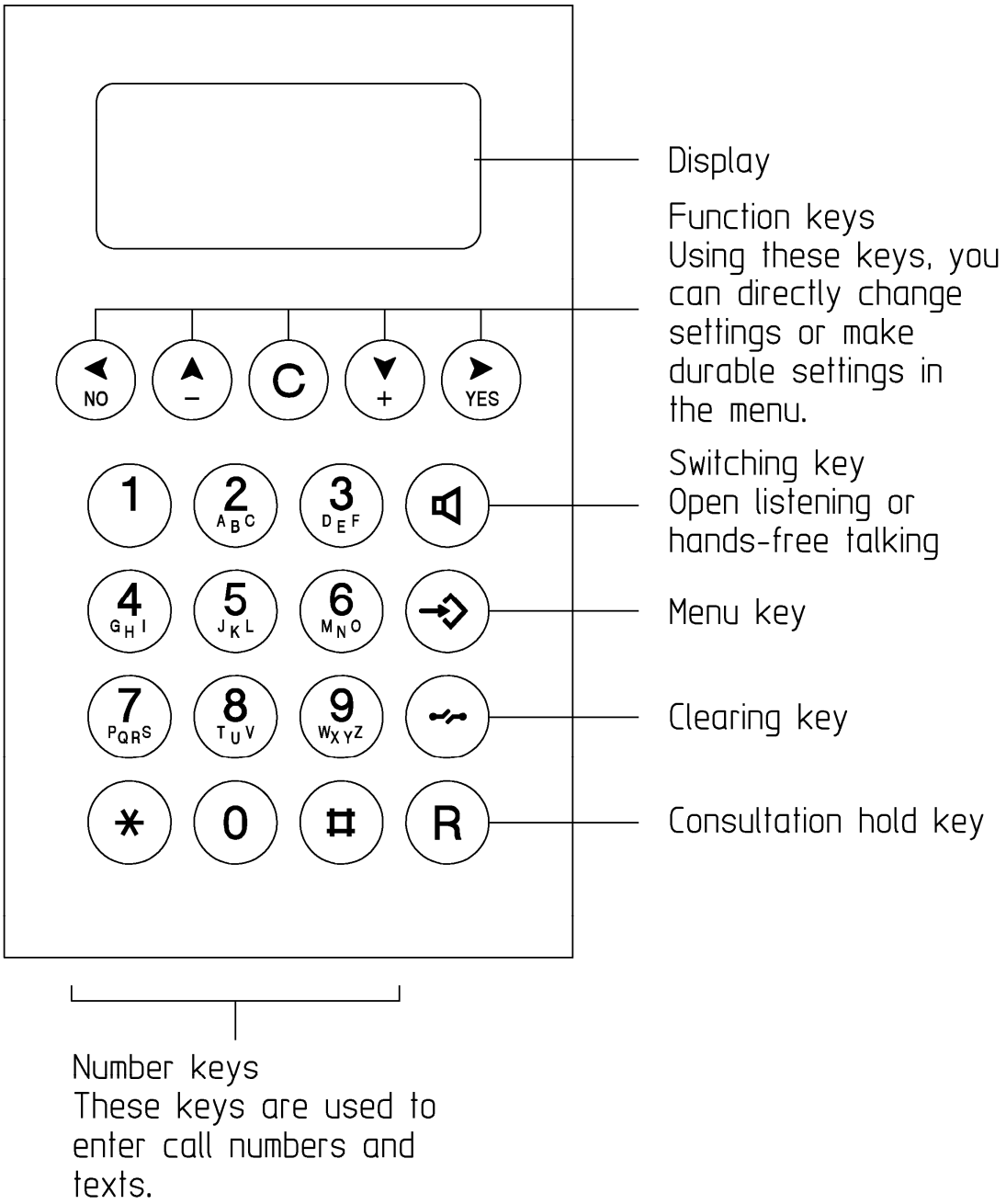


Figure 1: Keypad of the VoIP-Telephones

2.1.2 Description

Symbol	Description and Key Functions
	The Loudspeaker key is used to control the hands free and listening mode.
	The Menu key is used to open the main menu or to save changes.
	The Disconnect key is used to terminate calls or any menu.
(short)	The Enquiry key is used to enable the "Hold" and "Switch" functions. In idle mode, the Enquiry key is used to call up the list of missed calls. To execute the enquiry function the Enquiry key has to be pressed short (shorter than 0.5 seconds).
(long)	The Redial key is used to select the list of 100 phone numbers last dialled. In the menu, the redial key confirms the current selection. The phone has no single Redial key. To execute the redial function the Redial key has to be pressed long (longer than a second).
	Arrow keys are used for navigation in the menu and browsing in the telephone directory. The volume can only be adjusted during a call.
(long)	The asterisk key also serves as a mute key. During a call, a longer press switches the microphone off or on.
...	Digit keys for entering phone numbers. The asterisk and hash keys have special functions. To enter asterisk and Hash the keys have to be pressed short (shorter than 0.5 seconds). To enter Mute (asterisk) and Shift (hash) the keys have to be pressed long (longer than a second). After pressing of shift the digit keys (1 – 9 and 0) become function keys. After executing a function key the shift mode is ended.
	The Clearing key is used in input mode to delete the characters left to the cursor.

Symbol	Description and Key Functions
(long)	The headset key is used to make and to end a call in the headset mode. The telephone has no single headset key. To execute the headset key function the key has to be pressed long (longer than a second) and then the loudspeaker key has to be pressed. The headset key can be used only, if the headset is configured to on (see chapter 3.9.1 on page 125). This makes sense only, if a headset is connected to the phone.

Table 1: Keys and Function Elements

2.2 Display

The displays of the VoIP Telephones ResistTel IP2 / IP152 and ExResistTel IP2 / IP154 have 7 lines with max. 30 characters each line for showing information.

2.2.1 Default Display

The name and telephone number of the current registration is displayed in the first line.

The middle lines display special information relating to the condition.

The date, time and registration status is displayed in the last line.

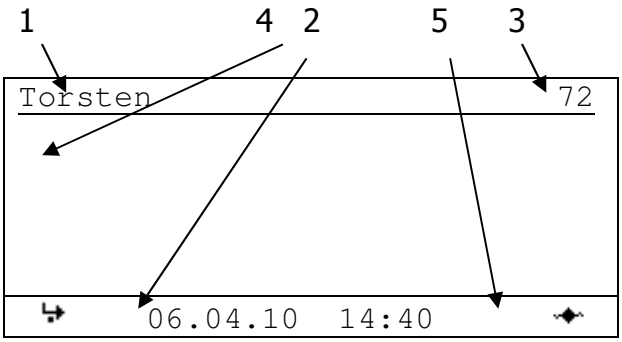


Figure 2: Default Display (Idle State)

In the busy state state-information, date, time and the duration of the active connection are displayed in the last line.

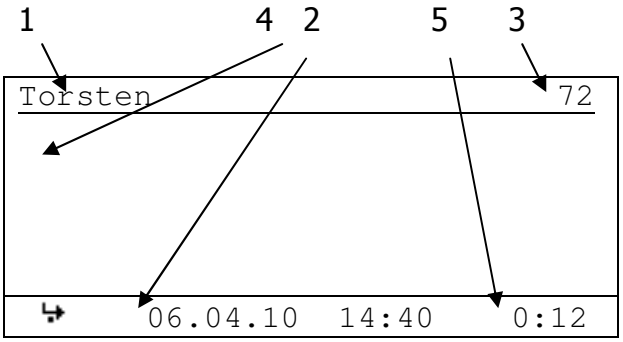


Figure 3: Default Display (Busy State)

Position	Symbol	Description
1		Name (H.323 or SIP ID or nickname of the PBX configuration)
2		Status line; provides information on the current status of the telephone by means of the following symbols.
	06.04.10	Date
	14:00	Time
		No connection to the Ethernet (primary Ethernet port)
		Connection established to the gatekeeper
		Connection established to the secondary gatekeeper
		Connection to the gatekeeper broken. (Both symbols are displayed in mutual change.)
		Open listening
		Hands free Mode
		Microphone switched off (symbol flashing)
		Call diversion activated
		Handset activate
		Headset active
		Telephone locked
		Calling number transmission locked
3		Own call number (E.164)
4		Called party
		Calling party
		Unknown number/name, unresolved number
		Diverting party
		Transferring party
		Returning call
		Call pending
		Call on hold
5		Shift Mode
		Headset configured
		Audio connection of the active call is encrypted (SRTP)
	0:12	Duration of the active call

Table 2: Contents of the Default Display

2.2.2 Menu and Listing Display

The first six lines are used for the menu and listing display.

The last line is used for display of menu level, display name, scroll information and type of entry.

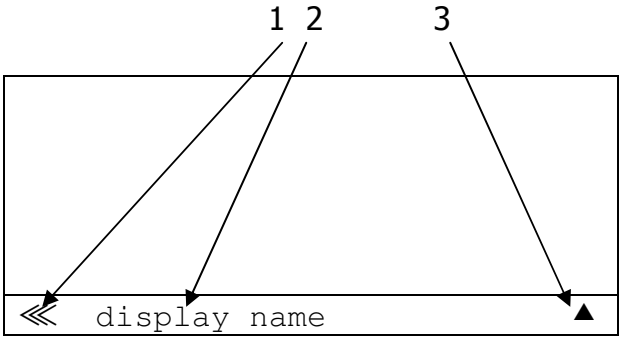


Figure 4: Menu and Listing Display of the VoIP Telephone

Position	Symbol	Description
1		Menu or listing level 0
	<	Menu or listing level 1
	≪	Menu or listing level 2
	⋘	Menu or listing level 3
	⋘	Menu or listing level 4 or lower
2		Display name
3	▲	Scrolling up possible
	⇕	Scrolling up and down possible
	▼	Scrolling down possible
	a	Alphanumerical input
	1	Numerical input
		Choice, next level

Table 3: Contents of the Menu and Listing Display

2.3 Types

The telephone is available in different types. There are two groups of types.

- Weatherproof types
- Explosive protected types

2.3.1 Weatherproof Types

The phone is available for delivery in different versions.

- Handset with armed court.
- Single LAN connection or switch LAN module with two LAN connections with internal connection and cable screw connection or external LAN connection and plug in connection.
- Housing in black or coloured in red or blue.
- Some Sealing plugs to connect option equipment
- Optional: max. 5 cable screw caps
- Optional: relay module

Accessories (optional):

- Headset with connection cable and attachment of the bracket.
- LAN connector from Phoenix Contact, consisting of:
    - RJ sleeve housing Type VS-08-T-RJ45/IP67, Art.-Nr.: 1688696
    - Male insert RJ45, CAT5, 8-polig Type VS-08-ST-RJ45/IP67, order-no.: 1688573
- LAN female connector for cable mounting from Tycoelectronics (AMP), order-no. 116604-2
- Cable screw cap
- Sealing plugs
- 2 keys for TORX socket screws TX20, TX30

2.3.1.1 Default Version one LAN Connection with a Cable Screw Cap

- 1 LAN connection internal
- Housing with 1 cable screw cap and 2 bored holes with sealing plugs at the upper side.

Box contents

The scope of the delivery includes:

- Telephone
- Printed short manual
- Manual on CD
- 1 LAN female connector for cable mounting from Tycoelectronics (AMP), order-no. 116604-2
- 2 keys for TORX socket screws TX20, TX30

2.3.1.2 Version one LAN Connection with a Female Housing Connection

- 1 LAN connection female housing connection
- 1 LAN connection (without LAN interface) and sealing plug at the housing
- Housing with 1 bored hole with sealing plug at the upper side

Box contents

The scope of the delivery includes:

- Telephone
- Printed short manual
- Manual on CD

- 1 LAN connector from Phoenix Contact, consisting of:
    - RJ sleeve housing Type VS-08-T-RJ45/IP67, Art.-Nr.: 1688696
    - Male insert RJ45, CAT5, 8-polig Type VS-08-ST-RJ45/IP67, order-no.: 1688573
- 2 keys for TORX socket screws TX20, TX30

2.3.1.3 Version one Switch LAN Module with two LAN Connections with Cable Screw Cap

- 2 LAN connections internal
- Housing with 1 cable screw cap and 2 bored holes with sealing plugs at the upper side.

Box contents

The scope of the delivery includes:

- Telephone
- Printed short manual
- Manual on CD
- 1 LAN female connector for cable mounting from Tycoelectronics (AMP), order-no. 116604-2
- 2 keys for TORX socket screws TX20, TX30

2.3.1.4 Version one Switch LAN Module with two LAN Connections with Cable Screw Cap

- 1 LAN connection female housing connection
- 1 LAN connection and sealing plug at the housing
- Housing with 1 bored hole with sealing plug at the upper side

Box contents

The scope of the delivery includes:

- Telephone
- Printed short manual
- Manual on CD
- 1 LAN connector from Phoenix Contact, consisting of:
    - RJ sleeve housing Type VS-08-T-RJ45/IP67, Art.-Nr.: 1688696
    - Male insert RJ45, CAT5, 8-polig Type VS-08-ST-RJ45/IP67, order-no.: 1688573
- 2 keys for TORX socket screws TX20, TX30

2.3.1.5 Example Pictures

Figure 5: VoIP Telephone ResistTel IP2 / IP152 with armed Court and 5 Cable Screw Caps

Figure 6: VoIP Telephone ResistTel IP2 / IP152 with armed Court, 2 LAN female Housing Connections and 3 Cable Screw Caps

2.3.2 Explosion Proof Types

2.3.2.1 Description

The telephone type ExResistTel IP2 / IP154 will be used as stationary telephone in areas, which may be put to risk by explosive gas or dust atmosphere and make is necessary to use devices of the device group II of the device class 2G and 2D. According to regulations the general purpose of the telephone is hanging vertically on a wall or hanging vertically on a mounting plate.

The telephone type ExResistTel IP2 / IP154 is realized according to the following type of protection:

- Type of ignition protection: Ex e [ib] mb IIC T4 Gb
- Type of ignition protection: Ex tb [ib] IIIC T135°C Db
- Degree of protection of enclosure: IP66
- Working environment temperature range: -40 °C ≤ Tu ≤ +60 °C

The telephone type ExResistTel IP2 / IP154 is designed for connecting to the Ethernet according to IEEE802.3.

The telephone has to be included into the potential equalisation either with the internal earth connecting bolt of the metal plate or with the external earth connecting bolt at the housing (see examples of connection). The potential equalisation must exist inside and outside of the explosion at risk area.

The telephone supports the connection of an intrinsically safe headset.

The headset is not part of this telephone. To connect the intrinsically safe headset the plug mounted on the left side of the housing has to be replaced be a acceptable explosion protected cable gland.

☞	**Note** The installation prescribed in the regulations according to IEC/EN 60079-14 and the national installation regulations have to be respected.	☞

2.3.2.2 Construction

2.3.2.2.1 Housing

The telephone type ExResistTel IP2 / IP154 has a non coloured housing made of an electrostatic conductive pressed basic material and a stainless steel keypad. Optionally the housing can be coloured with an electrostatic conductive colour.

In the front plate of the keypad is a display cut-out closed with a viewing glass.

The housing consists of a box-shaped bottom part with a tray for inserting the electronic and a curved top cover with a keypad.

The top cover will be pressed with four screws to the upper part with in between a revolving seal and generates the intrinsically safe as well as the non-intrinsically safe terminal compartment. In the tray is a grouting cup with the embedded electronic.

2.3.2.2.2 Configuration Plug Connector

A 6 pin plug connector sticks out of the grouting tray inside the telephone (14) (see Figure 12 on page 46).

The configuration plug connector will be used by the manufacturer of the telephone type ExResistTel IP2 / IP154 for configuration only and must not be connected.

The programming by the installer is not allowed.

2.3.2.2.3 Intrinsically Safe Keypad Connection

An intrinsically safe 14-terminal ribbon cable (7) with a female plug will be carried out of the grouting tray inside the telephone (see Figure 12 on page 46).

The female plug has to be plugged to the 14 pin plug connector (8) in the upper part of the housing securely, before the telephone will be screwed down.

2.3.2.3 Electrical Characteristic Parameter

2.3.2.3.1 Power Supply DC (not intrinsically safe)

Terminal no.: 16, 17

U_n = DC 19.2 … 52.8 V

U_m = DC 53 V

I_{sc} = 100 A

For this connection cables with a transversal section of 1.5 mm² to 4 mm² are allowed to be used only.

2.3.2.3.2 Power Supply PoE according to IEEE 802.3 af (not intrinsically safe)

Terminal no.: 11, 12, 14, 15

U_n = DC 24 … 48 V

U_m = DC 57 V

I_{sc} = 100 A

For the LAN connection it is only allowed to use cables of the type CAT5e or higher. To observe the EMC rules with netting shielded cables have to be used.

☞	**Note** Using a power supply via PoE it is only allowed to use the unused data cable pairs of a 10/100 Mbit/s Ethernet cable for the power.	☞

2.3.2.3.3 LAN Interface 10/100 BASE-TX according to IEEE 802.3 (not intrinsically safe)

Terminal no.: 8, 9, 10, 13

U_n = ±2.5 V (10 BASE-TX)

respectively

U_n = ±1 V (100 BASE-TX)

U_m = ±7 V

U_m = DC 57 V

For the LAN connection it is only allowed to use cables of the type CAT5e or higher. To observe the EMC rules with netting shielded cables have to be used.

2.3.2.3.4 Potential-free Relay Contacts (not intrinsically safe)

Terminal no.: 18, 20 respectively no.: 21, 23

- U_{max} = AC 250 V

  I_{max} = 5 A

  P_{max} = 100 VA

  For this connection cables with a transversal section of 1.5 mm² to 4 mm² are allowed to be used only.

- U_{max} = DC 230 V

  I_{max} = 0.5 A

  P_{max} = 100 W

  For this connection cables with a transversal section of 0.75 mm² to 4 mm² are allowed to be used only.

- U_{max} = DC 50 V

  I_{max} = 1 A

  For this connection cables with a transversal section of 0.75 mm² to 4 mm² are allowed to be used only.

- U_{max} = DC 30 V

  I_{max} = 5 A

  P_{max} = 100 W

  For this connection cables with a transversal section of 1.5 mm² to 4 mm² are allowed to be used only.

The terminals no. 19 and 22 according to the connection plan are not used and must not be connected.

2.3.2.3.5 Cable Shield

The cable shield of the LAN cable respectively the earth lead of the DC power cable have to be connected to the terminals no. 6 respectively no. 7. The cable shield of the LAN cable must be isolated according to the respective installation regulations. The standard IEC/EN 60079-14 must be respected.

The conductive shield of the network cable has to be handled in the following way:

- The cable coating of the network cable has to be striped.
- The single conductor and the cable screen have to be separated.
- The cable screen has to be drilled to a common conductor. When indicated existing screen foils and auxiliary wires have to be removed.
- Suitable isolating tube has to be pushed over the drilled cable screen. The total length should not be longer than necessary for a secure arrangement of the wiring.
- The bare end of the drilled cable shield may be connected directly (The terminals are approved for connecting flexible wires) or otherwise connected with a mounted end sleeve for strands.
- Advantageously these cable works should be done before inserting the cable into the housing.

The preinstalled cable connection between terminal no. 5 and internal earth connecting bolt of the metal plate is security relevant and must not be interrupted.

Caution

The air and the creepage distance at the terminals must not be reduced by the kind of connection of the wires at these connection terminals.

2.3.2.3.6 Configuration Plug Connector

The 6 pin configuration plug connector must not be connected.

2.3.2.3.7 Intrinsically Safe Headset

Terminal no.: 1, 2, 3, 4

U_o = 16.4 V

I_o = 220 mA

P_o = 450 mW

C_o = 424 nF

L_o/R_o = 78 µH/Ω

The headset type MT53H79B-56 according NEMKO 02ATEX059X respects the necessary connection requirements and can be used. The connection with other headsets must be checked according the respective installation rules. The standard IEC/EN 60079-25 must be respected.

2.3.2.3.8 Internal and External Earth and Potential Equalisation Connecting Bolt PA

For this connection cables with a transversal section of 4 mm² to 6 mm² can be used.

2.3.2.3.9 Voltaic Isolation

The supply DC, the supply PoE, the LAN interface and the intrinsically safe headset are safety voltaic separated up a voltage of 250 V_{eff}.

2.3.2.3.10 Voltaic Isolation of the Relay Contacts

The two potential free relay contacts are safety voltaic separated against each other up to a voltage of 440 V_{eff}.

2.3.2.4 Warning and Safety Instructions

This telephone is an explosion proof and weatherproof telephone especially for use in a harsh industrial environment.

The following warning and security instructions must be respected:

- The telephone is build up in protection class I and must be connected and used with the required voltages only. The connection cable has to be mounted without risk of stumbling.
- Is must be paid attention that the telephone, the connection cable, etc. must not be damaged. In a damaged state the use of the telephone is not allowed.
- For using the telephone the laws and the industrial regulations, the accident prevention, respectively the electrical regulations must be respected.
- For repairing only original exchange parts are allowed, which have to be changed professional. Other exchange parts may cause damages and the warranty will be lost.
- The required general purpose has to be respected. The telephone must be mounted on a closed rear panel in vertical mode.
- A magnetic field with disturbing frequencies can adjust a disturbance of the acoustic quality. Pay attention to an acceptable installing place.
- For opening the telephone must be free of power.
- In opened state of the telephone dust must not attain into the telephone.
- For the impermeability of the housing necessary gasket respectively the protective cover at the upper part must not be damaged during mounting or dismounting.
- After repairing of the telephone for use in dust environment, the repaired parts have to be tested again.

- The speech speed hopper of the handset consists out of a not electrical conductive plastic material. It may be charging with high air speed dangerously. A cleaning of the speech speed hopper with pressed air is not allowed.

- Changes of the product for technical improvement are possible without announcement before.

- The configuration conductor will be used for configuration by the manufacturer exclusively and must not be connected. Programming by the installer is not allowed.

- The telephone has to be included into the potential equalisation either with the internal earth connecting bolt of the metal plate or with the external earth connecting bolt at the housing (see examples of connection). The potential equalisation must exist inside and outside of the explosion at risk area. The potential equalisation is necessary to support the explosion protection.

Caution

The equipment is suitable for use in Group II, Category 2G and 2D or non-hazardous locations only.

WARNING – EXPLOSION HAZARD

Do not disconnect equipment unless power has been removed or the area is known to be non-hazardous.

WARNING – EXPLOSION HAZARD

Substitution of any components may impair suitability for Group II, Category 2G and 2D.

- The telephone may be operated solely under the stated ambient conditions. Unfavourable ambient conditions can lead to damage of the telephone and thus present a potential danger for the user.

Such unfavourable ambient conditions are:

- Humidity of air too high (>75% rel., condensing)
- Moisture and dust (pay attention to the degree of protection)
- Flammable gases, vapours and solvents not covered by the type of protection for the telephone.
- Too high ambient temperatures (> +60°C).
- Too low ambient temperatures (< -40°C).

- During operation of the telephone the temperature must not exceed nor fall below the prescribed range of ambient temperatures. It is not allowed to operate the telephone with an additional cover.
- Make sure the wiring is voltage-free upon connecting or disconnecting the wires in the terminal room.
- If electrical connections must be carried through in the hazardous area, the enclosure must be opened and closed as follows:
  - Remove voltage from the device.
  - Loosen the fastening screws from the keypad insert.
  - Remove the keypad insert and unfasten the keypad cable.
  - Make the connections while the telephone is open.
  - When the work is done, plug the keypad back on, and place the keypad insert back on the lower part of the telephone.

  Make sure the seal is correctly positioned and in perfect working order. Then tighten the fastening screws in a diagonal pattern.
- Only blind plugs and cable glands as prescribed by the manufacturer may be used.

Should these points not be observed, the explosion protection of the telephone cannot be guaranteed. The telephone then poses a potential threat to the user's life and can cause the ignition of an explosive atmosphere.

2.3.2.5 Requirements

There are no requirements.

2.3.2.6 Explosion Proof Type Versions

The explosion proof telephone is available for delivery in the following version.

- Handset with armed court.
- Single LAN Connection with internal terminals and cable screw caps.
- Housing in black or coloured in red or blue.
- Some sealing plugs to connect option equipment.
- Max. 5 cable screw caps.
- 2 Relays with internal terminals.

Accessories (optional):

- Explosion proof headset and attachment of the bracket.
- Cable screw cap
- Sealing plug
- 2 keys for TORX socket screws TX20, TX30

2.3.2.6.1 Default Version one LAN Connection with a Cable Screw Cap

- 1 LAN connector internal (terminals)
- Housing with 2 cable screw caps and 3 bored holes with sealing plugs at the upper side.

Box contents

The scope of the delivery includes:

- Telephone
- Printed short manual
- Manual on CD
- 2 keys for TORX socket screws TX20, TX30

2.3.2.7 Example Pictures

Figure 7: VoIP Telephone ExResistTel IP2 / IP154 with armed Court and 5 Cable Screw Caps

2.4 Mounting and Installing

2.4.1 Mounting, general

The telephone must be installed on a plane surface in vertical operating position only. Loosen the cover screws (2) (see Figure 9 to Figure 11) and detach the upper part of the telephone (1). If the optional accessory headset is being employed, attach the bracket (10) using two screws (11) to the rear panel of the lower part of the telephone. (With the accessories named before, the bracket and screws are in the scope of delivery. With all accessories a cable gland is delivered.) Put four screws, having a head diameter of 10 to 13 mm into the holes (20) and attach the lower part of the telephone (3) to the wall or to a holder.

Guide the telephone wire through the cable screw cap (4) and place it on the terminals. Only wires having a sheath diameter of 5.5 to 13 mm should be used because otherwise the IP66 housing protection standard is not guaranteed.

Prior to assembly, check cover seal for tightness. Using the plug connector (7), plug the ribbon cable onto the pin contact strip (8) in the upper part of the housing. Attach the upper part of the telephone and fasten it to the lower part of the telephone with the four cover screws (2). Upon disassembly of optional accessories, suited sealing plugs must be used to close the resulting openings.

In this telephone connected cords may have hazardous voltages.

To ensure that no water gets into the enclosure it is essential that no gaskets are damaged during installation. The ingress of water can cause accessible parts of the telephone to become live.

For mounting of the cable screw caps only dedicated toys are allowed.

The cable screw caps are useful for fixed mounted cables only.

The locking torque of the upper part screws (2) is 1.2 … 1.5 Nm.

Installation and connection must be carried out by competent personnel familiar with electrical and network installations.

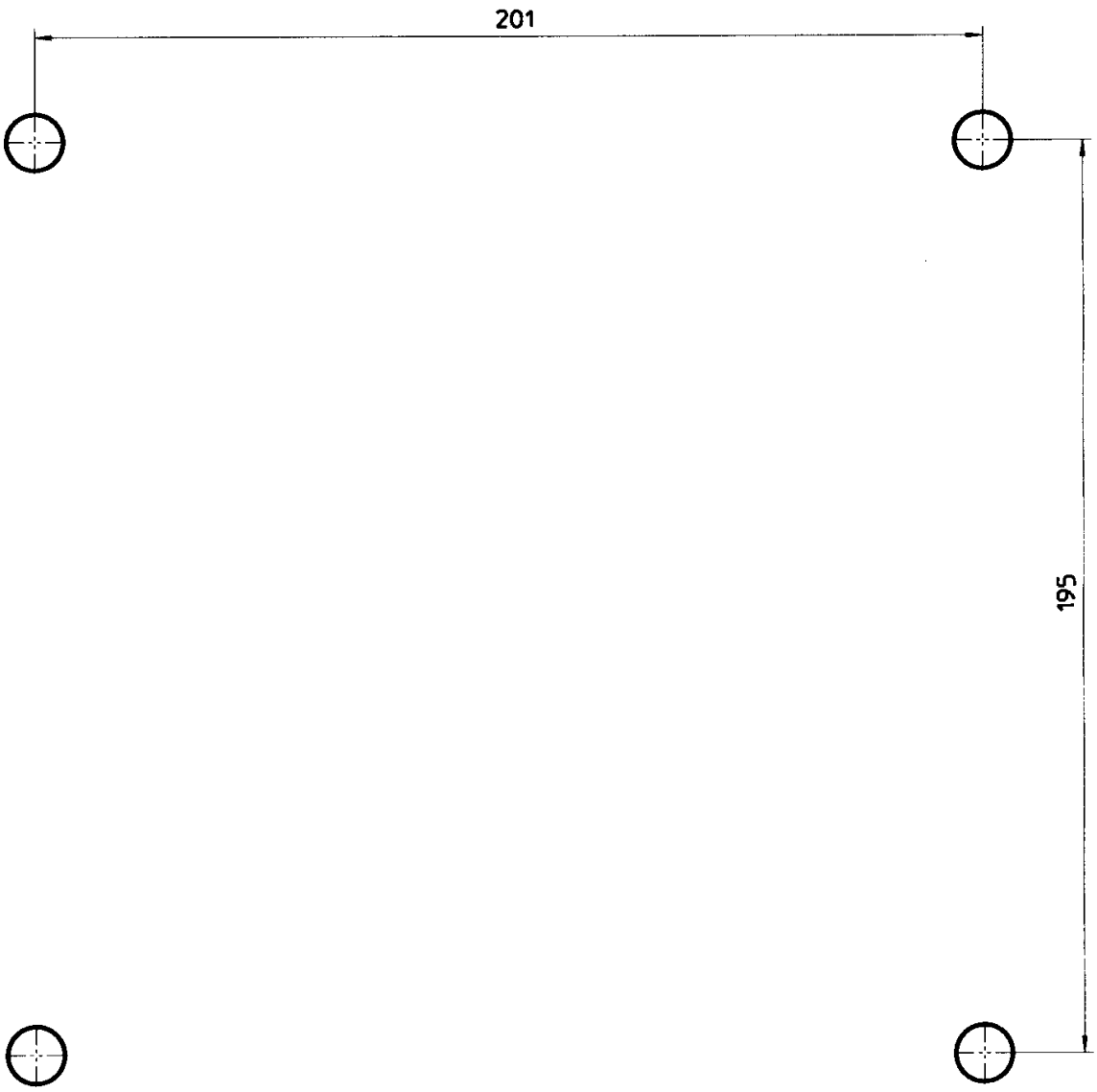


Figure 8: Drilling Diagram Wall Mounting

The diameter of the drilled hole is dependent on the screw employed (screw diameter max. 8 mm) and the type of supporting base material (steel, wood, concrete, plasterboard etc.) and must be chosen accordingly.

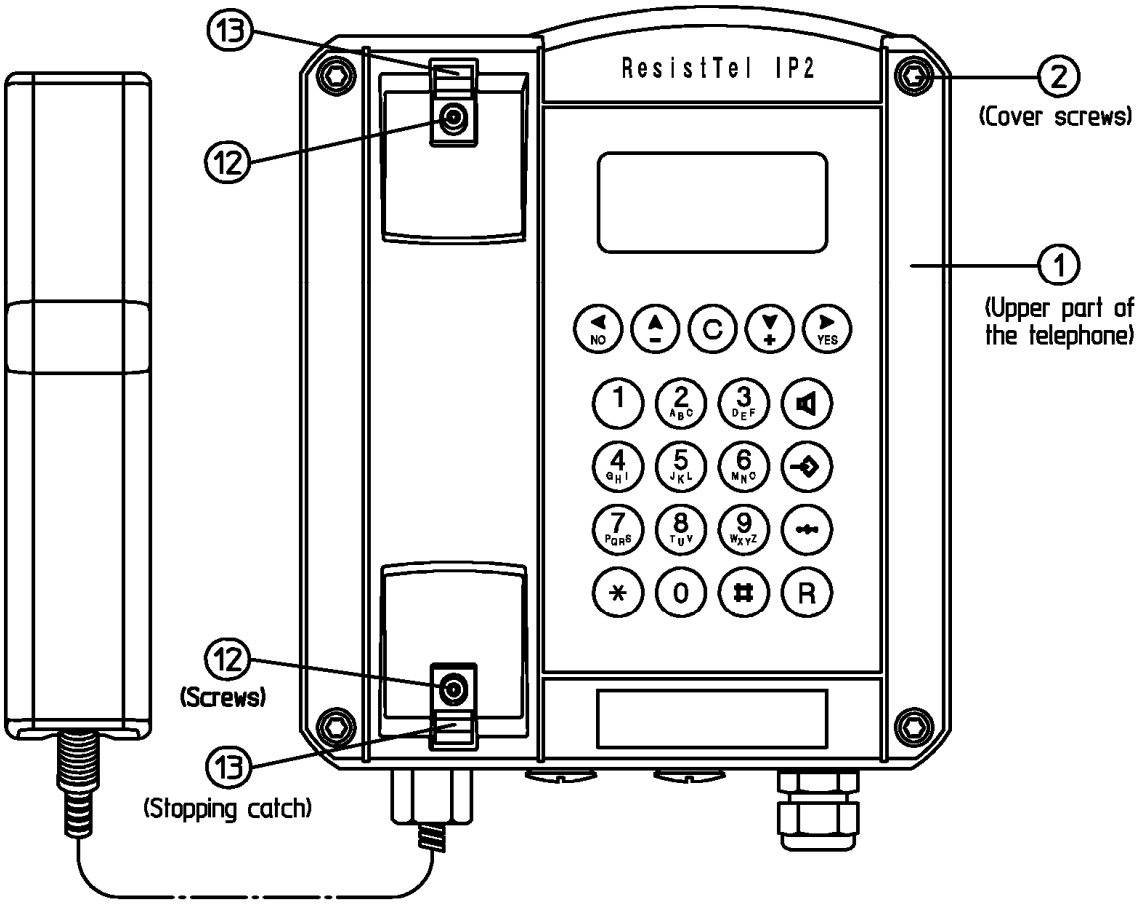


Figure 9: Set View

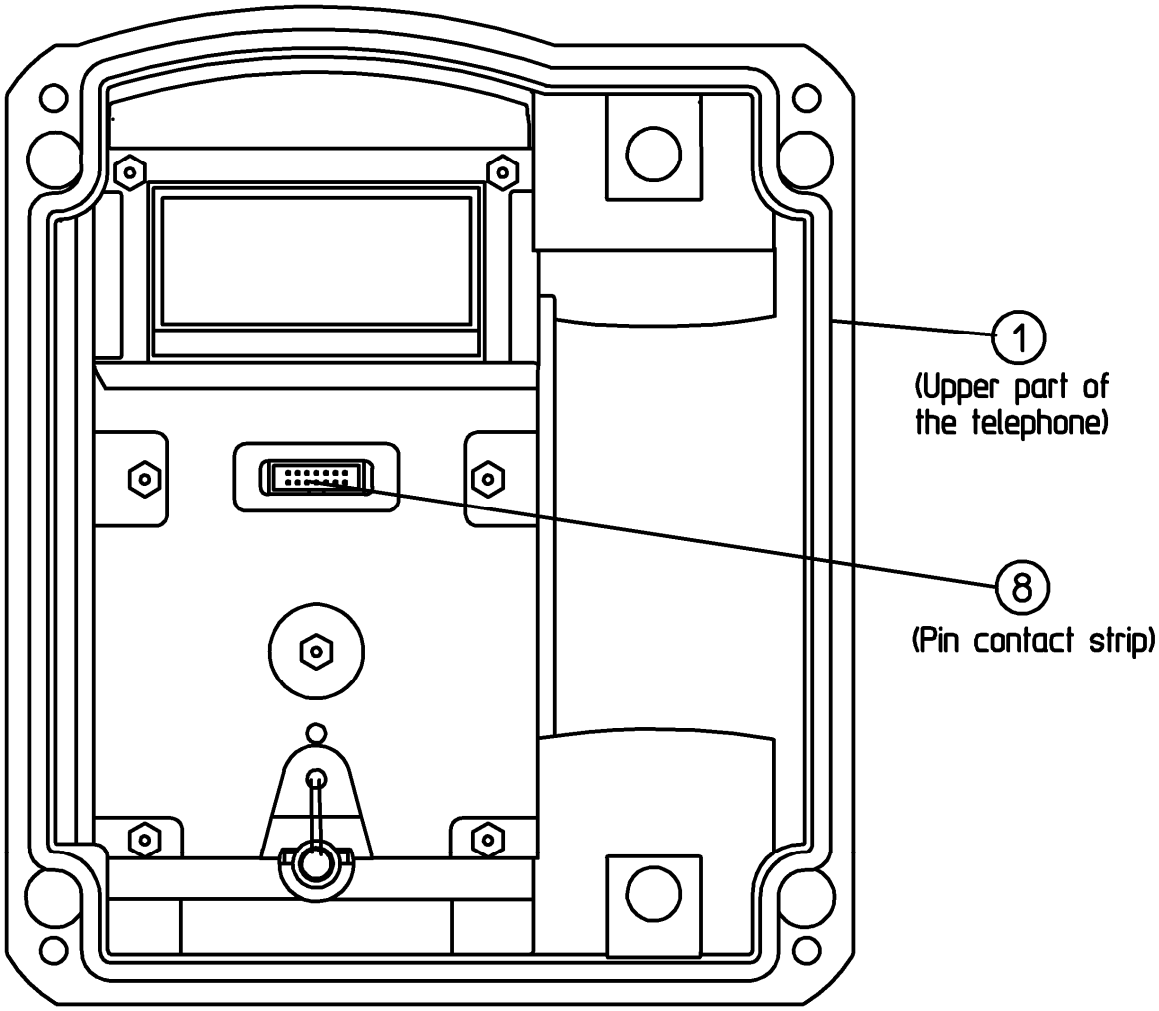


Figure 10: Inside View of Telephone upper Part

2.4.1.1 Weatherproof Telephone, lower Part

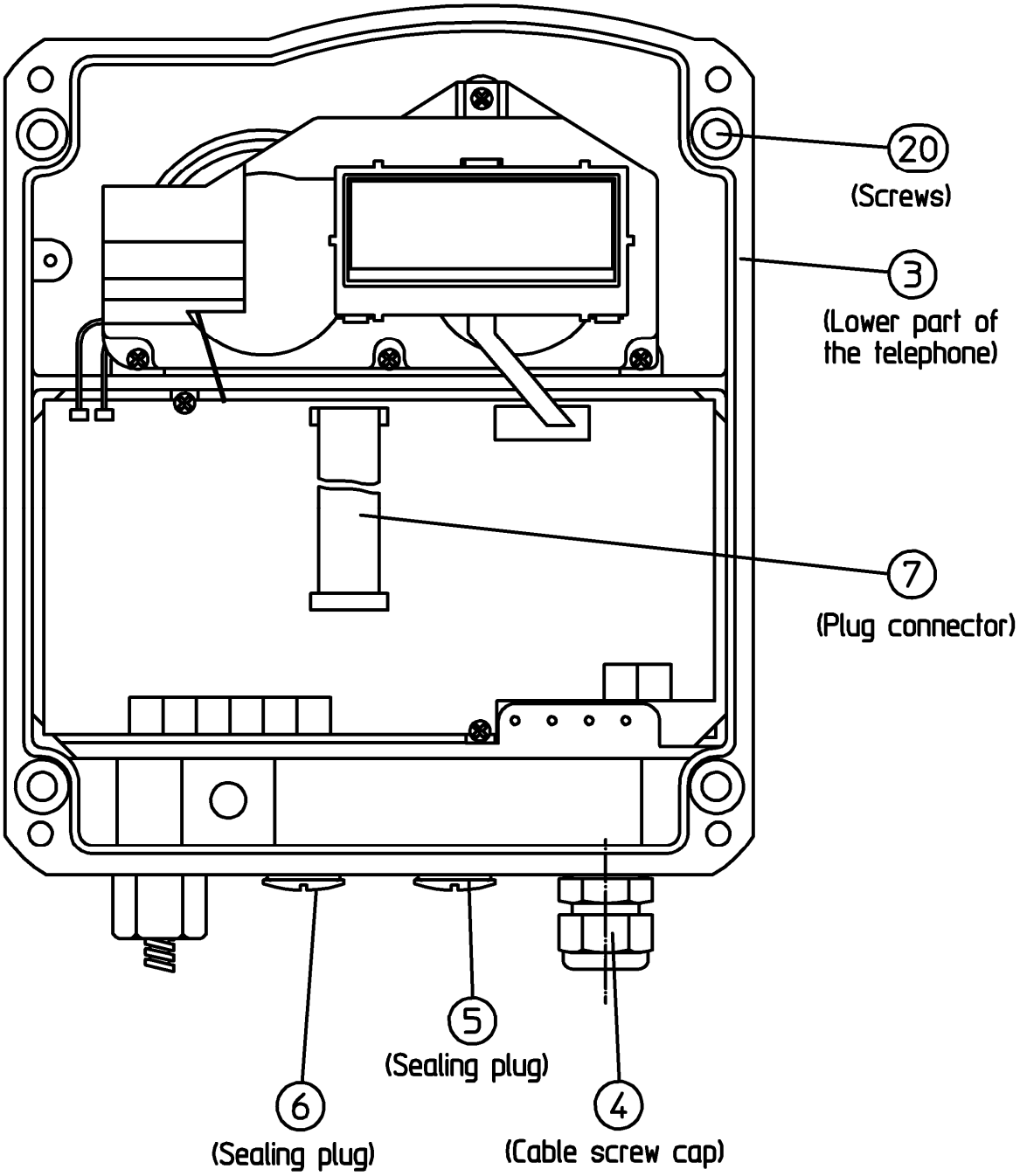


Figure 11: Inside View of Telephone lower Part ResistTel IP2 / IP152

2.4.1.2 Explosion proof Telephone, lower Part

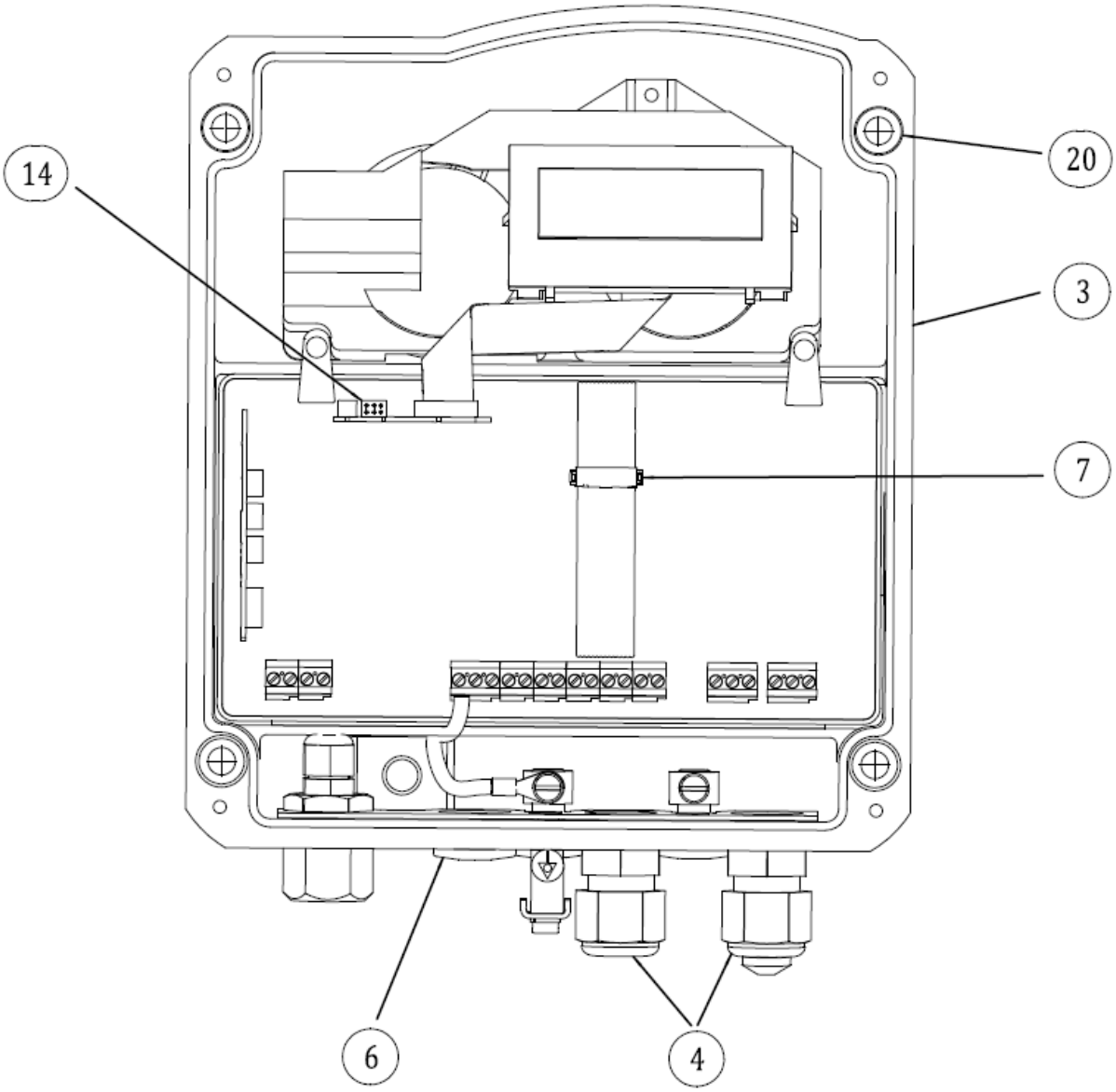


Figure 12: Inside View of Telephone lower Part ExResistTel IP2 / IP154

2.4.1.2.1 Cable Screw Caps of the Explosion Proof Telephone

The preinstalled cable screw caps (4) of the explosion proof telephones have the following properties:

certificate	IECEx PTB 05.0004 X, PTB 99 ATEX 3128 or equivalent
operating temperature	-40 °C to +70 °C
thread diameter	Ø M20 x 1.5
type of ignition protection	Ex e II
type of protection	IP66
cable diameter	Ø 5.5 mm to Ø 13 mm
locking torque coupling ring cable	2.5 Nm to 3.5 Nm

2.4.1.3 Sling Holder

The holding strength for the handset is continuously adjustable.

Loosen the screws (12) and move the stopping catches (13) (See Figure 9 on page 43). Pushing the stopping catches together increases the holding strength whereas pulling them apart reduces it. Tighten the screws again.

2.4.1.4 Receiver

The receiver is equipped with a leakage field spool for coupling of hearing aids. Users of a hearing aid with inductive receiver may receive the signal from the receiver inset directly.

2.4.2 Installation

2.4.2.1 Wiring of an Ethernet Cable

The specific assignments of the cable pairs to connector vary between the T568A and T568B standards.

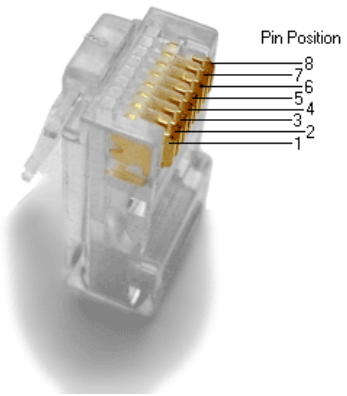
cable pin	T586A pair	T586B pair	signal ID	wire	T568A colour	T568B colour	Pins for plug face (socket is reverse)
1	3	2	DA+	tip	white/green stripe	white/orange stripe	
2	3	2	DA-	ring	green solid	orange solid	
3	2	3	DB+	tip	white/orange stripe	white/green stripe	
4	1	1	DC+	ring	blue solid	blue solid	
5	1	1	DC-	tip	white/blue stripe	white/blue stripe	
6	3	3	DB-	ring	orange solid	green solid	
7	4	4	DD+	tip	white/brown stripe	white/brown stripe	
8	4	4	DD-	ring	brown solid	brown solid	

Table 4: Wiring of an Ethernet Cable

2.4.2.2 Connecting RJ45 plug or RJ45 plug socket

Connect the telephone using a RJ45 plug (socket) with the following normative PoE allocation:

RJ45 Plug			
PIN	Spare-Pair Supply	Phantom Supply	
1	Rx+	Rx+ / V–	Rx+ / V+
2	Rx–	Rx– / V–	Rx– / V+
3	Tx+	Tx+ / V+	Tx+ / V–
4	V+		
5	V–		
6	Tx–	Tx– / V+	Tx– / V–
7	V–		
8	V–		

Table 5: RJ45 Pin Description

Upon connecting the cable, please make sure the exposed conductors are placed in the plug connector and are securely fastened.

2.4.2.3 Power over Ethernet

2.4.2.3.1 Available Power Classes

Class	Maximal available power at the powered device	Minimal injected power at the injector
0	12.96 W	15.4 W
1	3.84 W	4.00 W
2	6.49 W	7.00 W
3	12.95 W	15.4 W
4	25.5 W (only 802.3at/Typ 2)	34.2 W

Table 6: PoE Power Classes

2.4.2.3.2 General Characteristics

Distance

- Cable length up to 100 m

Variants of the power transmission

- Power feeding (power via wires used for data transmission)
- Power via wires not used for data transmission

Variants of the power injection

- Endpoint (direct supply via the switch)
- Midspan (supply via in between sources)

2.4.2.4 Installation of the Weatherproof Telephones

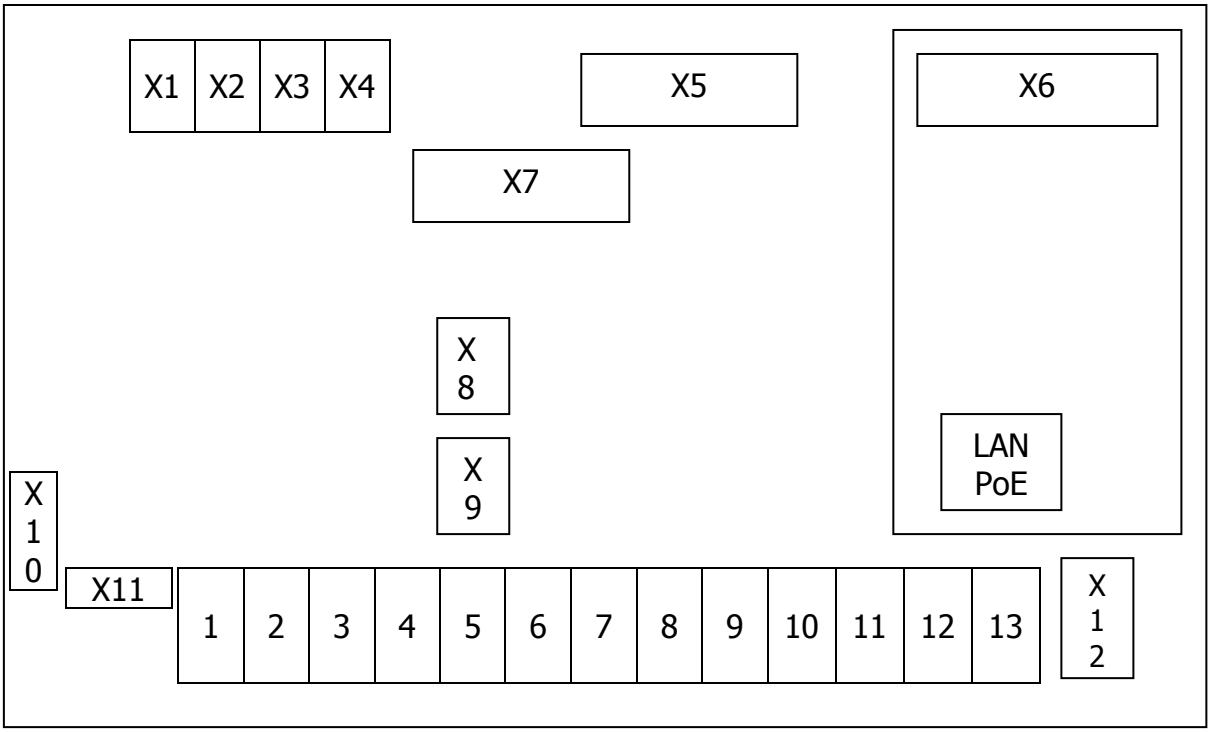


Figure 13: Connection Diagram weatherproof VoIP Telephone with Single LAN Module

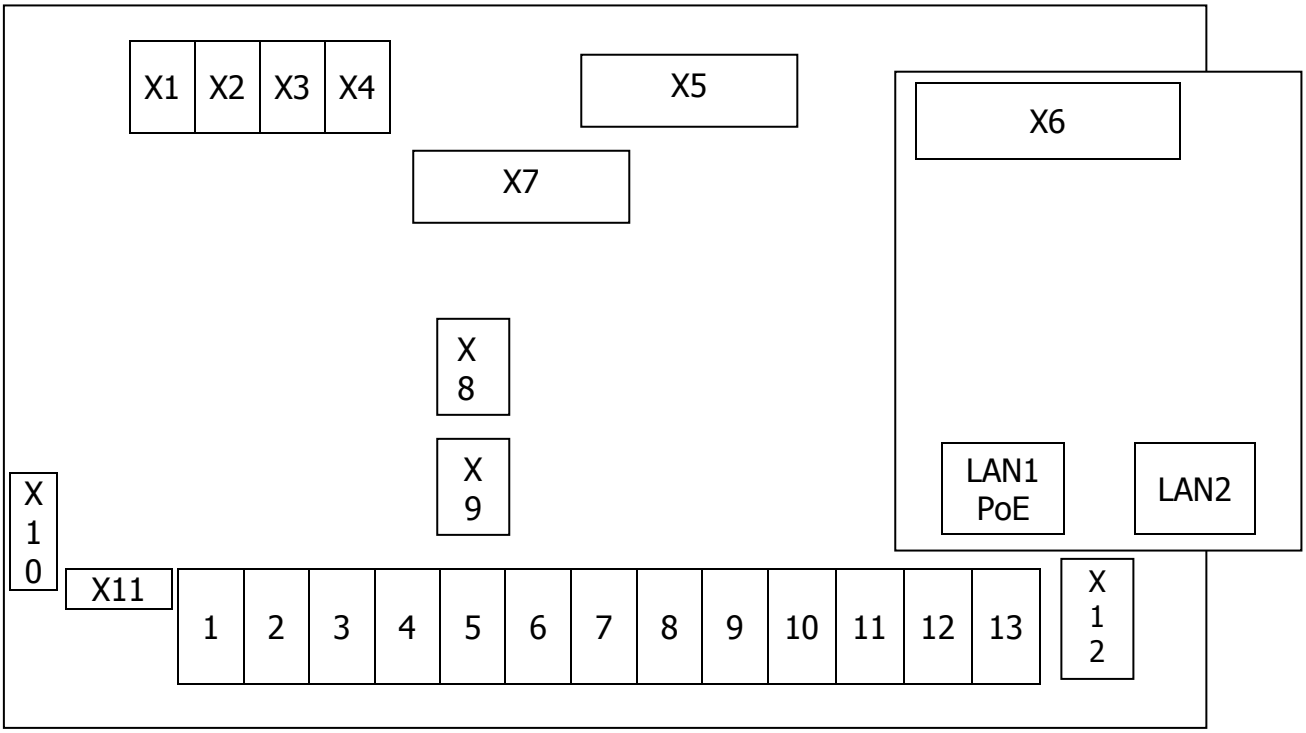


Figure 14: Connection Diagram weather proof VoIP Telephone with Switch LAN Module

Connector	description
X1	Loudspeaker left
X2	Loudspeaker right
X3	Heater of the Display
X4	Illumination of the Display
X5	Display
X6	LAN Module
X7	Keypad
X8	Hookswitch (Reed Contact)
X9	RS232 Module (optional)
X10	Amplifier Module (optional)
X11	Handset
X12	Relay Module (optional)
LAN PoE	LAN with PoE (LAN-Link, single LAN Module)
LAN1 PoE	LAN1 with PoE (LAN-Link, Switch LAN Module)
LAN2 (PC)	LAN2 (PC-Link, Switch LAN Module)
1 - 13	Terminals (Configuration see the following Chapters)

Table 7: Plug in Connectors and Terminals of the ResistTel IP2 / IP152

2.4.2.4.1 LAN-Connections

2.4.2.4.1.1 Default Version one LAN Connection with a Cable Screw Cap

The telephone has in the default version one internal LAN-connection with a cable screw cap. For the connection a LAN cable must be pulled through the cable screw cap. Inside the phone the female LAN connection from Tycoelectronics (AMP) has to be pressed on the cable (Refer to chapter 2.3 beginning on page 22). A female LAN cable connector belongs to the as-delivered condition. With the inside the phone existing little LAN connection cable, the LAN can be connected with the phone.

The LAN delivery can be available with PoE (Power over Ethernet). Alternatively the phone can be supplied with power external.

All not used cable feed through have to be closed with sealing plugs.

2.4.2.4.1.2 Version one LAN Connection with a Female Housing Connection

The phone has in this version one LAN-connection with a female LAN connection at the housing. LAN-cable, used for plug into the telephone ResistTel IP2 / IP152, have to be adapted with a connector from Phoenix contact (Refer to chapter 2.3 beginning on page 22), to preserve the IP66 degree of protection. A LAN cable connector belongs to the as-delivered condition. For the wiring of an Ethernet cable see chapter 2.4.2.1 on page 48.

The LAN-lead wire has to be connected to the connector in the front. Die LAN lead wire can to be with PoE (Power over Ethernet). Alternatively the phone can be supplied with power external.

The second LAN connector of the ResistTel IP2 / IP152 is a blind connector closed with a protective cap to preserve the IP66 degree of protection

All not used cable feed through have to be closed with sealing plugs.

Caution

You can use PoE (Power over Ethernet) or an external connection to supply the ResistTel IP2 / IP152 with power.

Don’t use both at the same time, to prevent damage to the equipment.

2.4.2.4.1.3 Version with Switch LAN Module with two LAN Connections with Cable Screw Caps

The telephone has in this version two internal LAN-connections with a cable screw cap. For the connection the LAN cable must be pulled through the cable screw cap. Inside the phone the female LAN connection from Tycoelectronics (AMP) has to be pressed on the cable (Refer to chapter 2.3 beginning on page 22). A female LAN cable connector belongs to the as-delivered condition. With the inside the phone existing little LAN connection cable, the LAN can be connected with the phone. For the wiring of an Ethernet cable see chapter 2.4.2.1 on page 48.

The LAN1 delivery can be available with PoE (Power over Ethernet). Alternatively the phone can be supplied with power external.

The LAN2 delivery doesn't support PoE. Also it can't be used to connect a phone directly, which should be powered with PoE.

All not used cable feed through have to be closed with sealing plugs.

2.4.2.4.1.4 Version with Switch LAN Module with two LAN Connections with two Female Housing Connections

The phone has in this version two LAN-connections with a female LAN connection at the housing. LAN-cable, used for plug into the telephone ResistTel IP2 / IP152, have to be adapted with a connector from Phoenix contact (Refer to chapter Refer to chapter 2.3 beginning on page 22), to preserve the IP66 degree of protection. A LAN cable connector belongs to the as-delivered condition. For the wiring of an Ethernet cable see chapter 2.4.2.1 on page 48.

The LAN-lead wire has to be connected to the connector in the front. Die LAN1 lead wire can to be with PoE (Power over Ethernet). Alternatively the phone can be supplied with power external.

The second LAN connector of the ResistTel IP2 / IP152 doesn't support PoE. Also it can't be used to connect a phone directly, which should be powered with PoE.

If the second LAN connector of the ResistTel IP2 / IP152 will not be used, it has to be closed with the at the phone available protection plug to preserve the degree of protection IP66.

All not used cable feed through have to be closed with sealing plugs.

2.4.2.4.2 External Power Supply Connection

An external power supply can be adapted to the terminals 5 (+) and 6 (–). The voltage has to be:

- Without using the optional voltaic separated inputs: 15 V – 57 V DC, 12.95 W
- With using the optional voltaic separated inputs: 21.5 V – 57 V DC, 12.95 W

If the external power connection will be used, you must not use PoE at the LAN connection.

2.4.2.4.3 Relay Connection

The phone can be build up with a relay module with two relays with a single changeover switch optional.

The maximal breaking capacity of a relay is depending on the voltage:

- 240 V, 6 A, AC
- 24 V, 6 A, DC
- 32 V, 5 A, DC
- 45 V, 1 A, DC

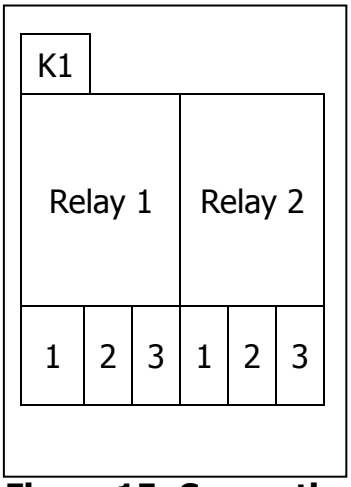


Figure 15: Connection Diagram Relay Module ResistTel IP2 / IP152

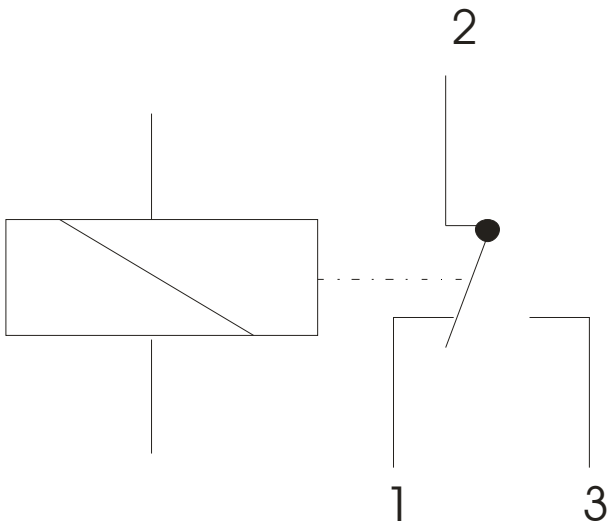


Figure 16: Connection Configuration Relay weatherproof Telephone (Exposition: Relay not active)

Connector	Description
K1	Cable to the main board (connection to plug in X12)
1 (relay 1)	Idle contact relay 1
2 (relay 1)	Base contact relay 1
3 (relay 1)	Switching contact relay 1
1 (relay 2)	Idle contact relay 2
2 (relay 2)	Base contact relay 2
3 (relay 2)	Switching contact relay 2

Table 8: Plug in Connectors and Terminals of the Relay Module of the Telephone ResistTel IP2 / IP152

The relay terminals are below a cover to be protected against random touching.

Pay particular attention to the following points if hazardous voltages (>48V) are to be connected to the relay outputs:

- Cable and cords must be insulated and have to be conducted below the cover.
- The circuits that the relay outputs are connected to must be of the same type; i.e. both mains, both SELV or both TNV circuits.
- It is not permissible to connect different types of circuits to these relays.

2.4.2.4.4 Other Terminals, Voltaic Separated Inputs

The terminals 7 – 13 voltaic separated inputs are provided. All of the voltaic separated inputs have a common null potential. Closing contacts (e. g. external push-buttons) can be connected at the inputs. The switching load for the closing contacts is 60 V DC, 10 mA.

Terminal	Description
7	Null potential of the voltaic separated inputs
8	Null potential of the voltaic separated inputs
9	Input 1
10	Input 2
11	Input 3
12	Input 4
13	Input 5

Table 9: Terminals of the voltaic separated Inputs

Caution

While using the voltaic separated inputs with external power supply, the input voltage has to be 21.5 V – 57 V DC.

2.4.2.4.5 Headset Weatherproof Telephones

Figure 17: Headset Type 5570-1 (MT53H79B-69, Order Number: 11264304)

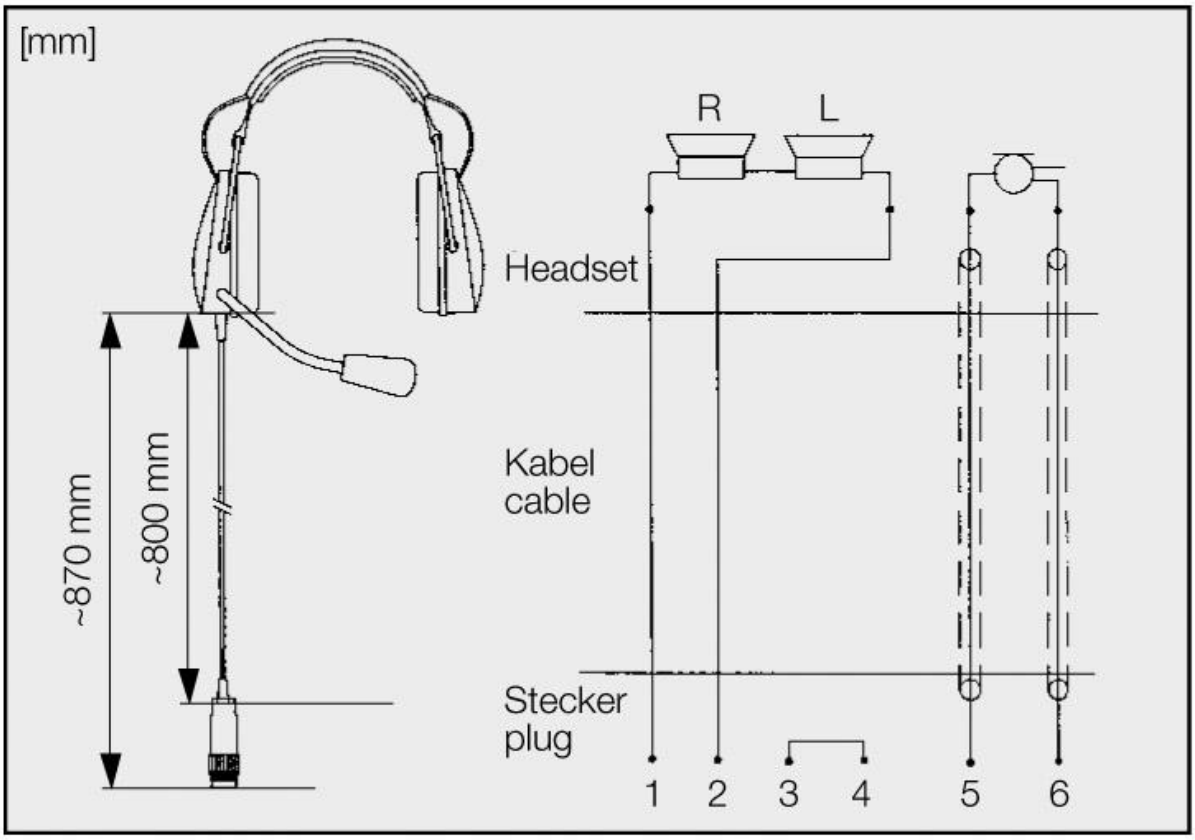


Figure 18: Headset Dimensions Type 5570-1 (MT53H79B-69, Order Number: 11264304)

2.4.2.4.5.1 Note

Prior to installing the headset, these operating instructions and the manual of the headset (MT53H79B-69) must be read carefully.

2.4.2.4.5.2 Application

The Headset-Kit permits the connection of a headset to the weather resistant telephone ResistTel IP2 / IP152. The headset improves essentially the communication in ambient noise areas. It protects against harmful ambient noise. It permits telephone communication during activities where both hands are needed.

2.4.2.4.5.3 Packing Contents

The kit consists of:

- Headset with dynamic receiver insets, noise compensating electret near field response microphone with windshield and gooseneck, as well as 80 cm smooth cord with connecting plug.

- A14 m long connecting cord with a connecting jack at one end and with wire ends with wire end sleeves at the other end to connect to the ResistTel IP2 / IP152.

- Cable gland M20x1.5 to lead the connecting cord into the ResistTel IP2 / IP152.

- Bracket and screws to hang up the connecting cord and the headset.

2.4.2.4.5.4 Mounting and Connection

For the attachment of the bracket there are two built in threaded bushings in the rear side of the ResistTel IP2 / IP152 case. The bracket has mating drill holes through which it can be fastened by means of flat head screws. So if you want to use the bracket it has to be mounted first on to the rear side of the telephone. Afterwards the wall mounting of the phone can take place. To connect the headset remove one of the sealing plugs to be found at the bottom part of the ResistTel IP2 / IP152 case and screw in the cable gland M20x1.5 IP66 completely. The wire ends in grey and pink have to be cut off as short as possible. Lead the connecting cord with the wire ends through the cable gland, fasten the cord with the cable gland and connect the other wire ends (according to the connection table) to the terminals in the ResistTel IP2 / IP152.

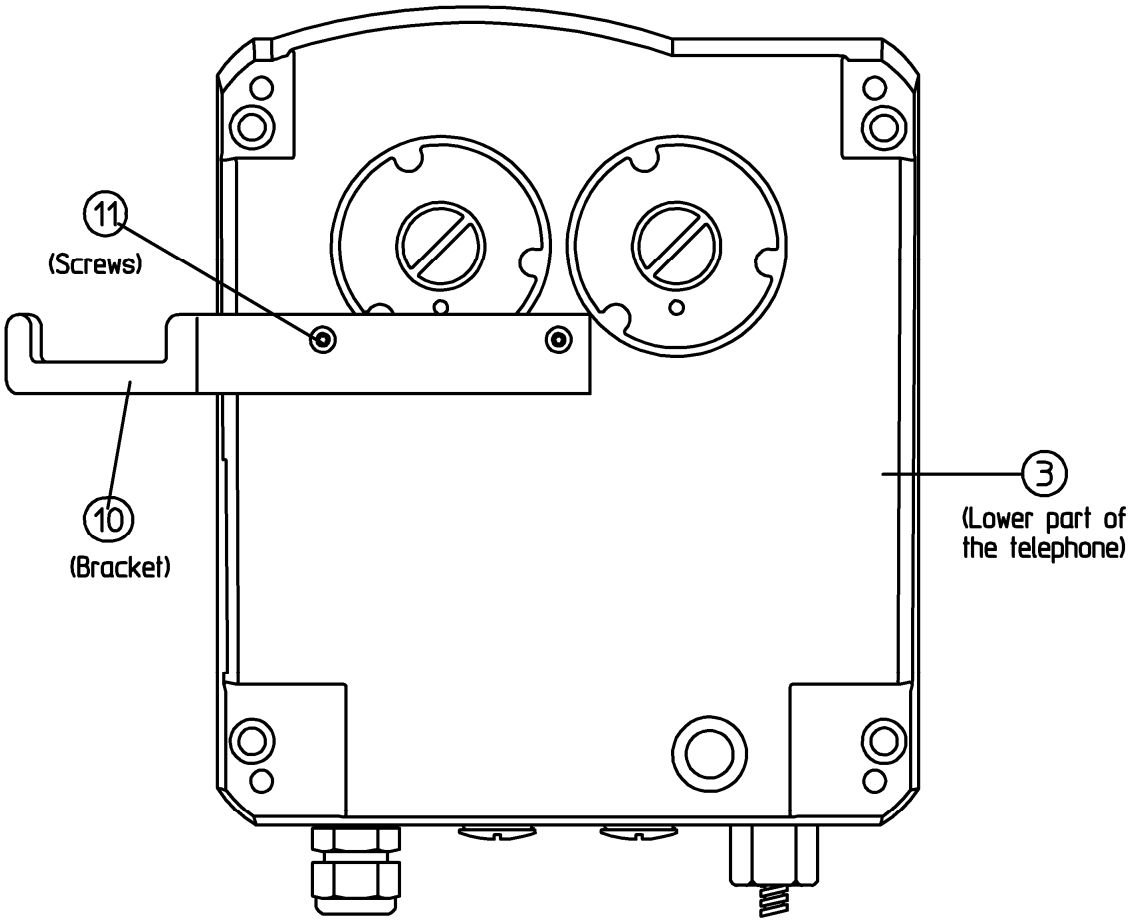


Figure 19: Outside View of Telephone lower Part ResistTel IP2 / IP152

Wire Colour	Number	Terminal
white	3	KGM+
brown	4	KGM–
yellow	1	KGH+
green	2	KGH–
grey	—	KGS1
pink	—	KGS2

Table 10: Connection of the Headset at the VoIP Telephone ResistTel IP2 / IP152

2.4.2.4.5.5 Commissioning and Operation

The headset must be released in the configuration of the ResistTel IP2 / IP152, to be used. The use of headset for calls will be controlled with the headset key (Key long (longer than a second) and afterwards press the hands free key .).

2.4.2.4.5.6 Maintenance

When cleaning, ensure that no moisture is allowed to penetrate the inside of the headset. Do not use any solvents (e.g. fuel, alcohol etc.). Remove any loose dust with a soft brush. If necessary, clean the outside with a suitable clean tissue only slightly moistened with clear water and subsequently rub the telephone dry again. If heavily soiled, a little dishwashing liquid can be used in addition. Clean the plug terminals with a commonly available contact cleaning agent.

2.4.2.4.5.7 Disposal

The complete disposal of the headset will be carried out by the electronic waste. By dismounting the components plastic, metal and electronics have to be disposed separately. In each case the disposal conditions of the respectively country have to be respected.

2.4.2.4.5.8 User Information

The headset is intended to be used only with the weather resistant phone ResistTel IP2 / IP152.

After use, keep the headset at normal room temperature and at normal relative air humidity.

The permissible operating temperature range is -10°C to +55°C; the permissible storage temperature range is -40°C to +80°C.

Do not twist the flexible gooseneck and do not carry the headset by the gooseneck.

When operating the headset, please heed the legal and commercial / industrial regulations, accident prevention regulations and electrical regulations / provisions.

Ensure that the connection cord does not get caught up in operational machines or wheels.

Before repair, the headset has to be disconnected from the ResistTel IP2 / IP152.

2.4.2.5 Installation of the Explosion Proof Telephones

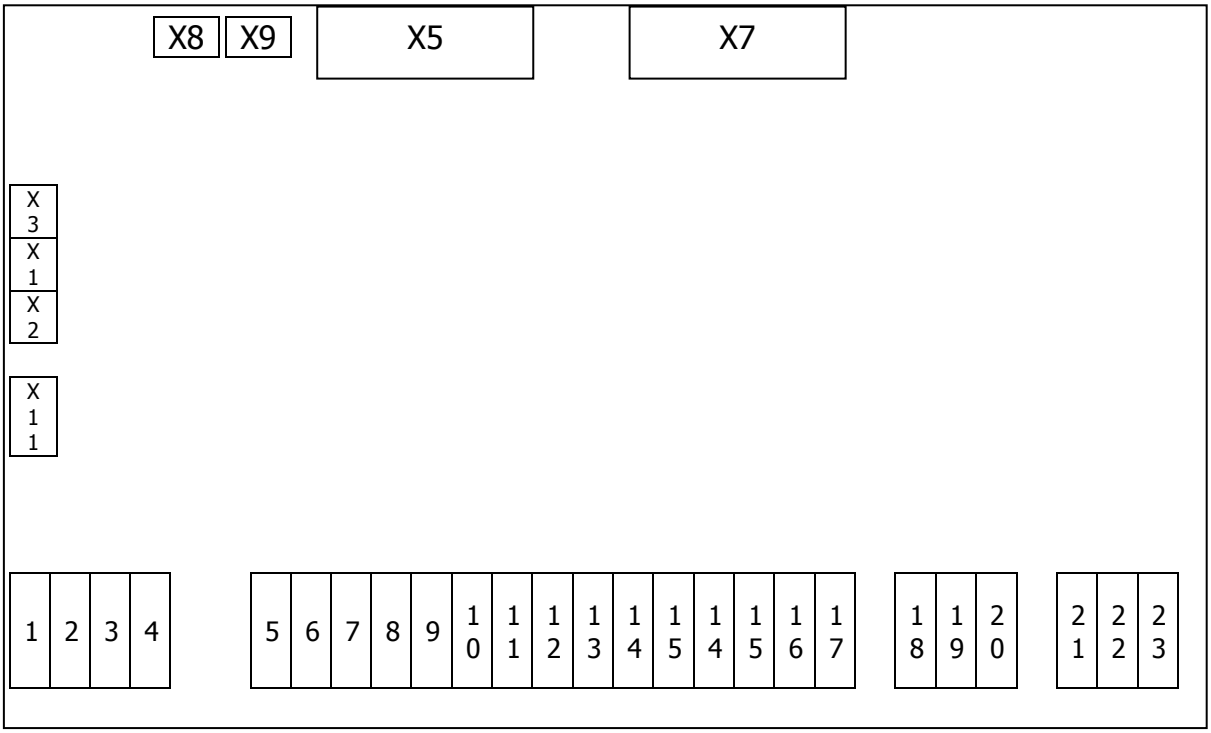


Figure 20: Plug Connectors and Data Links of the Explosion Proof VoIP Telephone ExResistTel IP2 / IP154

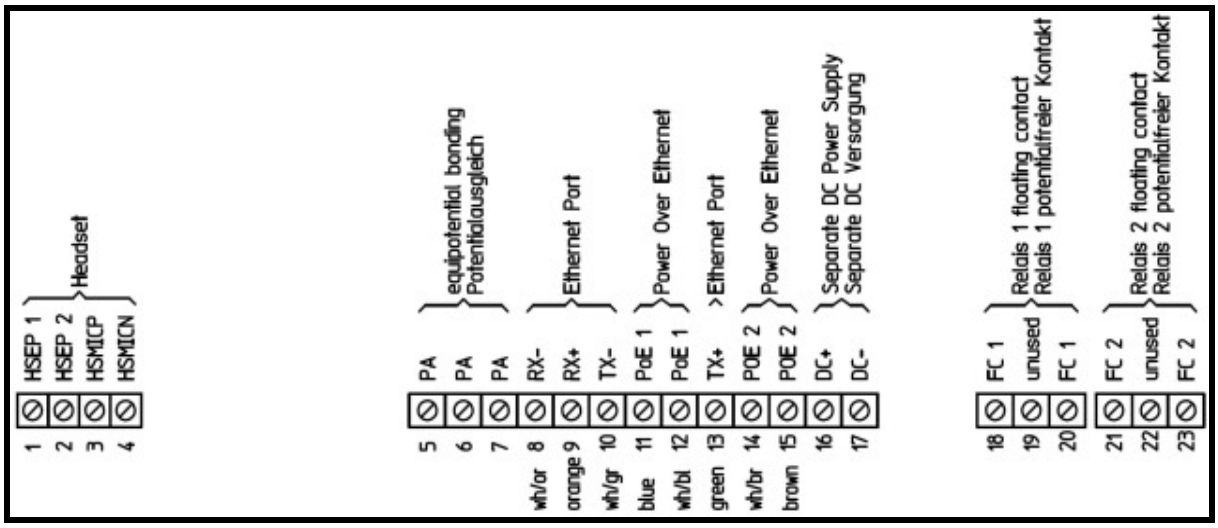


Figure 21: Terminals of the Explosion Proof VoIP Telephone ExResistTel IP2 / IP154

Connector	Description
X1	loudspeaker left (ringing)
X2	loudspeaker right (hands free and ringing)
X3	heating and illumination for the display
X5	display
X7	keypad
X8	hook switch (reed contact)
X9	RS232 module (optional)
X11	handset
1 – 23	terminals (configuration see the following chapter)

Table 11: Plug in Connectors and Terminals of the ExResistTel IP2 / IP154

2.4.2.5.1 Connection Potential Equalisation

The terminals 5 – 7 are available for the potential equalisation. The terminal 5 is reserved fort he connection of the printed board with the potential equalisation bolt.

2.4.2.5.2 Ethernet Connection

At the terminals 8 – 15 the Ethernet cable inclusive PoE can be connected. The assignment is as follows:

terminal	description
8	Rx –
9	Rx +
10	Tx –
11	PoE1
12	PoE1
13	Tx +
14	PoE2
15	PoE2

Table 12: Ethernet Connection of the ExResistTel IP2 / IP154

PoE will be supported with the unused pairs of data lines of a 10/100 Mbit/s Ethernet connection only. The polarity will be recognised by the phone automatically. For the wiring of an Ethernet cable see chapter 2.4.2.1 on page 48.

If the Ethernet interface of the VoIP telephone is configured to the auto or auto-mdi mode, the Rx and Tx pairs can be exchanged, because the telephone recognizes in these cases receive and transmit automatically.

2.4.2.5.3 External Power Supply Connection

An external power supply can be connected to the terminals 16 (+) and 17 (–). The following voltage will be necessary:

- U_n:19.2 V – 52.8 V DC
- U_m: 53 V
- I_{sc}: 100 A

If an external power supply is in use, the LAN connection must not be connected to PoE.

2.4.2.5.4 Relay Connection

The telephone has two relays with each a single switch at its proposal.

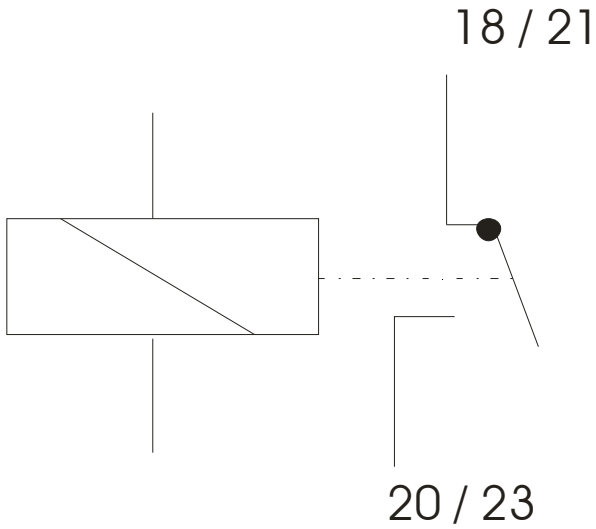


Figure 22: Terminal Assignment Relays of the Explosion proof VoIP Telephone ExResistTel IP2 / IP154 (Exposition: Relay not active)

terminal	description
18 (relay 1)	base contact relay 1
19 (relay 1)	not used
20 (relay 1)	switching contact relay 1
21 (relay 2)	base contact relay 2
22 (relay 2)	not used
23 (relay 2)	switching contact relay 2

Table 13: Terminals of the Relays of the Explosion proof VoIP Telephone ExResistTel IP2 / IP154

The relay terminals are below a cover to be protected against random touching.

2.4.2.5.5 Examples for Connection

2.4.2.5.5.1 Example for Connection 1

- LAN with PoE supply (red) and with shield (green)
- Potential equalisation connection outside (green)

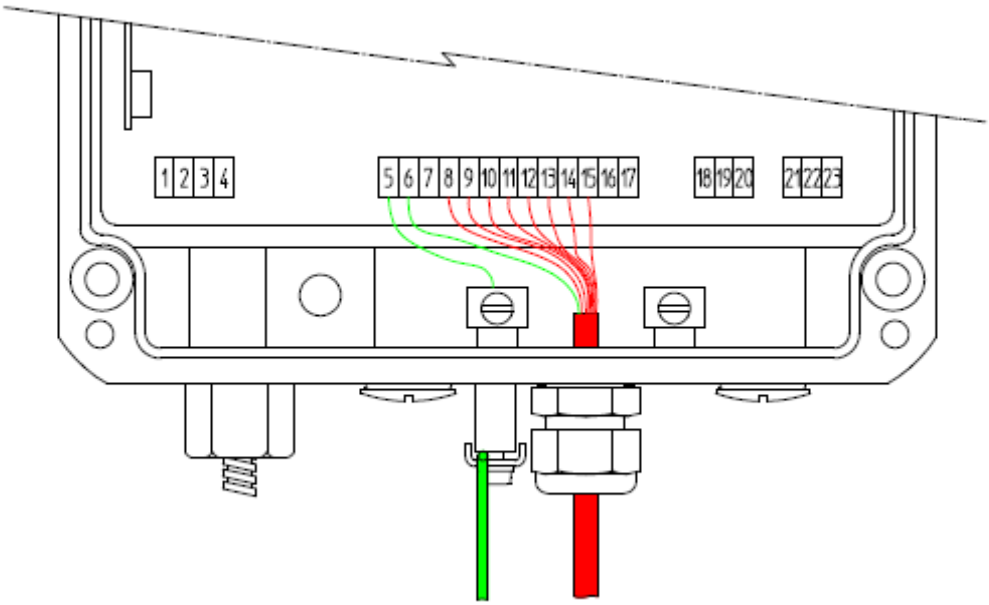


Figure 23: Example for Connection 1

2.4.2.5.5.2 Example for Connection 2

- LAN with PoE supply (red) and with shield (green)
- Potential equalisation connection inside (green)

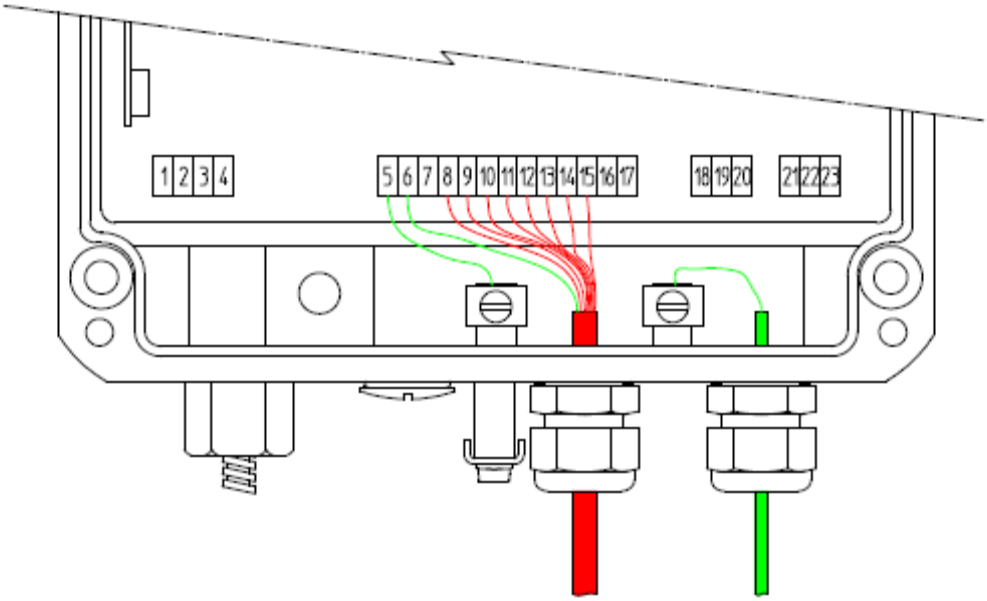


Figure 24: Example for Connection 2

2.4.2.5.5.3 Example for Connection 3

- LAN without PoE supply (red) and with shield (green)
- DC supply without earth connection line (red)
- Potential equalisation connection outside (green)

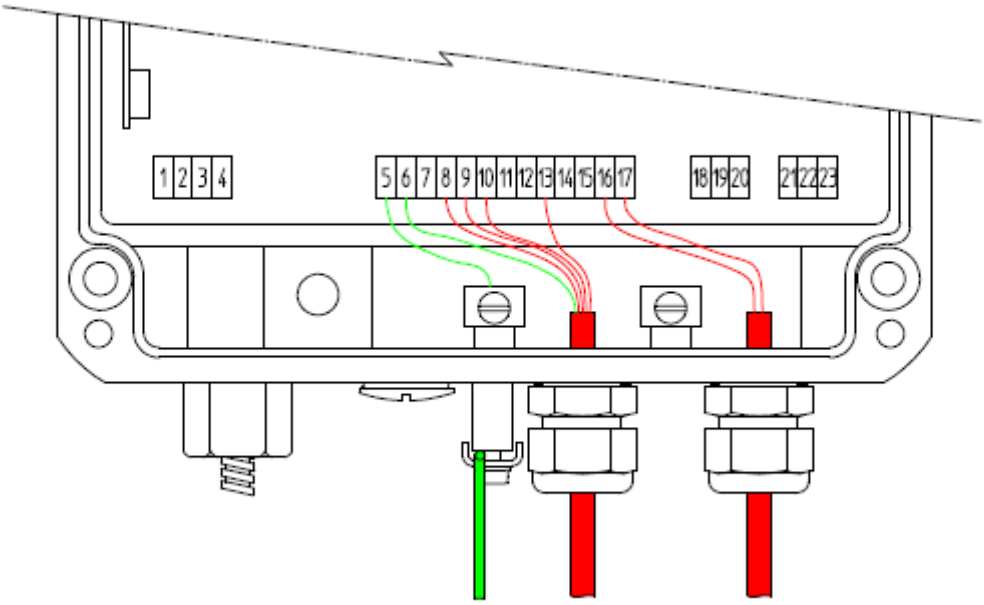


Figure 25: Example for Connection 3

2.4.2.5.5.4 Example for Connection 4

- LAN without PoE supply (red) and with shield (green)
- DC supply (red) with earth connection line (green)
- Potential equalisation connection inside (green)

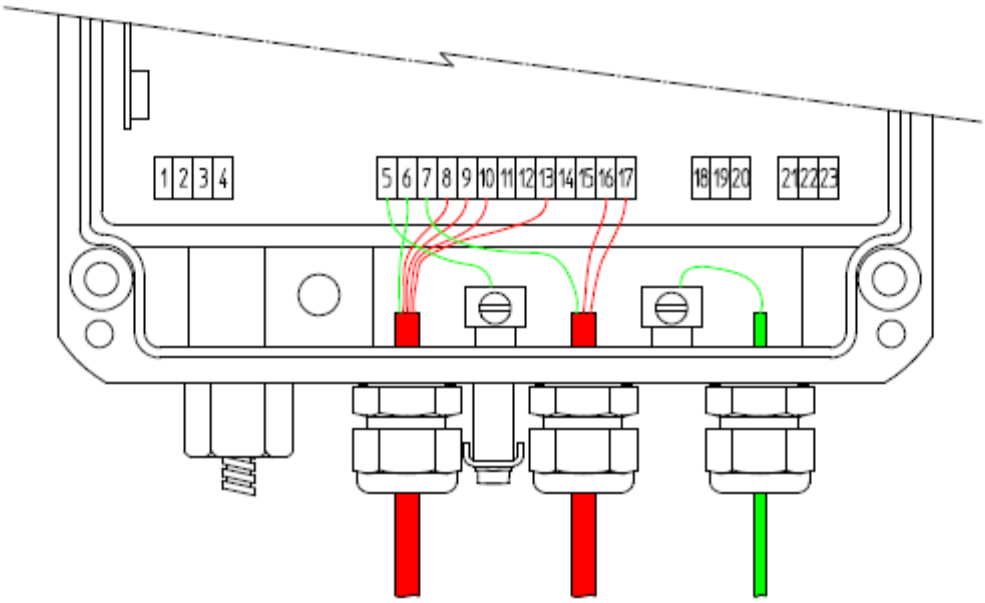


Figure 26: Example for Connection 4

2.4.2.5.5.5 Example for Connection 5

- LAN without PoE supply (red) and with shield (green)
- DC supply (red) without earth connection line (green)
- Two relay connections (violet) with earth connection line (green)
- Potential equalisation connection outside (green)
- Headset connection (blue)

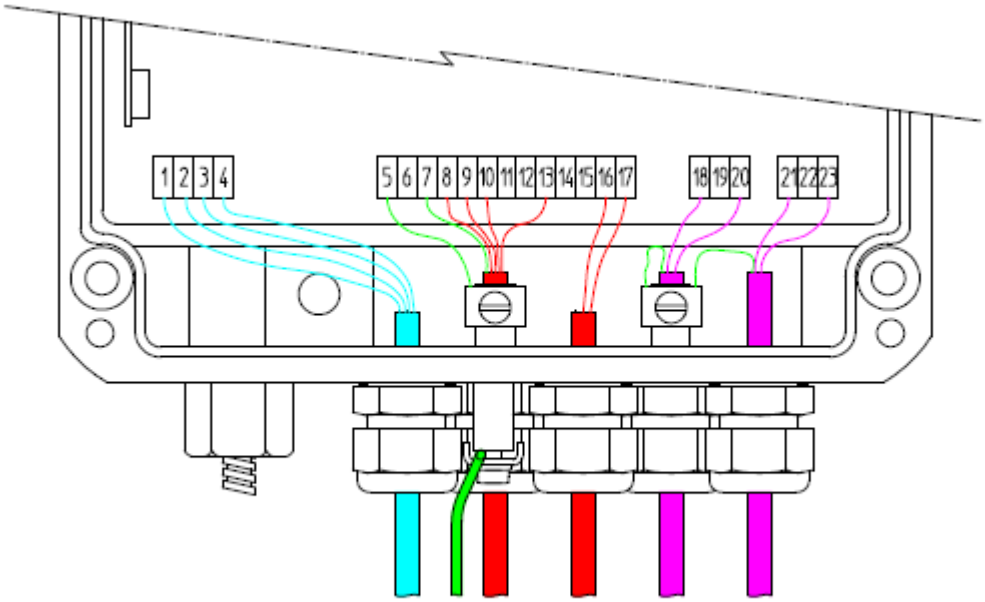


Figure 27: Example for Connection 5

2.4.2.5.6 Headset for the Explosion Proof Telephone

Figure 28: Headset Type 5570 (MT53H79B-56, Nemko 02 ATEX 059 X, Order Number: 11286104)

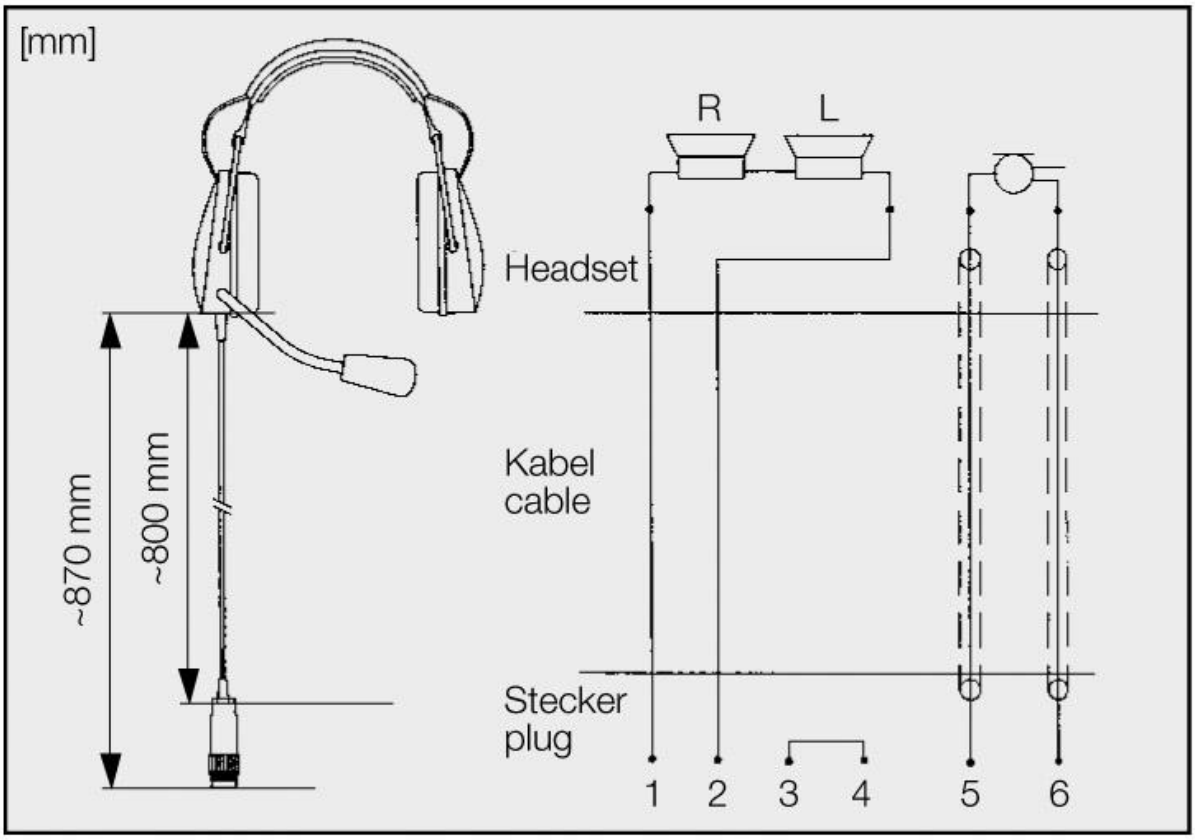


Figure 29: Headset Dimensions Type 5570 (MT53H79B-56, Nemko 02 ATEX 059 X, Order Number: 11286104)

2.4.2.5.6.1 Note

Prior to installing the headset, this operating instruction and the manual of the headset MT53H79B-56 (Nemko 02 ATEX 059 X, order number: 11286104) must be read carefully.

2.4.2.5.6.2 Application

The Headset-Kit permits the connection of a headset to the explosion proof telephone ExResistTel IP2 / IP154. The headset improves essentially the communication in ambient noise areas. It protects against harmful ambient noise. It permits telephone communication during activities where both hands are needed.

2.4.2.5.6.3 Packing Contents

The kit consists of:

- Headset with dynamic receiver insets, noise compensating electret near field response microphone with windshield and gooseneck, as well as 80 cm smooth cord with connecting plug.

- A 14 m long connecting cord with a connecting jack at one end and with wire ends with wire end sleeves at the other end to connect to the ExResistTel IP2 / IP154.

- Cable gland M20x1.5, IP66, EEx e II, -25°C bis +60°C to lead the connecting cord into the ExResistTel IP2 / IP154.

- Bracket and screws to hang up the connecting cord and the headset.

2.4.2.5.6.4 Mounting and Connection

For the attachment of the bracket there are two built in threaded bushings in the rear side of the ExResistTel IP2 / IP154 case. The bracket has mating drill holes through which it can be fastened by means of flat head screws. So if you want to use the bracket it has to be mounted first on to the rear side of the ExResistTel IP2 / IP154. Afterwards the wall mounting of the phone can take place. To connect the headset remove one of the sealing plugs to be found at the bottom part of the ExResistTel IP2 / IP154 case and screw in the cable gland M20x1.5, IP66, EEx e II completely. The wire ends in grey and pink have to be cut off as short as possible. Lead the connecting cord with the wire ends through the cable gland, fasten the cord with the cable gland and connect the other wire ends (according to the connection table) to the terminals in the ExResistTel IP2 / IP154.

☞	**Note** The installation prescribed in the regulations according to IEC/EN 60079-14 and the national installation regulations have to be respected.	☞

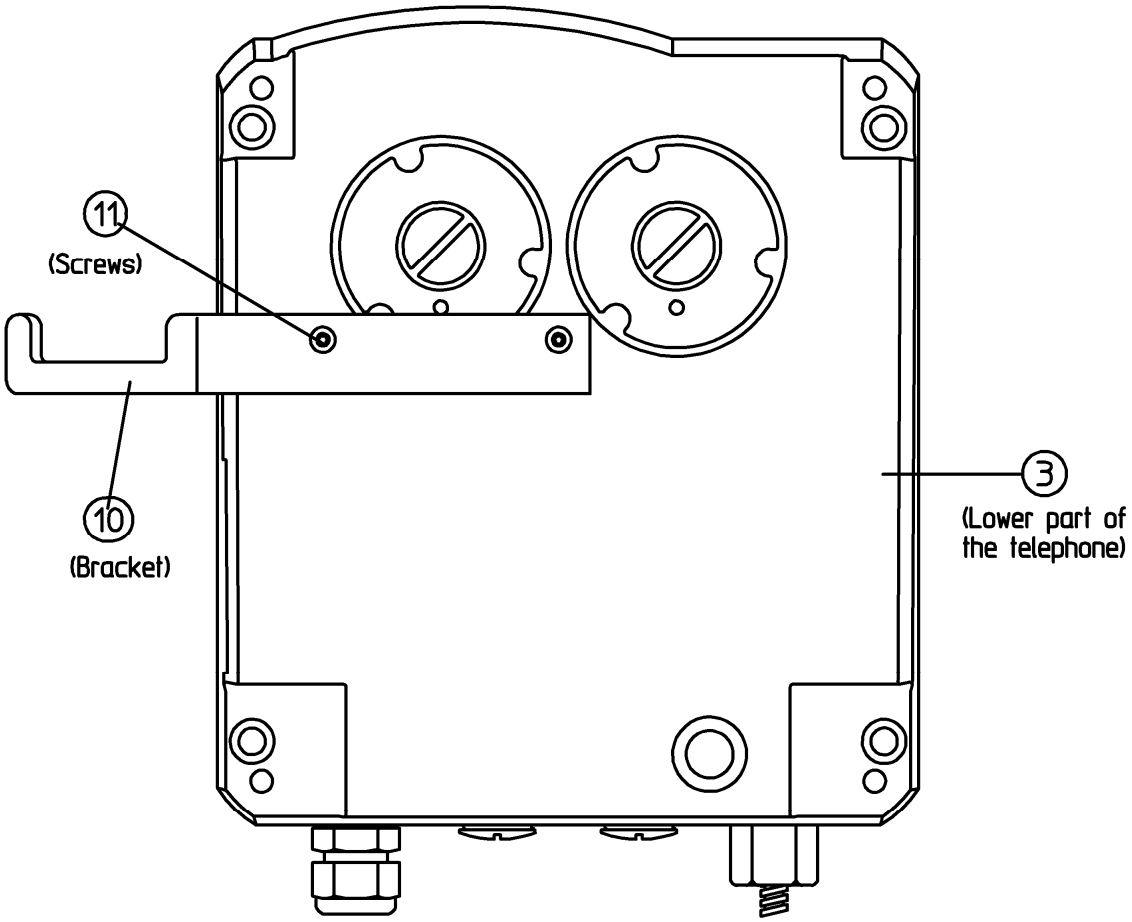


Figure 30: Outside View of the lower Part of the Explosion Proof VoIP Telephone ExResistTel IP2 / IP154

wire colour	number	terminal
white	3	KGM+
brown	4	KGM–
yellow	1	KGH+
green	2	KGH–
grey	—	KGS1
pink	—	KGS2

Table 14: Connection of the Headset at the Explosion Proof VoIP Telephone ExResistTel IP2 / IP154

2.4.2.5.6.5 Commissioning and Operation

The headset must be released in the configuration of the ExResistTel IP2 / IP154, to be used. The use of headset for calls will be controlled with the headset key (Key long (longer than a second) and afterwards press the hands free key .).

2.4.2.5.6.6 Maintenance

When cleaning, ensure that no moisture is allowed to penetrate the inside of the headset. Do not use any solvents (e.g. fuel, alcohol etc.). Remove any loose dust with a soft brush. If necessary, clean the outside with a suitable clean tissue only slightly moistened with clear water and subsequently rub the telephone dry again. If heavily soiled, a little dishwashing liquid can be used in addition. Clean the plug terminals with a commonly available contact cleaning agent.

2.4.2.5.6.7 Disposal

The complete disposal of the ex-headset will be carried out by the electronic waste. By dismounting the components plastic, metal and electronics have to be disposed separately. In each case the disposal conditions of the respectively country have to be respected.

2.4.2.5.6.8 User Information

The headset is intended to be used only with the explosion proof phone ExResistTel IP2 / IP154.

After use, keep the headset at normal room temperature and at normal relative air humidity.

The permissible operating temperature range is -10°C to +40°C; the permissible storage temperature range is -40°C to +55°C.

Do not twist the flexible gooseneck and do not carry the headset by the gooseneck.

When operating the headset, please heed the legal and commercial / industrial regulations, accident prevention regulations and electrical regulations / provisions.

Ensure that the connection cord does not get caught up in operational machines or wheels.

Before repair, the headset has to be disconnected from the ExResistTel IP2 / IP154.

The important user information in the manual of the ex-headset MT53H79B-56 has to be respected.

2.4.2.5.6.9 Technical Data of the Ex-Headset MT53H79B-56

Explosion category	II 2 G EEx ib IIC T4
EG type examination certificate	Nemko 02ATEX059X
Safety parameter for intrinsic safety	Ui = 17 V, Ii = 110 mA Pi = 110 mW, Li = 16 mH Ri = 263 Ω, Li/Ri = 61 µH/Ω

2.5 Commissioning

After connecting to the Ethernet and the power supply the telephone will be ready for use electrically.

An additional commissioning of the switching technology with configuration of the telephone (and the PBX) will be necessary.

3 Operating Manual

3.1 Operating Basics

The keys below the display (◀ ▼ Ⓒ ▲ ▶) of the VoIP telephone serve menu navigation and for edit field input purposes are assigned an additional function on top of their actual function, as explained below.

Key assignment in menu:

The function …	… is performed by …
scrolling upwards	Arrow key up ▲
scrolling downwards	Arrow key down ▼
one level up without saving	Arrow key left ◀
one level down	Arrow key right ▶
one level up with saving	Menu key
Leave the menu complete immediately	Disconnect key

Key assignment in edit field:

The function …	… is performed by …
scrolling right	Arrow key right ▶
scrolling left	Arrow key left ◀
Delete character in front of cursor	Clearing key Ⓒ

Pressing and holding the numeric key, activates the **character mode**. Refer to chapter 3.1.5 Input of Characters and Special Characters beginning on page 79.

The **initial condition** means that the telephone is in the switching state hang up. This state consists if the following conditions are fulfilled:

a) The telephone is hanged up or will be hanged off and then the key will be pressed.

b) The hands free mode isn't active.

c) The headset mode isn't active.

3.1.1 Adjusting the Volume

You can adjust the volume while establishing connections as well as during calls. The volume remains on this level after the call. The "Vol." indicator shows the current value (see Figure 31).

You can increase the volume level by pressing the key ⊙.

You can reduce the volume level by pressing the key ⊙.

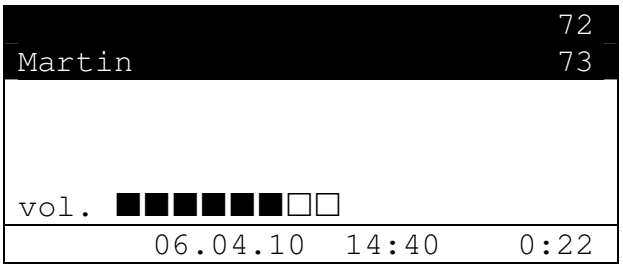


Figure 31: Adjusting the Volume

You control the volume of the active mode.

- At the handset mode you control the volume of the speaker of the handset.
- At the listening mode you control the volume of the additional connected speaker of the phone.
- At the hands free mode you control the volume of the speaker in hands free mode.
- At the headset mode you control the volume of the speaker of the headset.

3.1.2 Adjusting the Ring Tone Volume

You can adjust the ringer volume while incoming calls concerning to the actual call type (internal, external). The ringer volume remains on this level after the call. The "Vol." indicator shows the current value (see Figure 32).

You can increase the ringer volume level by pressing the key ⊙.

You can reduce the ringer volume level by pressing the key ⊙.

```
Torsten                    72
Martin
 73


vol. ■■■■■■□□
        06.04.10  14:40    0:22
```

Figure 32: Adjusting the Ringer Volume

3.1.3 Do not Disturb

You can turn off the do not disturb function of the VoIP telephone simply by pressing a key, for example if you do not wish to be disturbed during a meeting.

1. To activate the do not disturb function; press the key ⊛ for about a second whilst in idle mode until the display appears in Figure 33. The telephone reacts to an incoming call depending on how this feature is configured at the time. For further details on how to configure the do not disturb feature, see chapter 3.8.3 on page 121.

2. To deactivate the do not disturb function again; press the key ⊛ again for about a second until the signalling in the display is deleted. Afterwards the telephone will respond to calls in the usual way again.

```
Torsten                    72

        06.01.10  14:40
```

Figure 33: Do not Disturb

3.1.4 Different Types of Call Numbers

In addition to normal call numbers, your IP telephone can also dial H.323 names and IP addresses.

Call numbers consisting of characters other than the digits 0 to 9 and the characters * and # are considered to be H.323 names. Call numbers beginning with the character @ are always regarded as H.323 names. The character @ is removed before dialling however.

3.1.5 Input of Characters and Special Characters

You can enter any Western European characters in accordance with ISO 8859-1 using the keypad. The assignment of the characters and special characters to the keys can be seen in Table 15.

The letter mode is activated by pressing the respective key pad for an extended moment of time. Subsequently, it is possible to switch between the letters by pressing the key several times in short intervals or by keeping the key pressed.

key	possible characters and special characters
1	1 + ( ) , - & @ # " * ! $ % . / : ; < = > ? ' [ ] \ ^ _ `{ | } ~ £ § ¿ ÷
2	2 a b c A B C ä à á â ã å æ ç Ä À Â Ã Á Å Æ Ç
3	3 d e f D E F è é ê ë È É Ê Ë
4	4 g h i G H I ì í î ï Ì Í Î Ï
5	5 j k l J K L
6	6 m n o M N O ö ñ ò ó ô õ ø Ñ Ò Ó Ô Õ
7	7 p q r s P Q R S ß
8	8 t u v T U V ü ù ú û Ü Ù Ú Û
9	9 w x y z W X Y Z ý Ý ÿ
0	0 (space character)
*	*
#	#

Table 15: Input of Characters and Special Characters

3.2 Operating Modes

The phone allows making calls in different operating modes.

1. Handset mode

   At handset mode the call will be operated with the handset.

2. Handset mode with open listening

   At handset mode with open listening the call will be operated with the handset. The hands free speaker of the phone will be connected additionally. Persons present in the room can listen to the call.

3. Hands free mode

   At hands free mode the call will be operated with the hands free microphone and hands free speaker of the phone. All persons present in the room can take part to the call.

If a headset is connected and configured:

4. Headset mode

   At headset mode the call will be operated with the headset.

5. Headset mode with open listening

   At headset mode with open listening the call will be operated with the headset. The hands free speaker of the phone will be connected additionally. Persons present in the room can listen to the call.

The already active operating mode will be displayed in the state line of the phone.

3.2.1 Changeover from Handset Mode to Handset Mode with Open Listening

To change from handset mode to handset mode with open listening, you have to press the loudspeaker key during a call.

3.2.2 Changeover from Handset Mode with Open Listening to Handset Mode

To change from handset mode with open listening to handset mode, you have to press the loudspeaker key during a call.

3.2.3 Changeover from Handset Mode (with or without Open Listening) to Hands Free Mode

To change from handset mode (with or without open listening) to hands free mode, you have to press the loudspeaker key and hang up the handset with pressed loudspeaker key. Afterwards the loudspeaker key can be released.

3.2.4 Changeover from Handset Mode (with or without Open Listening) to Headset Mode

To change from handset mode (with or without open listening) to headset mode, you have to press the headset key (Key long (longer than a second) and then the loudspeaker key). Afterwards the handset can be hanged up.

3.2.5 Changeover from Hands Free Mode to Handset Mode

To change from hands free mode to handset mode, you have to lift off the handset.

3.2.6 Changeover from Hands Free Mode to Headset Mode

To change from hands free mode to headset mode, you have to press the headset key (Key long (longer than a second) and then the loudspeaker key).

3.2.7 Changeover from Headset Mode to Headset Mode with Open Listening

To change from headset mode to headset mode with open listening, you have to press the loudspeaker key during a call.

3.2.8 Changeover from Headset Mode with Open Listening to Headset Mode

To change from headset mode with open listening to headset mode, you have to press the loudspeaker key during a call.

3.2.9 Changeover from Headset Mode (with or without Open Listening) to Handset Mode

To change from headset mode (with or without open listening) to handset mode, you have to lift off the handset.

3.2.10 Other Changeover of the Operating Mode

Other changes of the operating mode can't take place directly. They are only possible with one of the above listed intermediate steps indirect.

3.3 Call Functions

3.3.1 Answering Calls

You receive a call and your phone rings. The name or phone number of the caller is displayed. The name or phone number of the person for whom the call is intended is also displayed. This is particularly useful in the event of multiple registrations on your telephone in order to identify the actual caller when a call is diverted to your telephone.

```
Torsten                    72
Martin
 73


        06.01.10  14:40    0:22
```

Figure 34: Answering a Call

Answering or rejecting calls:

If you would like to answer the call, you have different possibilities:

- Lift the handset.
- Press the loudspeaker key.
- Press the headset key (Key long (longer than a second) and then the loudspeaker key).

You will be connected to the caller.

To reject the call, press the key. The phone returns to the idle state and the caller will hear an engaged tone.

3.3.2 Terminating a Call

To finish a call respectively to the active operating mode:

- Put the handset back on its rest
- Press the key.
- Press the loudspeaker key.
- Press the headset key (Key long (longer than a second) and then the loudspeaker key).

3.3.3 Making Calls

To call someone, you can use single (if supported by the PBX) or block dialling.

3.3.3.1 Single Dialling

For single dialling take the following steps:

```
Torsten                    72
0211654321



Please dial
       06.01.10  14:40    0:00
```

Figure 35: Direct Dialling

1. Respectively to the wanted calling mode:
   - Pick up the handset (handset mode).
   - Press the loudspeaker key (hands free mode).
   - Press the headset key (Key long (longer than a second) and then the loudspeaker key) (headset mode).
2. Enter the phone number. In this case the VoIP telephone dials the number while it is being entered.
3. To finish a call respectively to the active operating mode:
   - Put the handset back on its rest (handset mode).
   - Press the key (All modes).
   - Press the loudspeaker key (hands free mode).
   - Press the headset key (Key long (longer than a second) and then the loudspeaker key) (headset mode).

3.3.3.2 Block Dialling

For block dialling do the following steps:

1. Let the handset on its rest and don't activate the hands free or headset mode.
2. Enter the phone number completely.

3. When entering the telephone number, you may edit already entered digits. Use the ⊳ and ⊲ keys to move the cursor, and the key Ⓒ to delete the digit to the left of the cursor.

4. Respectively to the wanted calling mode, you can setup the call as follows. In this matter, it will be dialled after one of the following activities.

   a. Lift off the handset (handset mode).

   b. Press the loudspeaker key ◁ (hands free mode).

   c. Press the headset key (Key # long (longer than a second) and then the loudspeaker key ◁) (headset mode).

   d. Press the key ⊳ or key Ⓡ (short or long). With a configured headset you will reach the headset mode otherwise the hands free mode.

   e. Using the key Ⓡ (short or long) executes the selection immediately. Using the key ⊳, however, executes the selection only if the cursor is situated to the right of the last entered digit.

5. When using block dialling, you may enter further properties of the selection. Do so by pressing the ⊖ key. See chapter 3.3.3.2.1 on page 84.

3.3.3.2.1 Menu Parameter Input Indirect Dialling

The following is displayed:

```
Send Message...................
Dial - Show own No............
Dial - Hide own No............
Dial - No Diversion...........
Dial as User..................
Dial to - Always..............
≪ Indirect dialling
```

Figure 36: Menu Parameter Input Indirect Dialling (1. Part)

```
Dial to - Busy................
Dial to - No reply............

≪ Indirect dialling
```

Figure 37: Menu Parameter Input Indirect Dialling (2. Part)

- If you use the cursor keys to select the menu item Send Message and then press the key ⊙ or the repeat dialling key (key ® (long)), the menu message appears (refer chapter 3.7.1 on page 115). It is now possible to send a message to the already entered number.

- If you use the cursor keys to select the menu item Dial – Show own No. and then press the key ⊙ or the repeat dialling key (key ® (long)), the entered number will be dialled and at the called telephone the number of the caller will be displayed.

- If you use the cursor keys to select the menu item Dial – Hide own No. and then press the key ⊙ or the repeat dialling key (key ® (long)), the entered number will be dialled and at the called telephone the number of the caller will be suppressed.

- If you use the cursor keys to select the menu item Dial – No Diversion and then press the key ⊙ or the repeat dialling key (key ® (long)), the entered number will be dialled and an activated call diversion will not be executed, if the PBX supports this feature.

- If you use the cursor keys to select the menu item Call as User and then press the key ⊙ or the repeat dialling key (key ® (long)), the menu User List appears (refer to chapter 3.10 on page 130). Now the User can be changed prior to dialling. The change affects the current call only. This item is only available, if more than one user is configured and enabled.

- If you use the cursor keys to select the menu item Dial to – Always and then press the key ⊙, then the call diversion (refer to chapter 3.8.1 on page 119). The already entered number will be passed into the field call diversion always and the call diversion variant must only be stored for activation. This menu item is available only, if the protocol H.323 or the protocol option local call forward (refer chapter 4.11.9 on page 360) is configured.

- If you use the cursor keys to select the menu item Dial to – Busy and then press the key ⊙, then the call diversion (refer to chapter 3.8.1 on page 119). The already entered number will be passed into the field call diversion busy and the call diversion variant must only be stored for activation. This menu item is available only, if the protocol H.323 or the protocol option local call forward (refer chapter 4.11.9 on page 360) is configured.

- If you use the cursor keys to select the menu item Dial to – No reply and then press the key ⊙, then the call diversion (refer to chapter 3.8.1 on page 119). The already entered number will be passed into the field call diversion no reply and the call diversion variant must only be stored for activation. This menu item is available only, if the protocol H.323 or the protocol option local call forward (refer chapter 4.11.9 on page 360) is configured.

3.3.3.3 Dialling during existing Connections

During existing connections all entered digits (0 – 9, *, #) are transmitted as DTMF signals. Using this DTMF procedure it is possible to access menu-controlled services (e. g. answering machines, voice boxes) directly via the telephone keypad.

3.3.4 Redialling

Up to 100 of the last numbers dialled are saved automatically, together with the time and date, and can be dialled again.

```
01 06.02.10 11:30
Martin 73
02 06.02.10 11:30
Thomas 70
03 06.03.10 11:29
Peter 36
< Calls (outbound)
```

Figure 38: List of Recently Dialled Numbers and Sent Messages

Dialling numbers from the redial list

1. In the initial condition, press the key ® (long). The list of numbers dialled last is displayed (see Figure 38).

   - Success (connected/not connected).
     The symbol on the display indicates that there has been a successful call. A not connected call will be displayed without a symbol.

   - The symbol on the display indicates that there has been a redirected call.

   - The symbol on the display indicates that there has been a transferred call.

   - The symbol on the display indicates that there has been a dialled number on a locked telephone.

   - The symbol on the display indicates that there has been an automatic call back.

- The symbol ✉ on the display indicates that there has been a message sent.

2. Use the arrow keys to select the desired entry.

3. Respectively to the wanted calling mode, you can setup the call as follows:

   a. Lift off the handset (handset mode).

   b. Press the loudspeaker key (hands free mode).

   c. Press the headset key (Key long (longer than a second) and then the loudspeaker key) (headset mode).

   d. Press key ® (short or long) or the key . With a configured headset you will reach the headset mode otherwise the hands free mode.

3.3.5 Call Back

Up to 100 of the last incoming calls are saved automatically, together with the time and date, and can be called back, if the number of the caller was transmitted.

```
01 06.02.10 11:30
Martin 73
02 06.02.10 11:30
Thomas 70
03 06.03.10 11:29
Peter 36
> Calls (inbound)
```

Figure 39: List of the Last Incoming Calls and Received Messages

Dialling numbers from the calling list

1. In the initial condition, press the key ® (short). The list of the last incoming calls is displayed (see Figure 39).

   - Success (connected/not connected).
     The symbol on the display indicates that there has been a call. A not connected call will be displayed without a symbol.

   - The symbol on the display indicates that there has been a redirected call.

   - The symbol on the display indicates that there has been a transferred call.

   - The symbol on the display indicates that there has been a dialled number on a locked telephone.

- The symbol on the display indicates that there has been an automatic call.
- The symbol on the display indicates that there has been a message received.

2. Use the arrow keys to select the desired entry.

3. Respectively to the wanted calling mode, you can setup the call as follows:

   a. Lift off the handset (handset mode).

   b. Press the loudspeaker key (hands free mode).

   c. Press the headset key (Key long (longer than a second) and then the loudspeaker key) (headset mode).

   d. Press key (short or long) or the key . With a configured headset you will reach the headset mode otherwise the hands free mode.

3.3.6 Muting

You can mute the microphone during a call to make a confidential enquiry in the room without being heard on the phone.

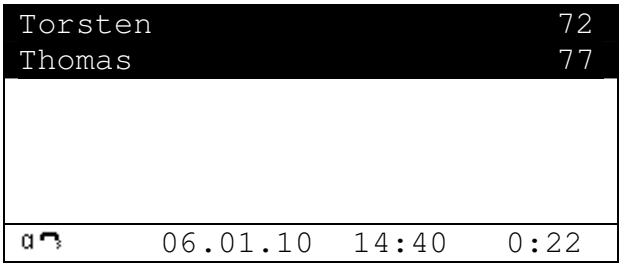


Figure 40: Muting

1. Press the key during a call for more than a second. The microphone symbol "" flashes (see Figure 40). The microphone is switched off. You can now make a room enquiry.

2. Press the Mute key during a call for more than a second again. The flashing microphone symbol disappears and the microphone is switched on again.

3.3.7 Making second Call

The line can be put on hold during a call. With the call on hold, you can make a second call to someone else. The person on hold can't hear the second call. The hold function is also needed to switch or transfer a call.

```
Torsten                    72
Peter                      36
Torsten                    72

Please dial
     06.01.10  14:40    0:22
```

Figure 41: Holding a Call

1. Press the key Ⓡ (short) during a call. The call is put on hold. You hear a dial tone. The line on hold is displayed normally, the active line inversely (see Figure 41).

2. Dial the call number. A further connection is established.

3. To terminate the enquiry call, press the key ⊖. You return to the conversation partner previously put on hold.

Tip

The call with the conversation partner highlighted on the display (active) is terminated by pressing the key ⊖. If you alternatively want to terminate a call with another conversation partner, first select the respective conversation partner whose connection you want to disconnect using the arrow keys and only then press the key ⊖.

3.3.8 Switching

You can switch between two connections using the switch function.

```
Torsten                    72
Peter                      36
Torsten                    72
Thomas                     70

      06.01.10  14:40    0:22
```

Figure 42: Switching

1. Press the key Ⓡ (short) two times or the key Ⓡ (short) followed by the key ② during a call with an active line and a line on hold. The active line is put on hold and the line on hold is activated (see Figure 42).

2. To terminate the active line, you must press the key ⊖. The connection to the active conversation partner is terminated.

Please note also the tip in chapter 3.3.7 "Making second Call" beginning on page 89.

3.3.9 Transferring a Call

You are making a call and would like to transfer it to another party.

```
Torsten                    72
Peter                      36
Torsten                    72
Thomas                     70

      06.01.10  14:40    0:22
```

Figure 43: Transferring a Call

1. Press the key Ⓡ (short) during a call.
   The call is put on hold. You hear a dial tone. The line on hold is displayed normally and the active line inversely.

2. Dial the call number of your choice.
   The connection is established. If the called party answers, this can be treated like a second call, as above.

3. To connect the caller will be connected with the dialled number you have the following possibilities:

a. Put the handset back on its rest (handset mode).

b. Press the loudspeaker key (hands free mode).

c. Press the headset key (Key long (longer than a second) and then the loudspeaker key) (headset mode).

d. Press the key (short) followed by the key . The caller will be connected with the dialled number.

Tip

When transferring a call, you do not have to wait until the desired subscriber answers. You can hang up immediately after dialling the phone number.

3.3.10 Transferring a Call directly

You are making a call and want to switch it to another connection.

```
Torsten                    72
Peter                      36

  Transfer                  1
```

Figure 44: Transferring a Call Directly

1. Press the key (long) during a call.
2. You will be left. The actual connection will not be displayed.
3. Dial the call number of your choice.
4. Press the key (short) or key .
5. The caller will be connected with the dialled port directly.
6. With handset mode hang up.

3.3.11 Initiating a Conference

You can use this function to set up a conference between two lines. To do so, you need an active line and a line on hold (refer to chapter 3.3.7 "Making second Call" beginning on page 89).

```
Torsten                    72
anonym
Torsten                    72
Peter                      36

3party
      06.01.10  14:40    0:22
```

Figure 45: Conference

1. Press the key ⊖ or the key Ⓡ (short) followed by the key ③ during a call with an active line and a line on hold.
   A conference is set up between the active line and the line on hold. All the subscribers can now talk with each other (see Figure 45).

2. You can end the conference by pressing the key ⊖ respective the key Ⓡ (short) followed by the key ③ or twice the key Ⓡ (short). If you end the conference with pressing the key ⊖ or the key Ⓡ (short) followed by the key ③, the call put on hold prior to the initiated conference is now on hold again and the previously active call is active once again. If you end the conference with pressing the key Ⓡ (short) twice, the call put on hold prior to the initiated conference is now active and the previously active call is now on hold.

3. To terminate the active line, you must press the key ⊖. The connection to the active conversation partner is terminated. Please note also the tip in chapter 3.3.7.

Note

If you

- hang up (handset mode)
- press the loudspeaker key (hands free mode)
- press the headset key (Key long (longer than a second) and then the loudspeaker key) (headset mode)

during the conference, the lines of both parties keep connected.

3.3.12 Return Call if engaged

An automatic return call can be initiated, if the line of the called party is engaged or not hanging up.

The telephone indicates that the line is free as soon as the called party has terminated the call.

If the person you are calling does not pick up the receiver because he or she is busy with another call, and this call is terminated, the telephone signals that the connection of the person you want to talk to is now available.

The call is initiated and the opposite telephone rings as soon as you pick up the handset of the telephone. The telephone network of the call partner must support this feature.

```
Peter

Recall
Redial
Intrude
Send Message
< Recall
```

Figure 46: Recall

1. If you hear the busy tone or the dial tone (free line signal), press the key. A menu appears in the display. Using the cursor keys, select the item Recall and press the key to activate the automatic return call. Replace the receiver and wait for the return call signal.

2. When return call is signalled, the return call can be initiated as follows:

   a) Pick up the handset (handset mode).

   b) Press the loudspeaker key (hands free mode).

   c) Press the headset key (Key long (longer than a second) and then the loudspeaker key) (headset mode).

   d) or press the Loudspeaker key to initiate the return call.

   The call with the opposite party is set up.

   or

   Press the key , to prevent the return call from being set up.

Note

The function **Return Call if engaged** is only possible within a PBX that supports this feature and the protocol is set to H.323.

If the **Do not Disturb** feature is also active on the telephone, the return call is not signalled acoustically or not signalled at all, depending on the settings.

If the **Call Diversion** is active, the active Do Not Disturb feature is not indicated in the display, due to the indicated call diversion target.

3.3.13 Automatic Redialling

If no-one answers your call, or you hear the busy tone, you may activate the automatic redialling.

If the telephone you called is busy again, the telephone indicates the possibility of redialling, and the telephone rings.

```
Peter

Recall
Redial
Intrude
Send Message
< Recall
```

Figure 47: Redial

1. Press the key ⊖ if the busy tone or the distant dial tone can be heard. Using the cursor keys, select the item Redial and press the ⊙ key to activate automatic redialling. Replace the receiver and wait for the return call signal.

2. The telephone attempts to call the opposite party every thirty seconds, which is indicated by an outgoing call signal. As soon as the opposite party has been reached by the automatic return call option, the call is activated. Redialling is restricted to 20 minutes.

3. If you want to delete the automatic redial function, press the key ⊖ while you can hear the outgoing call signal.

☞	**Note** A new call deletes the current automatic redial function.	☜

3.3.14 Intrusion

If the called dialogue partner is busy, an intrusion to the active call can be done, if the feature is enabled for the phone.

```
Peter

Recall
Redial
Intrude
Send Message
< Recall
```

Figure 48: Intrude

1. Press the key ⊖

2. If the busy tone can be heard, then press the key menu ⊖. Using the cursor keys, select the item Intrude and press the key ⊙.

3.3.15 Send Message

If no-one answers your call, or you hear the busy tone, you may send a message.

1. Press the key ⊖ if the busy tone or the distant dial tone can be heard. Using the cursor keys, select the item Send Message and press the key ⊙.

```
Peter

Recall
Redial
Intrude
Send Message
< Recall
```

Figure 49: Send Message

```
For:72

<< Message                a
```

Figure 50: Message

2. The message can be entered with the keypad alphanumerical. The message will be sent by pressing the key ⊖. The sending of the message can be aborted by pressing the key ⊖.

3.3.16 Management of the Waiting List

Your VoIP telephones are perfectly suited to be used as a small exchange. You are able to hold more than two calls at a time. The number of maximum serviceable calls can be freely configured. Contact your PBX administrator to find out more about your settings.

The waiting list can be operated in two operating modes.

3.3.16.1 Operating Mode 1

To access this operating mode, press the ⊙ key.

In this operating mode two calls from your waiting list are displayed.

```
Anna-Maria                    77
Torsten                       72
Anna-Maria                    77
Thomas                        70
   1 Call pending
Martin                        73
     06.01.10  14:40     0:22
```

----- hold call

----- active call

----- waiting calls

-- choosen waiting call

Figure 51: Operating Mode 1

This operating mode allows you to switch between the active and the waiting calls.

When handling the calls, you have the following options:

Key sequence	Effect
▲	Press the key ▲ repeatedly to switch between the active and the „selected waiting" call.
R (short) R(long)	If your waiting list contains more than 3 calls, you may use this key sequence (pressing one key after another) to randomly replace the „selected waiting" call by one of the remaining waiting calls.

3.3.16.2 Operating Mode 2

To access this operating mode, press the ▼ key.

This operating mode allows you to switch between the active and the selected waiting call.

In this operating mode one call from the waiting list is displayed.

```
Anna-Maria                    77
Torsten                       72

   2 Calls pending
Thomas                 70
     06.01.10  14:40     0:22
```

-- active call

-- choosen waiting call

Figure 52: Operating Mode 2

Caution

The call previously held from operating mode 1 ⓐ, in this operating mode 2 ⓥ now becomes the active call. The call previously defined as the active call from operating mode 1 ⓐ, in this operating mode 2 ⓥ now becomes the selected waiting call (see Figure 52).

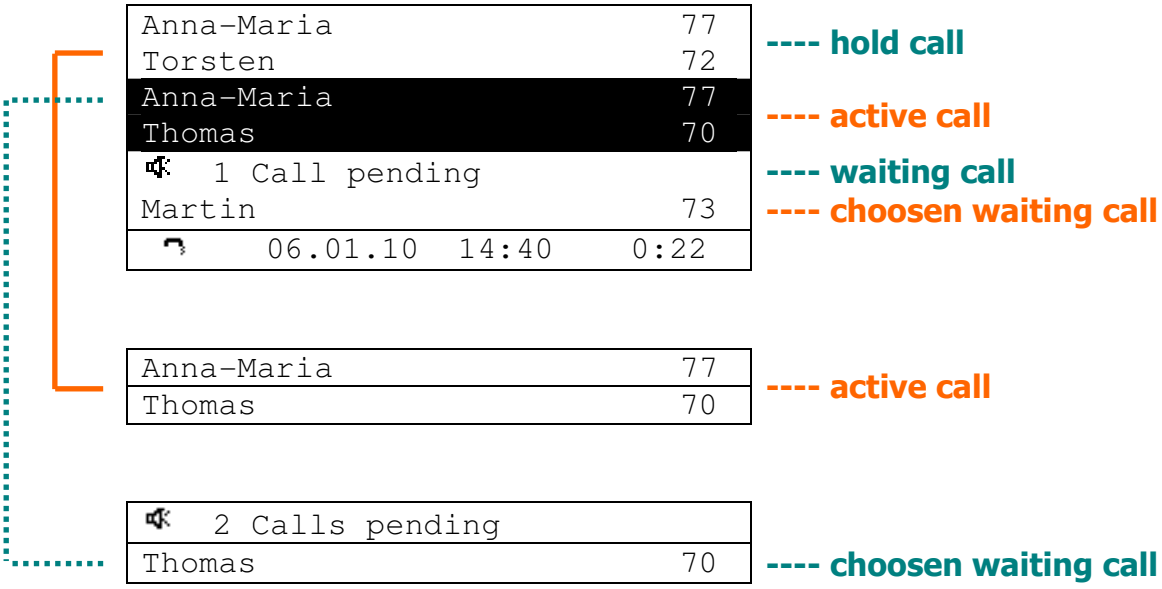


Figure 53: Compare of the Operation Modes

When handling the calls, you have the following options:

Key sequence	Effect
ⓥ	Press the key ⓥ repeatedly to switch between the active and the selected waiting call (see Figure 53). The selected waiting call becomes the active call, and the previously active call becomes the new selected waiting call.
Ⓡ(short) Ⓡ(long)	If your waiting list contains more than 3 calls, you may use this key sequence (pressing one key after another) to replace the „selected waiting" call by one of the remaining waiting calls.

3.3.17 Call Counter

The telephone has a call counter, which indicates the amount of incoming calls during a period of absence.

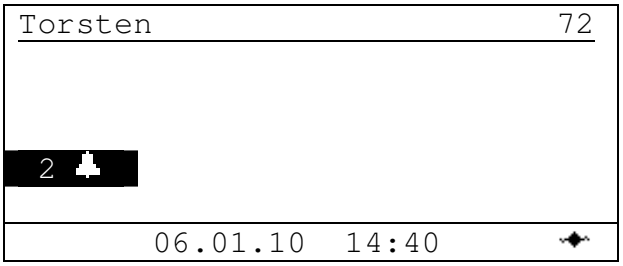


Figure 54: Call Counter

The call counter is deleted automatically if the call list is called up. You can call up the call list by pressing the key ® (short) or by calling from the menu.

3.3.18 Message Counter

The telephone has a message counter, which indicates the amount of incoming messages during a period of absence.

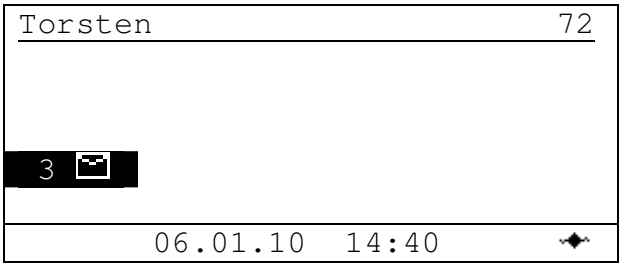


Figure 55: Message Counter

The call counter is deleted automatically if the message list is called up. You can call up the message list by pressing the key ® or by calling from the menu.

3.3.19 Recall Counter

The telephone has a recall counter, which indicates the amount of pending recalls activated during absence.

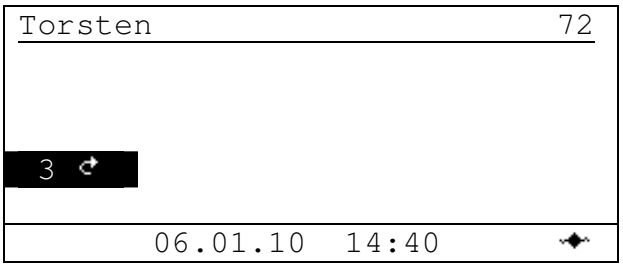


Figure 56: Recall Counter

The recall will be started after one of the following automatic.

1. Lift off the handset and pick it on the rest.

2. Press the loudspeaker key twice.

3. Press the headset key (Key long (longer than a second) and than the loudspeaker key) twice.

3.3.20 Answering Waiting Calls

You receive a call during a conversation. If the telephone is thus configured (refer to chapter 3.7 beginning on page 115) the caller's name or telephone number appears in the display.

The number of the administrated calls is configured in the administration. As long as the configuration limit has not yet been reached, incoming calls will be indicated by a call waiting signal.

The waiting call will not automatically be answered.

Note

When the configurable limit has been reached, further calls will be rejected by means of a busy signal.

The display clearly shows the waiting calls and the "chosen" call in the waiting line.

```
Torsten                    72
Thomas                     77

♣ 1 Call waiting
Martin                     75
 ↶      06.01.10  14:40   0:22
```

Figure 57: Call Waiting

Answering or terminating waiting calls:

If you want to answer the waiting call, press the Ⓐ and Ⓥ keys, or the key Ⓡ (short), followed by the key②. The current call is placed in Enquiry, and you are connected with the caller and may have a conversation.

To reject the call, press the key Ⓡ (short), followed by the key ⓪. The caller hears a busy tone.

☞	**Note** How to manage the waiting list is described in chapter 3.3.14 beginning on page 95.	☞

3.4 Main Menu

Press the key ⊖ respectively ⊙. The following is displayed:

```
Call Lists.....................
Directories....................
Messages.......................
User setup.....................
Phone Setup....................
User List......................
  Main Menu                   ▼
```

Figure 58: Main Menu (1. Part)

Press the key ⊙ six times. The following is displayed:

```
Administration................

  Main Menu                    ▲
```

Figure 59: Main Menu (2. Part)

3.5 Menu Call Lists

All incoming and outgoing calls will be stored in a call list.

1. In the initial condition, press the key ⊖ or ⊙.

2. With the Arrow keys, select the menu **Call Lists**.

3. Press the key ⊙. The following is displayed:

```
Calls (combined)..............
Calls (inbound)...............
Calls (outbound)..............
Active Recalls................

< Call Lists
```

Figure 60: Menu Call Lists

It is possible to dial the call number again directly via the **calls (combined)**, **calls (inbound)** and **calls (outbound)** menus. Refer to chapter 3.3.4, "Redialling", beginning on page 86 and chapter 3.5.2, "Call List (inbound)", beginning on page 104 for the procedure.

3.5.1 Calls (combined)

This function shows a combined call list with incoming and outgoing calls.

1. In the initial condition, press the key ⊖ or ⊙. The display appears in Figure 58.

2. With the Arrow keys, select the menu **Call Lists**.

3. Press the key ⊙. The display appears in Figure 60.

4. Press the key ⊙.

The following is displayed if entries are available:

```
>01 23.01.10 11:20
Peter 36
>02 23.01.10 11:20
Peter 36
<03 23.01.10 11:20
Peter 36
≪ Calls (combined)
```

Figure 61: Menu Calls combined

The combined call list contains the following information:

- Type of call (incoming/outgoing).
  Incoming calls are indicated with ">" and outgoing calls with "<".
- Consecutive numbering of the entries, beginning with 01 for the last entry.
- Date and time of the calls.
- Success (connected/not connected).
  The symbol on the display indicates that there has been a call.
- The symbol on the display indicates that there has been a redirected call.
- The symbol on the display indicates that there has been a transferred call.
- The symbol on the display indicates that there has been a dialled number on a locked telephone.
- The symbol on the display indicates that there has been an automatic call.
- Name of the caller / conversation partner (if entered in the directory) and call number of the caller / conversation partner (if transmitted). The initial number of the caller is transmitted, and not that of the diverted telephone, if the call is an incoming call from a diverted call number.

Using the cursor keys you may now select an entry. Pressing the key ® (long) now, dials the displayed number. If you press the ⊙ key, the menu Call List edit appears (refer to chapter 3.5.5 beginning on page 106).

3.5.2 Call List (inbound)

You may access this function using **Menu > Call Lists > Calls (inbound)**.

The following is displayed if entries are available:

```
01 23.01.10 11:20
Peter 36
02 06.01.10 14:40
Peter 36
03 23.01.10 11:20
Peter 36
≪ Calls (inbound)
```

Figure 62: Menu Call List inbound

The **Call List (inbound)** contains, among others, the following information:

- Consecutive numbering of the entries, beginning with 01 for the last incoming call.
- Date and time of the calls.
- Success (connected/not connected).
  The symbol on the display indicates that there has been a call.
- The symbol on the display indicates that there has been a redirected call.
- The symbol on the display indicates that there has been a transferred call.
- The symbol on the display indicates that there has been a dialled number on a locked telephone.
- The symbol on the display indicates that there has been an automatic call.
- Name of the caller (if entered in the telephone directory) and call number of the caller (if transmitted).

Using the cursor keys you may now select an entry. Pressing the key ® (long) now, dials the displayed number. If you press the ⊙ key, the menu Call list edit appears (refer to chapter 3.5.5 on page 106).

3.5.3 Call List (outbound)

You can call up this function via the **Menu > Call Lists > Calls (outbound)** call-up.

The following is displayed if entries are available:

```
01 23.01.10 11:20
Peter 36
02 23.01.10 11:20
Peter 36
03 23.01.10 11:20
Peter 36
≪ Calls (outbound)
```

Figure 63: Menu Call List outbound

You can find further information in chapter 3.3.4 "Redialling" beginning on page 86.

The **Call List (outbound)** contains, among others, the following information:

- Consecutive numbering of the entries, beginning with 01 for the call number dialled last.
- Date and time of the calls.
- Success (connected/not connected).
  The symbol on the display indicates that there has been a call.
- The symbol on the display indicates that there has been a redirected call.
- The symbol on the display indicates that there has been a transferred call.
- The symbol on the display indicates that there has been a dialled number on a locked telephone.
- The symbol on the display indicates that there has been an automatic call.
- Name of the conversation partner (if entered in the directory) and dialled call number.

Using the cursor keys you may now select an entry. Pressing the key Ⓡ (long) now, dials the displayed number. If you press the ⊙ key, the menu Call list edit appears (refer to chapter 3.5.5 on page 106).

3.5.4 Active Recalls

This function shows all active recalls.

You can call up this function via the **Menu > Call Lists > Active Recalls** call-up.

The following is displayed if entries are available:

```
01 23.01.03 11:20............
Peter 36
01 23.01.03 11:20............
Klaus 37
01 23.01.03 11:20............
Inge 39
≪ Active Recalls
```

Figure 64: Menu Call Lists Active Recalls

3.5.5 Call List Edit

```
Information..................
Save no. in Directory........
Indirect dialling............
Delete Entry................
Delete List.................

≪≪ Edit List
```

Figure 65: Menu Call List Edit

- If you use the cursor keys to select an item (incoming or outgoing call, but no automatic recall) and then press the key ⊙, the menu Call List Edit appears.

- If you use the cursor keys to select the menu item Information and then press the key ⊙, the menu Information appears (refer to chapter 3.5.5.1 beginning on page 107).

- If you use the cursor keys to select the menu item Save No. in Directory and then press the ⊙ key, the menu Directory Input appears (refer to chapter 3.6.4 beginning on page 111). Here the entry may be edited and used in the telephone book.

- If you use the cursor keys to select the menu item Indirect dialling and then press the ⊙ key, the telephone enters the Indirect dialling state. The display now shows only those telephone numbers that may be completed, changed or dialled (refer to chapter 3.3.3 beginning on page 82).

- If you use the cursor keys to select the menu item Delete Entry and then press the ⊙ key, the call list entry will be deleted.

- If you use the cursor keys to select the menu item Delete List and then press the ⊙ key, the complete Call List that was used to access this list entry, will be deleted.

3.5.5.1 Information (Call)

This menu shows details of the selected call.

1. Who called: name, telephone number.

2. Who was called up: name, telephone number.

3. Duration of the call: h:mm:ss (hours:minutes:seconds).

```
From:Meier 105
For:Schulze 106
Duration:0:23:45

<<< Information
```

Figure 66: Menu Information (Call)

3.5.5.2 Information (transferred Call)

This menu shows details of the selected redirected, switched or transferred call.

1. Who called: name, telephone number.

2. Who was called up: name, telephone number.

3. Who has redirected, switched or transferred: name, telephone number.

4. Duration of the call: h:mm:ss (hours:minutes:seconds).

```
From:Meier 105
For:Schulze 106
Via: Müller 107
Duration:0:23:45

⋘ Information
```

Figure 67: Menu Information (transferred Call)

3.6 Menu Directories

The telephone directory is your personal phone book in which the names and call numbers of your conversation partners are administered.

1. In the initial condition, press the key ⊖ or ⊙.

2. With the Arrow keys, select the menu **Directories**.

3. Press the key ⊙. The following will be displayed:

```
Directory Input...............
Search (local)................
Search (external)............
Search (PBX)..................
Search (combined)............

≪ Directories
```

Figure 68: Menu Directories

Depending on the configuration, it may be possible to access the directory of the telephone system (PBX) or of an external LDAP server.

Entries in the local telephone directory consist of the name (= search term), the call number and, if desired, further settings and notes.

The number of possible entries depends on the available storage space of the telephone. Up to 2000 entries can be managed. All entries are sorted alphabetically. The entire telephone directory can be saved on a PC and reloaded for further processing and in order to additionally back up the data. You can also import external address books from the PC.

To do so, please refer to your administrator.

3.6.1 Saving new Entries

Proceed as follows to create new telephone book entries:

1. In the initial condition, press the key ⊖ or ⊙.
2. With the Arrow keys, select the menu **Directories**.
3. Press the key ⊙. The display appears in Figure 68.
4. With the Arrow keys, select the menu **Directory Input**.
5. Press the key ⊙. The following will be displayed:

```
Subscriber

Number:
Name  :
Setup.......................

≪ Directory Input
```

Figure 69: Menu Directory Input

The input fields are displayed. The cursor in the field stands for the name of the subscriber.

6. In the field **Subscriber:** enter the name (max. 40 characters).
   The subscriber name is used as search reference in the local telephone directory and can be freely selected.
7. With the Arrow keys, select the input field **Number:**
8. Enter the call number.
9. With the Arrow keys, select the input field **Name:**
10. Enter the name.

Either the call number **or** the name must be entered. The call number is determined automatically by entering the name.

11. Enter the setup.
12. Press the key ⊖.

The message "Entry saved" appears and the display changes to Figure 68.

3.6.2 Searching for Entries

The directory is opened automatically by entering a letter. The entries of the subscribers beginning with the entered letters are displayed. If you enter * all entries are displayed.

1. Enter the first letter of the entry you are looking for. The entries beginning with these letters or all entries if you entered * appear on the display (see Figure 70).

2. Use the arrow keys to select the desired entry.

3. You can call this contact as usual by pressing the key Ⓡ (long) respectively ➤.

4. After pressing the key ⊖ you enter the menu parameter input indirect dialling (refer to chapter 3.3.3.2.1 beginning on page 84).

```
Böhme, Claus..................
Cezanne, Heinz................
Loch, Wolfgang................
Römer, Bernhard...............

*
  Indirect dialling
```

Figure 70: Indirect Dialling Display of the Directory

Tip

The key ⊖ leads to the current entry in a context menu. You can start dialling from this menu (with phone number suppression or with another user if desired).

3.6.3 Searching for Entries selectively

The search can also be carried out selectively in the **Menu > Directories**:

Search (local) only searches in the telephone directory of the phone.

Search (external) searches on an external LDAP server.

Search (PBX) searches in the telephone directory of the telephone system (PBX).

Search (combined) searches in all available directories.

```
≪ Search (local)
```

Figure 71: Search

1. Enter the initial letter of the entry you search for. The entries beginning with the entered letter, or all entries, if you have entered *, appears in the display (see Figure 71).

2. Use the arrow keys to select the desired entry.

3. Press the ⊖ key. You reach the menu Parameter Input Indirect Dialling (refer to chapter 3.3.3.2.1 beginning on page 84). Here, you may enter further parameters and dial.

3.6.4 Editing Entries

You can check, correct, supplement or delete your local entries at any time.

Editing the call number and name

1. Search for the desired entry as described in chapter 3.6.2 Searching for Entries beginning on page 110.

2. Press the key ⊙, key in order to edit the entry. The following is now displayed (the entry "Madonna" for example):

```
Subscriber
Madonna
Number:125
Name  :Madonna
Setup.........................
Delete........................
≪≪ Directory Input
```

Figure 72: Menu Directory Input

The input fields are displayed. The cursor in the field stands for the name of the subscriber.

3. If required, correct the **Subscriber** entry. This entry is relevant for the telephone book.

4. With the arrow keys, select the input field **Number** and correct the entry, if required.

5. With the arrow keys, select the input field **Name** and correct the entry, if required. This Entry is used for dialling.

6. In order to save your changes, press the key ⊖.

The entry saved message appears and the alphabetical telephone directory list is re-opened.

7. In order to delete an entry, use the arrow keys to select the menu **Delete** and press the key ⊙.

You are asked whether the entry is to be deleted.

8. In order to confirm the deletion, use the arrow keys to select the entry **Yes** and press ⊙.

The entry deleted message appears and the alphabetical telephone directory list is re-opened.

9. In order to abort the deletion, use the arrow keys to select the entry **No** and press ⊙.

You are returned to the subscriber data.

3.6.4.1 Setup

Proceed as follows to adjust the settings:

1. In the Directory Input, use the cursor keys to select the **Setup** menu.

2. Press the key ⊙. The following will be display:

```
Ringing                    On
Ringing Tone..................
Registration..................

≪ Setup
```

Figure 73: Menu Setup

3. Set the ringing tone

4. Set the registration

5. Press the key ⊖.

The message "Entry saved" appears and the display changes into the state of Figure 69.

3.6.4.1.1 Ringing Tone

Proceed as follows to set the ringing tone:

1. With the arrow keys, select the menu **Ringing Tone**.

2. Press the key ⊙. The following will be display:

```
Start.........................
Melody:                 Default
Vol:                        Def
Spd:                        Def


⋘ Ring Melody
```

Figure 74: Menu Ring Melody

3. In Ringing Tone, use the cursor keys to select the Start menu item. Press the key ⊙. You hear the set melody with the set volume and speed. The name of the current menu item changes to Stop.

4. If you press the ⊙ key when the Stop menu item is selected, the playback of the current melody is stopped.

5. In Ringing Tone, use the cursor keys to select the Melody menu item. Press the ⊙ or ⊙. key. Another melody is selected.

6. In Ringing Tone, use the cursor keys to select the Vol. menu item. Press the ⊙ or ⊙ key. Another volume is selected.

7. In Ringing Tone, use the cursor keys to select the Spd menu item. Press the ⊙ or ⊙ key. Another speed is selected. This setting option does, however, work with the standard ringing tones (present in the telephone at the time of purchase) only, and not with any subsequently downloaded ringing tones.

8. Press the key ⊖.

The message "Entry saved" appears and the display changes into the state of Figure 73.

3.6.4.1.2 Registration

To setup the registration proceed as follows:

1. With the arrow keys, select the Menu **Registration**.

2. Press the key ⊙. The following will be display:

```
FHF4                    104 +*

<<< Registration
```

Figure 75: Menu Registration

3.6.5 Multiple Registration

Multiple registrations make it possible to register up to 6 different users for one telephone. The display indicates which incoming calls are for which user. The data of the active user is used for outgoing calls. If the call data of another user is to be transmitted, the active user must be put on hold before the call is set up.

This feature enables a variety of options. It is possible, for example, for a co-worker working at several locations to log on to the telephone at different workplaces. Or it is possible to implement the telephone exchange or hotline function by allowing co-workers to log on as joint users of this circuit. It is also possible to stand in temporarily for a colleague (his/her call number) with multiple registrations.

Tip

This feature can only be used if it is possible to register call numbers at several telephones in the PBX component.

Join user setup

The registration of the (up to 6) joint users ensues by editing the menu **Phone/User-1** to **Phone/User-6** on the Web interface of the telephone. Refer to chapter 4.1 General respectively Web-Interface beginning on page 173.

After the joint user data has been entered on the Web-Interface calls for the active user of the telephone as well as for the joint user are signalled.

Changing user

By changing the user, the specific data about the selected user stored in the PBX is activated in the VoIP telephone. This includes, among others, the configuration of the telephone, the function key assignment, the telephone directories etc.

In order to change user, activate the desired user in the User List (Refer to chapter 3.10.1 beginning on page 131).

3.7 Menu Messages

```
New Message....................
Messages(incoming)............
Messages(outgoing)............

< Messages
```

Figure 76: Menu Messages

3.7.1 New Message

```
For:

≪ Message
```

Figure 77: Menu New Message

After ‚For:' you have to enter the calling number of the desired subscriber. After pressing the key ⊙ you reach the next line. Here you can enter the message alphanumerical. With pressing the key ⊖ the message will be sent. If the PBX can't detect an error, then for a short time the display appears in Figure 78. Then the display appears in Figure 2. If the PBX detects an error, then for a short time the display appears in Figure 79. Then the display appears in Figure 77. You can correct the message and try to send it again. With pressing the key ⊖ the input of a new message will be cancelled.

```
OK
```

Figure 78: Ok

```
Operation failed
```

Figure 79: Operation failed

3.7.2 Messages (incoming)

```
>01 06.02.10 11:30
Martin 73
>01 06.02.10 11:22
Peter 72

≪ Messages(incoming)
```

Figure 80: Menu Messages (incoming)

The desired message can be selected with pressing of the keys ⊽ or ⊼ and can be called with pressing of the key ⊳.

3.7.3 Messages (outgoing)

```
<01 06.02.10 11:30
Martin 73
<01 06.02.10 11:22
Peter 72

≪ Messages(outgoing)
```

Figure 81: Menu Messages (outgoing)

The desired message can be selected with pressing of the keys ⊽ or ⊼ and can be called with pressing of the key ⊳.

3.7.4 Message

```
It is raining now.
Action.......................
⋘ Message
```

Figure 82: Menu Message

The message will be displayed. With ‚Action' you can respond to the message.

3.7.5 Action

```
Number:501
Indirect dialling.............
Reply Message.................
Delete Entry..................
Delete List...................
⋘ Action
```

Figure 83: Menu Action

3.7.6 Incoming Message

```
From:501
It is raining now.
< Message
```

Figure 84: Incoming Message

If the phone is in idle state, an incoming message will be displayed for a short time immediately and the phone is ringing shortly.

3.8 Menu User Setup

```
Call Diversion................
Presence......................
Do not Disturb................
Call waiting:          On-def.
Number Present.:            On

< User Setup
```

Figure 85: Menu User Setup

Call Diversion, Presence and Do not Disturb can be set using the sub-menus.

Under call waiting you can set the telephone's response to inbound calls during an active call.

- **Call waiting Off:** An inbound call during an active call is only entered in the Call List. The call is not indicated. The caller hears a busy signal.
- **Call waiting On-def.:** An inbound call during an active call is being indicated. The caller hears a dial tone (free line signal). The waiting call is being indicated in the display of the caller. In the receiver, the caller hears a short acoustic signal.
- **Call waiting On-once:** Contrary to On-def., the caller hears a long acoustic signal in the receiver.
- **Call waiting On-mute:** Contrary to On-def., the caller hears no acoustic signal in the receiver.

The waiting call can be accepted by pressing the key Ⓡ (short) and then the ② key.

The waiting call can be rejected by pressing the key Ⓡ (short) and then the ⓪ key.

Setting Call waiting:

1. While the telephone is in its initial condition, press the key ⊖ or ⊙.

2. Use the cursor keys to select the **User Setup** menu.

3. Press the key ⊙. The screen in Figure 85 appears.

4. Use the cursor keys to select the line **Call waiting**.

5. Press the ⊙ key repeatedly (if necessary) and select the desired Call waiting variety.

6. In order to store the selection, leave the menu by pressing the key ⊖ three times.

The set Call waiting variety has now been activated.

The Number Presentation allows you to enable or disable the display of your own telephone number when making a call.

Setting the Number Presentation:

1. While the telephone is in its initial condition, press the key ⊖ or ⊙.
2. Use the cursor keys to select the **User Setup** menu.
3. Press the key ⊙. The screen in Figure 85 appears.
4. Use the cursor keys to select the **Number Present.** menu.
5. If you press the key ⊙ at this point, you can switch between „On" and „Off".
6. In order to store the selection, leave the menu by pressing the key ⊖ three times.

The current setting is valid for all subsequent calls, unless the setting is enabled or disabled specifically for an individual call.

A deactivated Number Presentation is displayed in the status bar by the symbol .

3.8.1 Call Diversion

The **call diversion** menu allows you to be available even if you are not in the office.

☞

Note

The call diversion is working according to the standard H.450. The gatekeeper must support this protocol.

Otherwise the option local call forward can be activated (see chapter 4.11.9 Protocol Option 'Local Call Forward on page 360).

If the gatekeeper doesn't support this protocol (The telephone is set to the protocol SIP/TSIP/SIPS.) and the local call diversion is not activated, the item "call diversion" doesn't appear in the menu of the VOIP telephone.

☞

Note

If the protocol option local call forward is activated, a call forward is set and the telephone is not reachable in the network, then the feature call forward will not work.

The VoIP telephone supports three different kinds of call diversion:

- **Unconditional**: All calls are immediately diverted to another subscriber.

Note

This diversion state disables the other kinds of diversions.

With this setting calls are diverted immediately. The called party cannot answer the call.

- **Busy:** Calls are diverted when a call is already active.
- **No reply**: Calls are diverted if they are not answered within a certain time limit.

Note

In contrast to the unconditional call diversion you have the possibility to answer the call within a certain time, before the call is diverted.

Note

In the initial condition of the VoIP telephone, an active call diversion is indicated in the status bar by the symbol .

If the call diversion is permanent, the call diversion target is also indicated in the display.

Setup call diversion, switching on and off

1. In the initial condition press the key ⊖ or ⊙.
2. Use the arrow keys to select the menu **User Setup**.
3. Press the key ⊙. The display appears in Figure 76.
4. Use the arrow keys to select the menu **Call Diversion**.
5. Press the key ⊙. The display appears in Figure 86.

```
Unconditional:                Off

Busy:                         Off

No reply:                     Off

≪ Call Diversion
```

Figure 86: Menu Call Diversion

6. Use the arrow keys to select the desired kind of call diversion **Unconditional**, **Busy** respectively. **No reply**.
7. If you press the ⊙ key at this point, you can switch between „on" and „off".
8. Press the cursor keys to go to the line below the desired type of call diversion.
9. Enter the telephone number of the desired call diversion target.
10. In order to store the selection, leave the menu by pressing the ⊖ key three times.

The set call diversion is now active, and if the permanent call diversion is active, this is indicated in the display of the telephone.

3.8.2 Presence

The **Presence** menu allows you to be available to send a caller a message about the reason of not being reachable automatically.

Setup presence, switching on and off

1. In the initial condition press the key ⊖ or ⊙.

2. Use the arrow keys to select the menu **User Setup**.

3. Press the key ⊙. The display appears in Figure 76.

4. Use the arrow keys to select the menu **Presence**.

5. Press the key ⊙. The display appears in Figure 87.

```
Activity:
Note

≪ Presence
```

Figure 87: Menu Presence

6. Use the arrow keys ⊙ or ⊙ to select the desired kind of Activity: Away, Busy, Lunch, Meeting or Vacation. If you select at activity nothing, the feature will be deactivated.

7. Press the key ⊙, you will enter note input area. Now you will be able to enter a message with the key pad alphanumerical.

8. To store the inputs press the key ⊖ two times. If no error will be detected, then for a short time the display ok appears in Figure 78.

3.8.3 Do not Disturb

The **Do not disturb** menu allows you not to be disturbed for a while.

The VoIP telephone supports different versions of Do Not Disturb:

- **Do not disturb Off:** All calls are switched through and acoustically and optically indicated.

- **Do not disturb On**:
    - **Action Ringing off:** An inbound call is indicated in the display and entered in the Call List. The telephone does not ring. The caller hears a dial tone (free line signal). The display indicates that the Do not disturb feature is active.
    - **Action Ring once:** An inbound call is indicated in the display and entered in the Call List. The telephone rings once. The caller hears a dial tone (free line signal). The display indicates that the Do not disturb feature is active.
    - **Action Silence:** An inbound call is not indicated in the display, but merely entered in the Call List. The telephone does not ring. The caller hears a dial tone (free line signal). The display indicates that the Do not disturb feature is active.
    - **Action Busy:** An inbound call is not indicated in the display, but merely entered in the Call List. The telephone does not ring. The caller hears a busy signal. The display indicates that the Do not disturb feature is active.
    - **Action Out of Office:** An inbound call is not indicated in the display, but merely entered in the Call List. The out of office message is sent to the caller.

  The Do not disturb feature can be activated for any call, for internal calls only, or for external calls only.

  If action is set to out of office, then you can enter an out of office message even if the do not disturb function is set to off.

Setup do not disturb, switching on and off

1. In the initial condition press the key ⊖ or ⊙.
2. Use the arrow keys to select the menu **User Setup**.
3. Press the key ⊙. The display appears in Figure 76.
4. Use the arrow keys to select the menu **Do not disturb**.
5. Press the key ⊙. The display appears in Figure 88.

```
Do not disturb:                Off
Action:                     Silence
For:                       Any Call

≪ Do not disturb
```

Figure 88: Menu Do not Disturb

```
Do not disturb:                Off
Action:                     Silence
For:                       Any Call
Out of Office Msg.............

≪ Do not disturb
```

Figure 89: Menu Do not Disturb (out of Office)

6. Use the cursor keys to select the line **Do not disturb**.

7. If you press the ⊙ key at this point, you can switch between "On" and "Off".

8. Use the cursor keys to select the line **Action**.

9. If you press the key ⊙ repeatedly at this point, you may switch between "Ringing off", "Ring once", "Silence", "Busy" and "Out of Office".

10. Use the cursor keys to select the line **For**.

11. If you press the key ⊙ repeatedly at this point, you may switch between "Any Call", "External Calls" and "Internal Calls".

12. In order to store the selection, leave the menu by pressing the key ⊖ three times.

The set call diversion is now active. If the permanent call diversion is active, this is indicated in the display of the telephone.

3.9 Menu Phone Setup

```
Headset:                    Off
Direct Dial...................
Lock Phone....................
Change PIN....................
LCD Contrast:                 7
LCD Light:                   On
< Phone Setup
```

Figure 90: Menu Phone Setup (1. Part)

```
Keypad Light:                On


< Phone Setup
```

Figure 91: Menu Phone Setup (2. Part)

3.9.1 Headset

Setup headset, switching on and off

1. In the initial condition press the key ⊖ or ⊙.
2. Use the arrow keys to select the menu **Phone Setup**.
3. Press the key ⊙. The display appears in Figure 90.
4. Use the arrow keys to select the line **Headset**.
5. If you press the key ⊙ at this point, you can switch between "On" und "Off". If a headset is connected to the telephone, the headset can be enabled.

3.9.2 Direct Dial

Setup direct dial, switching on and off

1. In the initial condition press the key ⊖ or ⊙.
2. Use the arrow keys to select the menu **Phone Setup**.
3. Press the key ⊙. The display appears in Figure 90.

4. Use the arrow keys to select the menu **Do not disturb**.

5. Press the key ⊙. The display appears in Figure 92.

```
Direct dial:                    Off
Number:
Delay (seconds):                  0


≪ Direct dial
```

Figure 92: Menu Direct dial

6. Use the cursor keys to select the line **Direct dial**.

7. If you press the key ⊙ at this point, you can switch between "On" and "Off".

8. Use the cursor keys to select the line **Number**.

9. Enter the desired Direct dial number.

10. Use the cursor keys to select the line **Delay**.

11. Enter the delay in seconds. Valid values are between 0 and 65535 seconds.

12. In order to store the selection, leave the menu by pressing the key ⊖ three times.

The set direct call is now active and is not indicated in the display of the telephone. If you set a delay t > 0 seconds after picking up the receiver, you have t seconds to make a call. Only when this time has expired, the programmed telephone number will be dialled.

Note

If the direct dial is active and the delay is set to 0 seconds, then after the try to enter digits in the idle state the following error message will be displayed: keyboard locked!

Also with active direct dial no inquiry calls can be made.

3.9.3 Lock Phone

Setup lock phone, switching on and off

1. In the initial condition press the key ⊖ or ⊙.
2. Use the arrow keys to select the menu **Phone Setup**.
3. Press the key ⊙. The display appears in Figure 90.
4. Use the arrow keys to select the menu **Lock Phone**.
5. Press the key ⊙. The display appears in Figure 93.

```
  Please enter PIN

PIN:


< Authentication
```

Figure 93: Menu Authentication

6. Enter the PIN and confirm the entry by pressing the ⊖ key. Each entered digit is shown as * in the display.
7. If the entered PIN is not valid, the message in Figure 94: is shown briefly. The screen in Figure 93 appears again.

```


          PIN invalid


```

Figure 94: Menu PIN Invalid

8. If the entered PIN is valid, the message in Figure 95 is shown briefly. Thereafter, the telephone is in its initial condition. A display message indicates that the telephone is locked.

```
Attention
no emergency calls
possible!

<
```

Figure 95: Menu Authentication PIN Valid

9. If the telephone is locked, and you press one of the keys ◄, ▼, Ⓒ, ▲, ►, ⇨, Ⓡ (short or long), ⊛(long) or some programmed function keys the message in Figure 93: Menu Authentication appears. Enter the PIN and confirm the entry by pressing the ⇨ key.

10. If the PIN entry is correct, the telephone is unlocked and in its initial condition.

11. If the entered PIN is not correct, the message in Figure 94: appears briefly. Then the message in Figure 93: Menu Authentication appears again.

3.9.4 Change PIN

1. In the initial condition press the key ⇨ or ►.

2. Use the arrow keys to select the menu **Phone Setup**.

3. Press the key ►. The display appears in Figure 90.

4. Use the arrow keys to select the menu **Change PIN**.

5. Press the key ►. The display appears in Figure 96.

```
Cur PIN:
New PIN:
New PIN:

< Change PIN
```

Figure 96: Menu Change PIN

6. Enter the old PIN.

7. Press the key ▼ to go to the next line.

8. Enter the new PIN. Allowed are the characters 0 – 9, *, #. The PIN can be 0 – 12 characters long.

9. Press the key ⊙ to go to the next line.

10. Enter the new PIN one more time.

11. Press the key ⊖ to confirm the entry.

12. If the entered PIN change is valid, the message in Figure 95 is shown briefly. Then the screen in Figure 58 appears.

Changes activated

Figure 97: Menu Changes Activated

13. If the entered PIN change is not valid, the message in Figure 94 is shown briefly. Then the screen in Figure 96 appears.

3.9.5 LCD Contrast

1. In the initial condition press the key ⊖ or ⊙.

2. Use the arrow keys to select the menu **Phone Setup**.

3. Press the key ⊙. The display appears in Figure 90.

4. Use the arrow keys to select the menu **LCD Contrast**.

5. With the keys ⊙ und ⊙ you can change the LCD contrast.

3.9.6 LCD Light

1. In the initial condition press the key ⊖ or ⊙.

2. Use the arrow keys to select the menu **Phone Setup**.

3. Press the key ⊙. The display appears in Figure 90.

4. Use the arrow keys to select the menu **LCD Light**.

5. If you press the key ⊙ at this point, you can switch between "On" und "Off".

3.9.7 Keypad Light

This feature is only available for telephones with an illuminated keypad.

1. In the initial condition press the key ⊖ or ⊙.
2. Use the arrow keys to select the menu **Phone Setup**.
3. Press the key ⊙. The display appears in Figure 90.
4. Use the arrow keys to select the menu **Keypad Light**.
5. If you press the key ⊙ at this point, you can switch between "On" und "Off".

3.10 Menu User List

```
1 FHF4                    104 +*
2 FHF204                  204 -
3
4
5
6
< User List
```

Figure 98: Menu User List

The User List lists all configured users. One line contains the following user information:

- name
- call number
- state (+ for registered, - for unregistered)
- active user (* appears at the end of the line)

Use the cursor keys to select a user, and press the ⊙ key. A screen appears as shown in Figure 99 to Figure 102.

```
Preferences...................
Ring Melody...................
Function Keys................
≪ FHF4 104
```

Figure 99: Menu <active user 1>

```
Activate......................
Preferences...................
Ring Melody...................
Function Keys................
≪ FHF4 104
```

Figure 100: Menu <inactive user 1>

```
Preferences...................
Ring Melody...................
Function Keys................
Registration.................
≪ FHF4 104
```

Figure 101: Menu <active user 2 - 6>

```
Activate......................
Preferences...................
Ring Melody...................
Function Keys................
Registration.................
≪ FHF4 104
```

Figure 102: Menu <inactive user 2 - 6>

3.10.1 Activate

Activate a user

1. In the initial condition press the key ⊖ or ⊙. The display appears in Figure 58.

2. With the arrow keys select the menu **User List**.

3. Press the key ⊙. The display appears in Figure 98.

4. With the arrow keys select the desired user.

5. Press the key ⊙. The display appears like in Figure 99 to Figure 102.

6. With the arrow keys select the menu **Activate**.

7. Press the key ⊙. The display appears for a short time in Figure 103.

Activate
OK

Figure 103: Menu OK

8. The display appears in Figure 98.

3.10.2 Preferences

In the Preferences menu, the operating language of the telephone and the date format may be set as follows:

1. In the initial condition press the key ⊖ or ⊙. The display appears in Figure 58.

2. With the arrow keys select the menu **User List**.

3. Press the key ⊙. The display appears in Figure 98.

4. With the arrow keys select the desired user.

5. Press the key ⊙. The display appears like in Figure 99 to Figure 102.

6. With the arrow keys select the menu **Preferences**.

7. Press the key ⊙. The display appears in Figure 104.

```
Language:                English
Date:                    Default

⋘ Preferences
```

Figure 104: Menu Preferences

Select language

8. With the arrow keys select the menu **Language**.

9. If you now press the ⦿ key repeatedly, you may set the operating language. The following languages are supported:

   - German (Deutsch)
   - English (English)
   - French (Francaise)
   - Dutch (Nederlands)
   - Italian (Italiano)
   - Spanish (Espanol)
   - Swedish (Svenska)
   - Danish (Dansk)
   - Norwegian (Norsk)
   - Finnish (Suomi)
   - Czech (Cestina)
   - Estonian (Eesti)
   - Portuguese (Portugues)
   - Latvian (Latvieou)
   - Croatian (Hrvatski)

- Polish (Polski)

Select format of date

10. With the arrow keys select the menu **Date**.

11. If you now press the ⊙ key repeatedly, you may set the date format. The following formats are supported:

    - Default
    - 24H
    - AM/PM

12. In order to store your personal settings, press the ⊖ key twice and answer **Yes** to the confirmation question.

```
Settings changed!
Save Changes?


No.............................
Yes............................
≪ Decision
```

Figure 105: Menu Decision Save Changes

13. The display appears in Figure 98.

3.10.3 Ring Melody

The embedded ringing tone can be set individually for each user for the various types of calls.

1. In the initial condition press the key ⊖ or ⊙. The display appears in Figure 58.
2. With the arrow keys select the menu **User List**.
3. Press the key ⊙. The display appears in Figure 98.
4. With the arrow keys select the desired user.
5. Press the key ⊙. The display appears like in Figure 99 to Figure 102.
6. With the arrow keys select the menu **Ring Melody**.

7. Press the key ⊙. The display appears in Figure 106.

8. With the arrow keys select the menu Ring Melody.

9. If you now press the key ⊙ repeatedly, you may choose between Ring Melody (int), Ring Melody (ext), Ring Melody (ret) or Ring Melody (msg). The set melody, volume (Vol) and speed (Speed) is displayed for the current type of call.

10. The possible settings are described in chapter 3.6.4.1.1 "Ringing Ton" on page 113.

11. In order to store the selection, leave the menu by pressing the ⊖ key twice, confirm the change with „Yes" and press the ⊖ key twice.

```
Ring Melody (int)............
Start........................
Melody:                Default
Vol:                       Def
Speed:                     Def

⋘ Ring Melody
```

Figure 106: Menu Ring Melody

3.10.4 Registration

```
Setup
Unregister...................
Delete.......................

⋘ Registration
```

Figure 107: Menu User List Registration Unregister

```
Setup
Register.....................
Delete.......................

⋘ Registration
```

Figure 108: Menu User List Registration Register

3.10.4.1 Setup

Refer to chapter 3.11.3 Registration

3.10.4.2 Register

With the arrow keys select the menu Register and press the key ⊙. For a short time the display appears in Figure 103. Then the display appears in Figure 98.

3.10.4.3 Unregister

With the arrow keys select the menu Unregister and press the key ⊙. For a short time the display appears in Figure 103. Then the display appears in Figure 98.

3.10.4.4 Delete

With the arrow keys select the menu Delete and press the key ⊙. The screen in Figure 109 appears.

```
delete?



No.............................
Yes............................
⋘ Decision
```

Figure 109: Menu Decision Delete

With the arrow keys select the menu No and press the key ⊙. Then the display appears in Figure 98.

With the arrow keys select the menu Yes and press the key ⊙. For a short time the display appears in Figure 110. Then the display appears in Figure 98.

```
User deleted
```

Figure 110: User Deleted

3.10.5 Function Keys

On a telephone with a 21 key keypad, you have 10 function keys. To get the function keys (F1 – F10) you have to press the hash key ⊞ (long) (for more than a second) (shift function) and than to press a digit key (1 – 9, 0). You don't have a lamp or a display field in the phone display for any function key.

On a telephone with additional input lines, you can connect additional keys. Depending on the configuration of the additional input lines up to 10 additional function keys will be available. Even if the additional function keys are not or not all released, they will appear in this menu.

```
1 ............................
2 ............................
3 ............................
4 ............................
5 ............................
6 ............................
⋘ Function Keys              ▼
```

Figure 111: Function Keys ResistTel IP2 / IP152 (1. Part)

```
7 ............................
8 ............................
9 ............................
10 ...........................
11 ...........................
12 ...........................
⋘ Function Keys              ⇕
```

Figure 112: Function Keys ResistTel IP2 / IP152 (2. Part)

```
13 ...........................
14 ...........................
15 ...........................
16 ...........................
17 ...........................
18 ...........................
⋘ Function Keys              ⇕
```

Figure 113: Function Keys ResistTel IP2 / IP152 (3. Part)

```
19 ...........................
20 ...........................

⋘ Function Keys              ▲
```

Figure 114: Function Keys ResistTel IP2 / IP152 (4. Part)

```
1 ............................
2 ............................
3 ............................
4 ............................
5 ............................
6 ............................
⋘ Function Keys              ▼
```

Figure 115: Function Keys ExResistTel IP2 / IP154 (1. Part)

```
7 ............................
8 ............................
9 ............................
10 ...........................

⋘ Function Keys              ▲
```

Figure 116: Function Keys ExResistTel IP2 / IP154 (2. Part)

3.10.5.1 Function Keys General

In general, there are two different kinds of function keys, which can take one or more conditions:

1. Function keys that are assigned to the telephone display, can be defined with the parameters Text or Icon, according to the particular state.

Text	Here, you enter the text to be shown in the display beside the function key. The text can be freely chosen and may consist of 20 characters per function key.
Icon	Alternatively, an icon (a symbol) can be shown in the display. The assignment of graphics to names is described in the following table „Icon Definition" (Figure 194 on page 246).

2. Function keys with an LED indicator can be assigned to the states:

   - off
   - blink
   - flicker

- on

All function keys can be configured at the phone. A complete configuration with all options is only possible with the web interface of the phone.

If a line in the function key overview is beginning with a *, then the programming of the key can't be displayed and can't be modified.

3.10.5.2 Function Key Undefined

```
Type:                    Undefined
                                  
                                  
                                  
                                  
                                  
<<< Function Keys
```

Figure 117: Function Key (Type Undefined)

3.10.5.3 Function Key Destination Number

```
Type:             Destination No.
Text:
Icon:
Number:
Announcement:                 Off
Prepare:                      Off
<<< Function Keys
```

Figure 118: Function Key (Type Destination No.)

This function enables the user to assign a number to a function key in such a way that the function key can be used to call a distant end directly.

The following configurable parameters are at the user's disposal:

Number	the number will be dialled directly
Number	Direct inward dialling
Announcement	This function activates an announcement function. If this telephone system is switched to hands-free or loudspeaker, a direct announcement is possible.

Prepare	This is a set option, under which the connection is not immediately established, but which serves as dialling preparation in the sense that the number can be completed by further digits. Only as a consequence of subsequent actions, like picking up the receiver or turning on the enabling telephone, the number is dialled.

3.10.5.4 Function Key Partner

```
Type:                    Partner
Text:
Icon:
Number:
Intrude:                      No
Display Number................
<<< Function Keys              ▼
```

Figure 119: Function Key (Type Partner, 1. Part)

```
Presence:                     Off

<<< Function Keys              ▲
```

Figure 120: Function Key (Type Partner, 2. Part)

```
calling:                       On
connected:                    Off

<<< Display Number
```

Figure 121: Display Number (calling, connected)

The partner function is subdivided into three states.

Idle	In this idle state, the key performs direct dialling.
Alerting	This state indicates that the partner telephone rings, and you can use this key to answer the call (pick-up).
Busy	In case the line is busy, the function key indicates the partner state only.

In „number", the partner telephone is defined with the corresponding number.

Caution

The PBX must support the feature, both telephones must be in a common group, and the partner functions must be enabled.

Note

The described functions can only be used if both users (the assigning and the assignee) belong to the same group. The same group is selected in the PBX.

Additional the following options are selectable.

Intrude	Send Intrusion call to busy partner. When this feature is active, you can select the type of the call. • No • Conference • Monitor
Display Number calling	Show calling party in alerting state
Display Number connected	Show connected party in busy state
Presence	Subscribe for Presence

3.10.5.5 Function Key Park

```
Type:                          Park
Text:
Icon:
Number:
Position:
Display Number................
<<< Function Keys
```

Figure 122: Function Keys (Type Park)

```
calling:                         On


<<< Display Number
```

Figure 123: Display Number (calling)

This function can be used to park a call. The following parameter can be selected:

Number	Number
Position	Position
Display Number calling	Show parked party

3.10.5.6 Function Key Pickup

```
Type:                    Pickup
State:                        1
Text:
Icon:
Display Number................

⋘ Function Keys
```

Figure 124: Function Keys (Type Pickup, State 1)

```
Type:                    Pickup
State:                        2
Text:
Icon:
LED:                        Off
Display Number................

⋘ Function Keys
```

Figure 125: Function Keys (Type Pickup, State 2)

Within a group, an incoming call can be picked up by a participant, whereby the telephone number is shown in the display. If several participants of the group are being called, a list of calls is generated, enabling the participants to choose in advance which call to pick up.

Display Number calling	Display calling party

3.10.5.7 Function Key Message Waiting Indicator

```
Type:                          mwi
State:                           1
Text:
Icon:
Number:
Append Own Nr.:               Off
⋘ Function Keys                ▼
```

Figure 126: Function Keys (Type MWI, State 1, 1. Part)

```
Global:                        Off


⋘ Function Keys                ▲
```

Figure 127: Function Keys (Type MWI, State 1, 2. Part)

```
Type:                          mwi
State:                           2
Text:
Icon:
LED:                          Off
Number:
⋘ Function Keys                ▼
```

Figure 128: Function Keys (Type MWI, State 2, 1. Part)

```
Append Own Nr.:               Off
Global                        Off


⋘ Function Keys                ▲
```

Figure 129: Function Keys (Type MWI, State 2, 2. Part)

In order to get into the message center, you need the access data, which are defined on the basis of the telephone number and the name. Optionally you can append your own number to the message center account number.

If no messages are present, you may play back old messages (state 1) or for instance rephrase the announcement. In state 2 you may listen to the new messages.

Number	Calling number of the message center
Append Own Nr.	Append own calling number to the dialled number
Global	Off/On

3.10.5.8 Function Key Call Forwarding

```
Type:            Call Forwarding
State:                         0
Text:
Icon:
Call Diversion................

⋘ Function Keys
```

Figure 130: Function Keys (Type Call Forwarding, State 0)

```
Unconditional:               Off

Busy:                        Off

No Replay                    Off

⋘ Call Diversion
```

Figure 131: Call Diversion

```
Type:            Call Forwarding
State:                         1
Text:
Icon:
LED:                         Off
Call Diversion................
⋘ Function Keys
```

Figure 132: Function Keys (Type Call Forwarding, State 1, 2 or 3)

```
Type:            Call Forwarding
State:                         4
Text:
Icon:
LED:                         Off

<<< Function Keys
```

Figure 133: Function Keys (Type Call Forwarding, State 4)

This function allows incoming calls to be diverted. Four states with different destinations can be configured (for example, mobile phone, voicemail), which are offered in succession. In each of these states, the following options can be used:

Always	This indicates a permanent call diversion.
Busy	The call diversion is activated if one's own telephone is busy.
No Response	The call diversion is activated after a delay, e.g. four rings.

3.10.5.9 Function Key Call Group

```
Type:                 Call Group
State:                         1
Text:
Icon:
Name:

<<< Function Keys
```

Figure 134: Function Keys (Type Call Group, State 1)

```
Type:                 Call Group
State:                         2
Text:
Icon:
LED:
Name:
<<< Function Keys
```

Figure 135: Function Keys (Type Call Group, State 2)

Using this function, a user can log on or off the call distribution of a collective line group. For the registration the name of the group identification is necessary.

Group Identification:

Name	Name of the group identification

3.10.5.10 Function Key Directory

```
Type:                    Directory
Text:
Icon:
Searching:               Combined

⋘ Function Keys
```

Figure 136: Function Keys (Type Directory)

This function can be used for searching for entries in the telephone book. For searching parameters can be selected:

- Combined Directories
- Local Directory
- PBX Directory
- External Directory

3.10.5.11 Function Key Register

```
Type:                    Register
State:                          1
Text:
Icon:
Reg.ID:
Activate Reg.:               Off
⋘ Function Keys
```

Figure 137: Function Keys (Type Register, State 1)

```
Type:                    Register
State:                          2
Text:
Icon:
LED:                          Off
Reg.ID:
 ⋘Function Keys                ▼
```

Figure 138: Function Keys (Type Register, State 2, 1. Part)

```
Activate Reg.:               Off

⋘ Function Keys                ▲
```

Figure 139: Function Keys (Type Register, State 2, 2. Part)

Using this function, a user is enabled or locked. If the user was the active user, the previous user automatically becomes the active user.

The following parameters are selectable:

Reg. ID	Numeric configuration identifier of the target registration (1..6)
Activate Reg.	The target registration shall become the active registration when enabled.

3.10.5.12 Function Key Activate

```
Type:                    Activate
Text:
Icon:
Reg.ID:
Disable act. Reg:             Off
Act.next. Reg.                Off
⋘ Function Keys
```

Figure 140: Function Keys (Type Activate)

As soon as several users are logged on, this function can be used to switch to the other user.

Tip

When the new registration has become active after use, the settings of the new registration are also valid.

Reg. ID	Numeric configuration identifier of the target registration (1..6)
Disable act. Reg.	Disable the current registration when activating the actual target registration.
Act. next Reg.	Activate next registration

3.10.5.13 Function Key Ringing off

```
Type:                Ringing off
State:                         1
Text:
Icon:
Do not disturb................

<<< Function Keys
```

Figure 141: Function Keys (Type Ringing off, State 1)

```
Type:                Ringing off
State:                         2
Text:
Icon:
LED:                         Off
Do not disturb................

<<< Function Keys
```

Figure 142: Function Keys (Type Ringing off, State 2)

The Do Not Disturb function can be controlled via a function key. You can choose between the states 'On' and 'Off'.

Action	Under Action the Do not Disturb variant can be selected. • Silence • Busy • Ringing off
For	Under Apply to the kind of call to be treated by the feature can be selected. • Any Call • External Calls • Internal Calls

3.10.5.14 Function Key Call Waiting

```
Type:                Call waiting
State:                          1
Text:
Icon:

<<< Function Keys
```

Figure 143: Function Keys (Type Call Waiting, State 1)

```
Type:                Call waiting
State:                          2
Text:
Icon:
LED:                          Off

<<< Function Keys
```

Figure 144: Function Keys (Type Call Waiting, State 2)

If a call is already active, an incoming call can be treated in different ways, depending on the current state. The state can be determined by the function key.

State 1	If the Call Waiting function is deactivated, the second caller hears a busy signal.
State 2	If the ‚Call Waiting' function is activated, the call is shown in the display, and a short signalling tone can be heard by the person who is being called. The person who is being called, may then • end the call, in order to answer the new call, • put the active call on hold, in order to switch to the new call, or • reject the call.

3.10.5.15 Function Key Number Presentation

```
Type:            Number Present.
State:                         1
Text:
Icon:

⋘ Function Keys
```

Figure 145: Function Keys (Type Number Presentation, State 1)

```
Type:            Number Present.
State:                         2
Text:
Icon:
LED:                         Off

⋘ Function Keys
```

Figure 146: Function Keys (Type Number Presentation, State 2)

Transmitting one's own number can be temporarily suppressed by means of this function.

- State 1 = Telephone number is suppressed
- State 2 = Telephone number is transmitted

3.10.5.16 Function Key Transfer

```
Type:                    Transfer
Text:
Icon:

<<< Function Keys
```

Figure 147: Function Keys (Type Transfer)

In case of a new incoming call during an already active call, the new call must be answered (switch active call using the 'R' key). During the two established calls, the ‚Transfer' function can be used to connect the two callers with each other, and to place one's own VoIP telephone in idle mode.

3.10.5.17 Function Key Redirect

```
Type:                    Redirect
Text:
Icon:
Number:

<<< Function Keys
```

Figure 148: Function Keys (Type Redirect)

This function puts two options at your disposal:

1. Using this key, you may divert an incoming call to the configured number.
2. If during a call, a second call occurs, this function can be used to divert the active caller, in order to answer the new call.

Number	The number to be called.

3.10.5.18 Function Key Phone Lock

```
Type:                    Phone Lock
State:                            1
Text:
Icon:

⋘ Function Keys
```

Figure 149: Function Keys (Type Phone Lock, State 1)

```
Type:                    Phone Lock
State:                            2
Text:
Icon:
LED:                          Off

⋘ Function Keys
```

Figure 150: Function Keys (Type Phone Lock, State 2)

This function can be used to lock the telephone. A setup of the functions to be locked can be done under protect (see chapter 4.7.5 on page 275).

The PIN can be entered respectively changed as follows:

- "Menu"
- "Telephone access"
- "Change PIN"

In the as-delivered condition, no PIN is stored.

3.10.5.19 Function Key Headset

```
Type:                       Headset
State:                            1
Text:
Icon:

⋘ Function Keys
```

Figure 151: Function Keys (Type Headset, State 1)

```
Type:                    Headset
State:                         2
Text:
Icon:
LED:                         Off

⋘ Function Keys
```

Figure 152: Function Keys (Type Headset, State 2)

In order to control the telephone when a headset is connected, a key, depending on the particular VoIP telephone, works as a hook switch:

State 1	• Headset control off
State 2	• Headset control on

3.10.5.20 Function Key Hotdesk

```
Type:                    Hotdesk
State:                         1
Text:
Icon:

⋘ Function Keys
```

Figure 153: Function Keys (Type Hotdesk, State 1)

```
Type:                    Hotdesk
State:                         2
Text:
Icon:
LED:                         Off

⋘ Function Keys
```

Figure 154: Function Keys (Type Hotdesk, State 2)

If different participants often log on using a certain telephone, the function Hot Desking can be used to obtain the access data upon each logon. If the state changes to state 1, the co-user is logged off again.

3.10.5.21 Function Key Create Registration

```
Type:                Create Reg.
State:                         1
Text:
Icon:
Registration..................

⋘ Function Keys
```

Figure 155: Function Keys (Type Create Registration, State 1)

```
Type:                Create Reg.
State:                         1
Text:
Icon:
LED:                         Off
Registration..................
⋘ Function Keys
```

Figure 156: Function Keys (Type Create Registration, State 2)

```
Protocol:               H323
Name:                        1
Number:
Passw.:
VoIP Gatekeeper...............
Activate...................Off
⋘ Registration
```

Figure 157: Function Keys (Type Create Registration, Registration)

In the active state, a further user is logged on for the telephone. According to this, the logon can take place

- in the same telephone system,
- in another telephone system, or
- directly at an IP telephony provider

The protocols H323, SIP, TSIP or SIPS can be used for this purpose. The allocation of the parameters in the Active State can be obtained from the particular provider of the system. The option "activate" is used to activate the new registration.

☞	**Note** You can determine an 'active user'. The outbound calls are conducted under his parameters, and the function keys are, if necessary, applied on another VoIP telephone.	☜

Protocol	H323, SIP, TSIP or SIPS
Name	The name that is to be entered here is required for the registration only if the number has not been entered.
Number	Telephone numbers that are required for the registration are entered here.
VoIP Gatekeeper	The submenu to enter the VoIP gatekeeper can be activated here.
Activate	Following registration, this registration is set as the active registration.

```
Gatekeeper ID

Gatekeeper IP Address
   .    .    .

⋘ VoIP Gatekeeper
```

Figure 158: Function Keys (Type Create Registration, VoIP Gatekeeper (Protocol H323))

Gatekeeper ID	If several gatekeepers are to be active on one address, among these a certain gatekeeper is identified on the basis of the name that is to be entered here.

Gatekeeper IP Address	This is the IP address, under which the PBX or the responsible gatekeeper can be reached.

For the protocol H323 the gatekeeper can be defined by IP address only. Therefore you can enter digits only.

```
Gatekeeper ID

Proxy

⋘ VoIP Gatekeeper
```

Figure 159: Function Keys (Type Create Registration, VoIP Gatekeeper (Protocol SIP/TSIP/SIPS))

Gatekeeper ID	If several gatekeepers are to be active on one address, among these a certain gatekeeper is identified on the basis of the ID that is to be entered here.
Proxy	This is the IP address or domain name, under which the PBX or the responsible gatekeeper can be reached. The input has to be alphanumerical. If an IP address has to be entered only. The dots (.) have to be entered also (alphanumerical input with the key 0).

Note

If a domain name is defined, a DNS server must be defined and reachable. The DNS server must be able to resolve the name.

3.10.5.22 Function Key Delete Registration

```
Type:                Delete Reg.
Text:
Icon:

<<< Function Keys
```

Figure 160: Function Keys (Type Delete Registration)

The still active co-user, in this option is deregistered, and the previous user thus automatically restored to the state of active user.

3.10.5.23 Function Key Switch User

```
Type:                Switch User
Text:
Icon:
Registration..................

<<< Function Keys
```

Figure 161: Function Keys (Type Switch User)

```
Protocol:                  H323
Name:
Number:
Passw.:
VoIP Gatekeeper...............
Disable act. Reg:           Off
<<< Registration
```

Figure 162: Function Keys (Type Switch User, Registration)

With this function key the registration can be switched.

Protocol	H323, SIP, TSIP, SIPS
Name	The name that is to be entered here is required for the registration only if the number has not been entered.
Number	Telephone numbers that are required for the registration are entered here.
VoIP Gatekeeper	Here you can enter the submenu to enter the VoIP gatekeeper (See chapter 3.10.5.21 on page 155).
Disable act. Reg.	Disable active registration

3.10.5.24 Function Key Recording

```
Type:                    Recording
State:                           1
Text:
Icon:

⋘ Function Keys
```

Figure 163: Function Keys (Type Recording, State 1)

```
Type:                    Recording
State:                           2
Text:
Icon:
LED:                           Off

⋘ Function Keys
```

Figure 164: Function Keys (Type Recording, State 2)

This function key can activate or deactivate the recording function.

3.10.5.25 Function Key Boolean Object

```
Type:                    Bool Obj.
State:                           1
Text:
Icon:
LED:                           Off
Number:
⋘ Function Keys                  ▼
```

Figure 165: Function Keys (Type Boolean Object, State 1 - 4, 1. Part)

```
Toggle                         Off


⋘ Function Keys                  ▲
```

Figure 166: Function Keys (Type Boolean Object, State 1 - 4, 2. Part)

The boolean object can assume four states.

- Automatic off state
- Automatic on state
- Manual override off state
- Manual override on state

The identification will be done with calling number and name.

Number	Number
Toggle State	Toggle state with each key position change

3.10.5.26 Function Key Presence

```
Type:                    Presence
State:                          1
Text:
Icon:

⋘ Function Keys
```

Figure 167: Function Keys (Type Presence, State 1)

```
Type:                    Presence
State:                          2
Text:
Icon:
LED:                          Off

⋘ Function Keys
```

Figure 168: Function Keys (Type Presence, State 2)

The presence can be activated or deactivated with this function key.

By subsequent pressing this function key, someone toggles own presence activity until desired activity reached.

This function key is a handy shortcut for a long navigation way through main menu: main menu, user settings, presence, toggle activity, menu, menu.

3.10.5.27 Function Key Prepare Override

```
Type:              Prep. override
State:                          1
Text:
Icon:

⋘ Function Keys
```

Figure 169: Function Keys (Type Prepare Override, State 1)

```
Typ:                Prep. override
State:                           2
Text:
Icon:
LED:                           Off

⋘ Function Keys
```

Figure 170: Function Keys (Type Prepare Override, State 2)

This function key can be used to prepare a call with some override options and to complete the calling number or the name with further digits or characters. The calling will be started with lifting up of the handset or pressing the load speaker or headset key:

If a key is pressed and if…

- the phone is in the idle state and the option dial is activated, then the outgoing call will be executed immediately, expect if both parameter fields (number) and (name) are empty.

- the phone is in the idle state and the option dial is not activated, then the indirect calling menu will appear. The menu footer displays the override option (*CO* - Caller Override , *DO* - Diversion Override).

- the indirect calling menu is active (called with this or another key), then a call with the given override options (entered in the menu) will be executed.

- the handset will be lift off and no digits will be entered, then the call with the entered options will be repeated.

- the handset will be lift off and some digits have been entered, then the key will be ignored.

- a connected call exists, then an inquiry call will be executed.

- more than one connected call exists, then the key will be ignored.

3.10.5.28 Function Key Toggle

```
Type:                    Toggle
State:                        1
Text:
Icon:

⋘ Function Keys
```

Figure 171: Function Keys (Type Toggle, State 1)

```
Type:                    Toggle
State:                        2
Text:
Icon:
LED:                        Aus

⋘ Function Keys
```

Figure 172: Function Keys (Type Toggle, State 2)

This function key is used to send alternating DTMF sequences in an active call, for example to implement a Push to Talk button.

If the key is pressed the DTMF digits assigned to the current state are sent and the state is switched to the alternate state.

If there is no active call the key is ignored.

A complete configuration of this function key is only possible with the web interface of the phone. (See chapter 4.7.1.5.28 on page 269.)

3.10.5.29 Function Key Message

```
Type:                   Message
Text:
Icon:
Message.......................

⋘ Function Keys
```

Figure 173: Function Keys (Type Message)

Sending messages can be started with this function key.

This function key is a handy shortcut for a long navigation way through main menu: main menu, messages, new message.

3.10.5.30 Function Key Spare

```
Type:                    Spare
Text:
Icon:

<<< Function Keys
```

Figure 174: Function Keys (Type Spare)

With this Function a spare function key to reserve key positions for administrative purposes can be configured.

3.11 Menu Administration

The Administration menu contains the administrative data relating to the network and the registration of the VoIP telephone.

```
Information...................
IP Settings...................
Registration.................
Reset Configuration...........

< Administration
```

Figure 175: Menu Administration

On setting the option „Protect Configuration at Phone" at the web interface of the phone changing of the configuration will be checked with an authentication.

```
User Name:
Password:

< Authentication
```

Figure 176: Menu Authentication

On setting the option „Hide Configuration at Phone" on the web interface of the phone only the information can be asked.

```
Information..................

< Administration
```

Figure 177: Menu Administration (Hide Configuration at Phone)

If in the Web interface of the telephone the optional menu "Tuning" is activated, then below Administration appears an additional menu item. The activation of the menu is described in the chapter 4.11.2 on page 356.

```
Information..................
IP Settings..................
Registration.................
Reset Configuration..........
Tuning

< Administration
```

Figure 178: Menu Administration (Tuning active)

3.11.1 Information

1. In the initial condition press the key ⊖ or ⊙.

2. Use the arrow keys to select the menu **Administration**.

3. Press the key ⊙. The display appears in Figure 175.

4. Use the arrow keys to select the menu **Information**.

5. Press the key ⊙. The display appears in Figure 179.

```
IP 192.168.0.251
Ser 00-50-c2-6a-50-02
8.00 hotfix 1
IP152[80500.04]
Bootcode[8050004]
HW[101]
≪ Information
```

Figure 179: Menu Information

In the following the current IP address, serial number (MAC address), firmware version number, bootcode version number and hardware version number are shown.

3.11.2 IP Settings

The **IP Settings** menu contains information about IP network integration. These are only of interest to the administrator and may not be changed by the user.

1. In the initial condition press the key ⊖ or ⊙.
2. Use the arrow keys to select the menu **Administration**.
3. Press the key ⊙. The display appears in Figure 175.
4. Use the arrow keys to select the menu **IP Settings**.
5. Press the key ⊙. The display appears in Figure 180.

```
DHCP Mode:                Client
IP Addresses..................
VLAN..........................

≪ IP Settings
```

Figure 180: Menu IP Settings

In this menu, you may set the following IP properties:

Menu Item	Possible settings
DHCP Mode	Client Server Off
IP-Addresses	Interface IP Address IP Address Mask Default IP Gateway
VLAN	VLAN Header Off VLAN Header On (by VLAN Header On additional:) VLAN Identifier Priority RTP Data Priority Signaling

Table 16: IP-Properties Menu IP Settings

3.11.2.1 IP Addresses

```
Interface IP Address
   .   .   .
IP Address Mask
   .   .   .
Default IP Gateway
   .   .   .
⋘ IP Addresses
```

Figure 181: Menu IP Addresses

3.11.2.2 VLAN

```
VLAN Header:                Off


⋘ VLAN
```

Figure 182: Menu VLAN Header Off

```
VLAN Header:                 On
VLAN Identifier:
Prio. RTP Data :
Prio. Signaling


⋘ VLAN
```

Figure 183: Menu VLAN Header On

3.11.3 Registration

The **Registration menu** contains information about gatekeeper registration.

These are only of interest to the administrator and may not be changed by the user.

1. In the initial condition press the key ⊖ or ⊙.
2. Use the arrow keys to select the menu **Administration**.
3. Press the key ⊙. The display appears in Figure 175.
4. Use the arrow keys to select the menu **Registration**.

5. Press the key ⊙. The display appears in Figure 184.

```
Protocol:                    H323
Name:
Number:
Passw.:
VoIP Gatekeeper...............
Options......................
≪ Registration
```

Figure 184: Menu Registration

Note

If the protocol SIPS is selected, the domain name of the registration of the telephone must be the same as the parameter CN or Subject Alternative Name of the device certificate of the PBX.

If this is not the case, then you have to get a certificate accordingly or if the security requests or not so high you can generate a certificate by yourself. This certificate must be installed at the PBX and if necessary in the trust list of the telephone.

Furthermore there is a possibility to suppress this check with the SIPS protocol option 'No Certificate Check' (see chapter 4.11.45 on page 371).

If there are any problems with the protocol SIPS, then these values must be verified with the web interface of the telephone.

3.11.3.1 VoIP Gatekeeper

```
Gatekeeper ID

Gatekeeper IP Address
   .   .   .
Gatekeeper IP Address
   .   .   .
≪≪ VoIP Gatekeeper
```

Figure 185: Menu VoIP Gatekeeper (Protocol H323)

The gatekeeper and the alternate gatekeeper can be entered for the protocol H323 with their IP address only. Therefore digits can be entered only.

```
Gatekeeper ID

Proxy

Proxy 2

⋘ VoIP Gatekeeper
```

Figure 186: Menu VoIP Gatekeeper (Protocols SIP/TSIP/SIPS)

The SIP server (proxy) and the alternative SIP server (proxy 2) can be defined for the protocols SIP/TSIP/SIPS with their IP address or their domain name. The input has to alphanumerical. If an IP address is entered only, then the dots (.) have to be entered too (alphanumerical input with the key 0).

Note

If a domain name is defined, a DNS server must be defined and reachable. The DNS server must be able to resolve the name.

Note

If a telephone is updated from an older software version and is configured to one of the protocols SIP, TSIP or SIPS or the protocol is changed from H323 to SIP, TSIP or SIPS and neither proxy nor alternate proxy are configured, then the at gatekeeper address configured IP address will be used for the registration at a SIP server.

If the gatekeeper or alternate gatekeeper address will be sent via DHCP to the device, then this address will be used independent of the configuration of the gatekeeper in the device and independent of the selected protocol.

If a gatekeeper address is defined as domain name via DHCP, then this is not working with the protocol H323 and not working with devices with older software versions.

3.11.3.2 Options

Under options you may choose the template of tones generated by the VoIP telephone. You have the choice between the following templates:

- europe-pbx
- europe-public
- us
- uk
- italy-pbx
- italy-public
- czech-pbx
- czech-public
- sweden
- france
- swiss
- belgium
- netherlands
- norway
- denmark
- germany
- spain
- finland
- austria
- ireland
- australia
- newzealand
- malaysia
- turkey
- russia
- south africa
- brazil

```
Tones:                  europe-pbx

<<< Options
```

Figure 187: Menu Options

3.11.4 Reset Configuration

The **reset configuration** menu offers the possibility of restoring the default settings for the device. All settings made in the meantime will be lost in the process.

1. In the initial condition press the key ⊖ or ⊙.

2. Use the arrow keys to select the menu **Administration**.

3. Press the key ⊙. The display appears in Figure 175.

4. Use the arrow keys to select the menu **Reset Configuration**.

5. Press the key ⊙. The display appears in Figure 188.

```
Do you want to reset
the device to the
factory defaults?

No.............................
Yes............................
≪ Reset Configuration
```

Figure 188: Menu Reset Configuration

You are then asked whether the device is to be reset to its initial condition.

6. Using the arrow keys, select the entry **No** if you do not wish to restore the default settings.

7. Using the arrow keys, select the entry **Yes** if you wish to restore the default settings. All changes will be lost in the process.

Caution

All data in the phone will be deleted and the phone will be reset to its initial condition if you carry out this function.

8. Press the key ⊙, to confirm your selection.

9. If you choose **no** you return to the previous menu, if you choose **yes**, you must answer a security question.

```
Are you sure?



No.............................
Yes............................
≪ Reset Configuration
```

Figure 189: Menu Security Request Reset Configuration

10. Use the cursor keys to choose **no**, if you do not wish to reset the as-delivered condition.

11. Press the key ⊙, to confirm your selection.

12. If you choose **no**, you return to the previous menu, if you choose **yes**, the device is restarted.

3.11.5 Tuning

The **menu Tuning** is an optional menu, which is locked on default. The activation of the menu is described in the chapter 4.11.2 on page 356. The menu supports to setup some protocol timer. A configuration is only necessary in special cases.

```
TCP keepalive   :
TCP miss alive  :
RAS time to live:
RAS retry count :
RAS request t.o.:
RAS restart t.o.:
≪ Tuning
```

Figure 190: Menu Tuning

The following values can be configured:

- Prioritized TCP Connection Keepalive
  - Packet Send Interval (TCP keepalive)
  - Max Missing Responses (TCP miss alive)
- RAS Gatekeeper Registration Keepalive
  - Time to Live (RAS time to live)
  - Max Retries (RAS retry count)
  - Request Timeout (RAS request t.o.)
  - Restart Timeout (RAS restart t.o.)

4 Administration

The administration of your VoIP telephone is performed by the telephone system administrator.

Below you are provided some administrative information about the telephone specific topics relating to the operation.

4.1 General

4.1.1 Web-Interface

The administration of the VoIP telephone setup conveniently ensues via the Web interface. Some functions can only be programmed via the Web interface, not the telephone menu.

The **user interface** has been tested with Firefox, Internet Explorer (version 7 or higher), Chrome and Safari. Other browsers may work also. Browsers need to support XSLT, JavaScript and CSS.

In order to call up the Web interface of the telephone, the protocols HTTP and HTTPS can be used. Proceed as follows:

1. Start your Web-Browser.

2. Ensure that the telephone is connected to the network.

3. Find out the IP address of your telephone. For this purpose, open the **menu > Administration > Network**.
   The IP address of the telephone should be displayed in the fourth line (e. g. IP: 192.168.200.14).

4. Enter the IP address into the address field of your browser and confirm your entry.
   Example IP-Address:
   http://192.168.200.14
   or
   https://192.168.200.14

5. If the PBX is used as a DNS Server, some PBX types allow you to alternatively enter a combination of the telephone designation and the last 3 hex digit groups of the MAC address in the address field of the browser. Find out the MAC address of your telephone. Do this by opening **Menu > Administration > Information**.

In the second line the MAC address of your telephone should be displayed (e. g.: Ser 00-50-c2-6a-50-02).

6. Confirm your entry here, too.
   Example of type name and part of the MAC address:
   http://IP152-6a-50-02
   or
   https://IP152-6a-50-02

The information page of the telephone is displayed. For further entries you require the user name and password. Refer to chapter 4.1.2.

4.1.2 User Name and Password

In order to set up the VoIP telephone via the Web interface, you must login with a user name and password.

The same user name and the same password will be checked changing the configuration at the interface of the phone, if the option "Protect Configuration at Phone" is active or the telephone will be accessed via the protocol telnet.

User name and password can be changed in the menu **Configuration > General > Admin** of the Web interface.

4.1.2.1 User Name and Password ResistTel IP2 / IP152

In initial condition of the VoIP telephone, the **user name** is admin and the **password** ip152.

4.1.2.2 User Name and Password ExResistTel IP2 / IP154

In initial condition of the VoIP telephone, the **user name** is admin and the **password** ip154.

4.1.3 General Structure

The telephone configuration interface consists of the desktop and up to four menu levels.

1. The first category menu is situated right above of the working desktop. It consists of general items which can be accessed from anywhere with a few exceptions only.

2. The second category menu (main menu) is situated on the left top below the URL of the telephone without protocol information and the product name of the telephone.

3. The third category menu (menu) is situated below the main menu if existing.

4. The fourth category menu (submenu) is situated on the left side of the desktop if existing.

The first 4 main menus,

1. General

2. ETH0 (Ethernet port 0)

3. IP4 (IP version 4)

4. IP6 (IP version 6)

serve the general configuration of the telephone. The area is maintained by the administrator of the telephone system. Note also the information in the administration manual of the PBX.

In many networks, the configuration is conducted by means of the IP service DHCP. For this purpose, the telephone is placed in the DHCP-client mode (menu item IP4/ETH0 (Ethernet)/DHCP).

The VoIP telephone automatically gets the values from the network. The values are visible beside the entry fields of the individual configurations, but if necessary may be overwritten / changed in the left entry field.

4.2 Global Menu <Name of Logged in Administrator>

Here the logged in administrator can be changed. The menu item will be visible after someone has logged in and another item of the main menu will be selected.

4.3 Main Menu General

4.3.1 Menu Info

This area is displayed on the telephone only after the browser has successfully connected, and at first does not require a log-in. The homepage of the VoIP telephone displays the following information:

Version	The version string of the device. This string has the format <Version><label><Product>[<Firmware Build>], Bootcode[<Bootcode Build>], HW[<Hardware Build>]
SerialNo	The serial number or Ethernet MAC address of the VoIP telephone. It consists of 6 pairs of hexadecimal digits separated by '-'. It is followed by a two digits checksum.
DRAM	DRAM Size
FLASH	FLASH Size
Coder	The number of voice channels and the available language compressions (Coder).
SNTP Server	The IP address of the time server (if configured).
Time	The local time of the VoIP telephone according to data from the SNTP server and the time zone.
Uptime	The operating time since the last cold or warm start.

4.3.2 Menu Admin

In this submenu, the user can change the user name and the password at will.

The basic configuration is described in chapter 4.1.2 User Name and Password. For your own safety, we recommend changing the values after commissioning. In order to make it easier to manage several browser windows during configuration, via the content under „Device Name" each window can be given a unique name, instead of the preset IP address.

Entry fields	Description
Device Name	The name of the device. This name is displayed in the browser as a title. It is also added to the product id sent with outgoing registrations. This way it is displayed e.g. on the registrations page of the telephone.
User Name	The administrator account. This account can be used for telnet access (if configured), all password protected pages of the web user interface and (if configured) for changing the configuration with the operating interface of the phone. By default all pages except Administration/General/Info are password protected. The web server of the device can be configured to protect all pages.
Password	The password cannot be left empty. If an empty password is entered, the password won't be changed.
Password Retype	The password has to be entered twice.

You can set up additional administration accounts.

User Name	The administrator account. This account can be used for telnet access (if configured), all password protected pages of the web user interface and (if configured) for changing the configuration with the operating interface of the phone. By default all pages except Administration/General/Info are password protected. The web server of the device can be configured to protect all pages.
Password	The password cannot be left empty. If an empty password is entered, the password won't be changed.
Password Retype	The password has to be entered twice.

Access Right	Administrator / Viewer

Delegated Authentication

Devices with software V8 can delegate authentication of administrative users to an authentication server using Kerberos. To enable remote user authentication the device has to join the realm of a Kerberos server. Delegated authentication can only be used with HTTPS.

The server location of the realm has to be configured, first (see section "Authentication Servers"). Click "Join realm" and specify the username and password of an administrator in the target realm to add the device to the remote host database. This works only with special servers. If you want to authenticate users from a normal third-party server setup cross-realm authentication.

Authentication Servers

The addresses of Kerberos servers have to be configured locally on each host or client device.

If there is no server configured for a realm, the device will try to locate it using DNS. Normally this should work for Windows servers in the LAN.

Clicking to the link Join realm, an input window with the following input parameter will be opened:

Input	Description
Realm	Realm Name
Host name	Host name
Admin user name	Admin user name
Admin password	Admin password

It is possible to enable additional Kerberos encryption types. The following input parameters are available.

Input	Description
Enable RC4	Enable the PC4 Encryption

It is possible to setup more than one authorisation server with the following input parameter:

Input	Description
Realm/Domain	Realm/Domain Name
Address	IP Address
Port	Port Number
Secondary Address	Alternate IP Address
Secondary Port	Alternate Port Number

With clicking the button ok the inputs will be transferred. A new empty input line will be displayed.

Leave realm

An administrator username and password from the realm is needed to deregister from the realm and remove the device from the remote host database. If the server does not exist any longer the registration can be deleted manually.

Disable local authentication

If this option is selected only users from the Kerberos server are accepted. Logins using local administrator accounts will be rejected.

4.3.2.1 Delegated Authentication

4.3.2.1.1 Overview

Each device has its own administrator/viewer accounts.

In version 8 and later a single device can act as an authentication server for the rest of the devices. User accounts that are managed on the authentication server can be used to login on each device in the installation. You can also configure devices to accept user accounts from a PBX or a Windows domain.

4.3.2.1.2 How it works

Version 8 devices can use Kerberos to authenticate users that are not managed locally but on a remote Kerberos server.

4.3.2.1.2.1 Kerberos

A Kerberos server manages users and services for a realm that is specified by a distinct name. It shares a secret password with each user and each service. Users can obtain a ticket for a service from the Kerberos server if they prove that they know their own password. Services can then authenticate users by validating tickets instead of passwords. Therefore many devices can be accessed using the same user credentials but only the Kerberos server and the user have to know it.

4.3.2.1.2.2 Logging in

The main idea of how the centralized login process works in version 8 is the following:

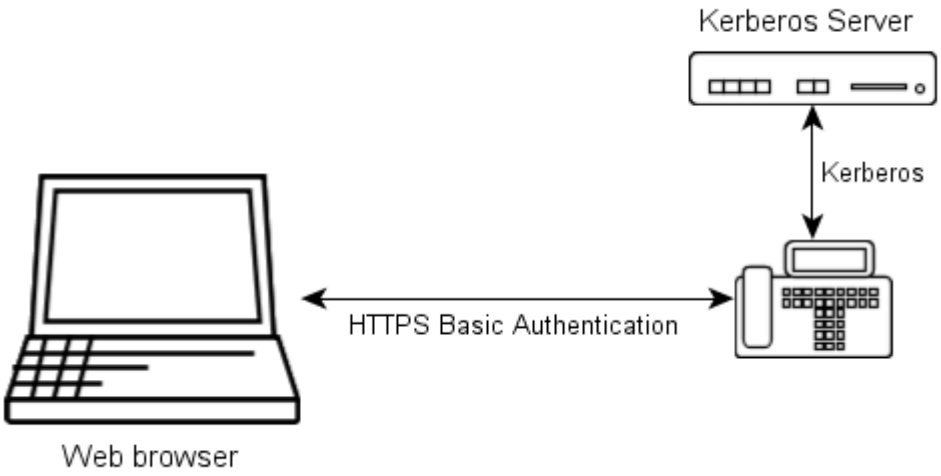


Figure 191: HTTPS Basic Authorisation

1. The browser sends user name and password to the box, using **HTTPS basic authentication**.
2. The box then uses **Kerberos** to obtain a ticket on behalf of the user from the Kerberos server for its own web server.

If that was successful and the password is valid, then the user is authenticated.

4.3.2.1.2.3 Cross Realm Authentication

Cross-realm authentication means that users from one realm/domain can login to services from another realm/domain. To do so, the realms have to trust each other and have a shared secret password to decrypt tickets from the other realm. This password has to be configured on both Kerberos servers. The picture shows how cross-realm authentication is used to login with a Windows domain user at a device.

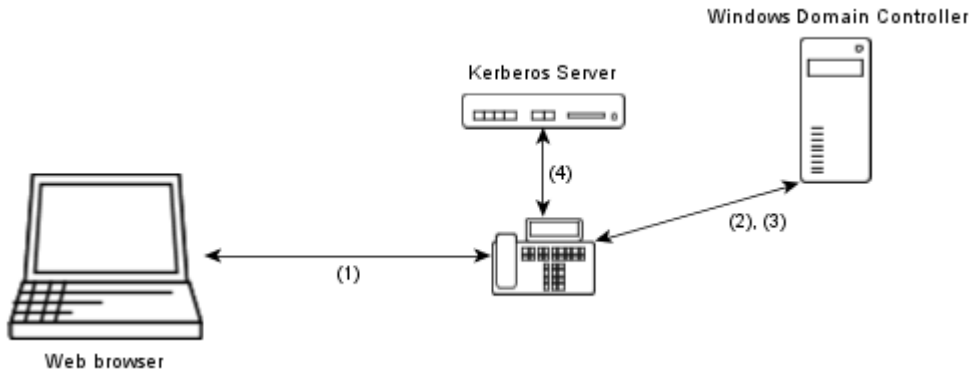


Figure 192: Cross Realm Authentication

1. The browser sends user name and password of a Windows domain user to the box, using HTTPS basic authentication.
2. The box authenticates with the user credentials against the Windows Kerberos server and gets back a ticket-granting ticket.
3. The box uses the ticket-granting ticket to get a ticket for the own Kerberos server.
4. The box uses the cross-realm ticket to obtain a ticket on behalf of the user from the own Kerberos server for its own web server.

If that was successful the password is valid and the user is authenticated.

4.3.2.1.2.4 HTTPS for Encryption

The box needs username and password in the clear to delegate authentication. Basic authentication is used to send that information from the web browser to the box. This message exchange has to be encrypted using HTTPS.

In order to protect user passwords from eavesdropping and to stay compatible with existing configurations at the same time, the devices implement the following behavior if Kerberos is enabled.

HTTP

- No change to the normal behavior
- Digest or Basic authentication is offered
- Local users from the box, only

HTTPS

- Basic authentication, only
- Local users and remote Kerberos users.

As a consequence you have to use HTTPS if you want to login with a Kerberos user account.

4.3.2.1.2.5 Authorization

Tickets issued by an own Kerberos server contain some information whether the user is an administrator or a viewer. When it comes to cross-realm authentication with a Windows domain the own Kerberos server can map between Windows group memberships and administrator rights.

4.3.2.1.2.6 The PBX as a Kerberos Server

Special PBX also provides for Kerberos authentication for its users without additional configuration:

- The *System Name* of the PBX is the name of the realm.
- Users with both a password and rights defined can be used for delegated authentication.
- The *Name* of the user object in the PBX can be used as the user name for authentication.
- Users with the right *Full PBX Administration* are administrators in the Kerberos realm. Users with other rights are viewers.
- LDAP replication also works with the Kerberos information.
- There is a special user called *_KADMIN_* that can be used to add devices to the realm but not to login to the user interface.

4.3.2.1.3 Configuration

4.3.2.1.3.1 Setting up the Kerberos Server

The Kerberos server of a PBX is configured using the PBX/Security page.

Configuration of the stand-alone Kerberos server is done using the General/Kerberos page.

1. Enter a LDAP password. This password is used to encrypt keys in the LDAP directory of the server.
2. Configure the name of the realm.

Now the server is running. You can now create and manage user accounts.

4.3.2.1.3.2 Setting up the Client Devices

Configuration of the clients is done using the General/Admin page from the web administration interface.

1. Configure the *Server Locations* of the Kerberos servers of all involved realms. Don't forget servers that are needed for cross-realm authentication.
2. *Join* the desired Kerberos realm. You will need administrator credentials from that realm in order to do that.

Now the device can authenticate users from the realm for HTTPS connections. You can deactivate the local user accounts on the device, if needed.

Tip

The box that hosts the Kerberos server might also be a client device and have to join the realm.

4.3.2.1.3.3 Setting up Cross-Realm Authentication

1. On the server device, specify the *Trusted Realms*, the corresponding passwords and the methods of authorization mapping.
2. Configure the *Server Location* on each client device.

There are different methods of mapping authorization between realms

- keep (works only with special servers)
- Grant administrator access to all users
- Grant viewer access to all users
- Map the Windows domain group membership from the ticket to administrator or viewer rights

If you use the latter, please specify the RID of the groups that shall have administrator or viewer rights, respectively.

4.3.2.1.3.4 Determining the RID of a Windows Domain Group

The RID (relative ID) of a Windows domain group is the last numeric part of the domain group SID (secure ID).

The easiest way to determine it for a group you are a member of is using the following command:

```
whoami /groups /sid
[Group  1] = "DOMAIN\Domain-Users"  S-1-5-21-854245398-616249376-725345543-513
[Group  2] = "DOMAIN\Admins"  S-1-5-21-854245398-616249376-725345543-1180
```

In this example the RID for *DOMAIN|Domain-Users* is *513* and the RID for *DOMAIN|Admins* is *1180*.

4.3.2.1.3.5 Prerequisites for Windows Groups

You can use a Windows group for authorization if

- it is in the domain of the users
- it is a global security group
- it does not contain nested groups

4.3.2.1.4 Using it

If your Kerberos Server is once configured you can use Kerberos user accounts for logging into the administration interface of boxes using your web browser.

4.3.2.1.4.1 Use HTTPS for Kerberos Users

Delegated authentication works only with HTTPS connections. Using HTTP the boxes accept only local user accounts.

4.3.2.1.4.2 User Names

To distinguish between local users and users of a Kerberos realm, the name of the realm has to be pretended to the user name, separated by a backslash (\). Alternatively you can append the realm to the user name separated by an at (*@*).

Example:

- Local user: *admin*
- Remote user: REALM\username or username@REALM

☝	**Tip** Mind that realm names are case sensitive and that they are usually written in upper case letters.	☝

4.3.2.1.5 Security Considerations

4.3.2.1.5.1 Use local Users only for Recovery Purposes

Although the old local user accounts of devices can still be used to login, this should not be done.

We recommend choosing a different secure administrator password for each device. After Single Sign-On has been configured, the list of admin passwords should be locked away and used only for recovery purposes. For normal configuration only user accounts from the Kerberos realm should be used to access devices.

We recommend that because it is much easier to change the password of or delete a compromised user account on the Kerberos server than changing the local administrator passwords on each device.

4.3.3 Menu Certificates

4.3.3.1 File Formats

The following file formats are supported:

- DER (Distinguished Encoding Rules)
- PEM (Personal E-Mail)
- PKCS#12 (Public Key Cryptography Standard 12) (read only)

4.3.3.2 Certificate Types

The following certificate types are supported:

- X.509 versions 1-3

4.3.3.3 Certificate Extensions

The following certificate extensions are supported:

- basicConstraints
- keyUsage
- extKeyUsage
- subjectAltName
- subjectKeyIdentifier
- authorityKeyIdentifier

☞	**Note** Validation will fail, if an unsupported extension is marked as critical.	☞

4.3.3.4 Signature Algorithms

The following signature algorithms are supported:

- sha1WithRSAEncryption

4.3.3.5 Key Types

The following key types are supported:

- RSA key
    - 1024-bit (default)
    - 2048-bit
    - 4096-bit

4.3.3.6 Signature Request Types

The following signature request types are supported:

- PKCS#10 certification request v1

4.3.3.7 Certificate File Encryptions

The following certificate file encryptions in PKCS#12 files are supported:

- pbeWithSHAAnd128BitRC4 (1.2.840.113549.1.12.1.1)
- pbeWithSHAAnd40BitRC4 (1.2.840.113549.1.12.1.2)
- pbeWithSHAAnd3-KeyTripleDES-CBC (1.2.840.113549.1.12.1.3)
- pbeWithSHAAnd128BitRC2-CBC (1.2.840.113549.1.12.1.5)
- pbewithSHAAnd40BitRC2-CBC (1.2.840.113549.1.12.1.6)

4.3.3.8 Certificate Configuration

Trust list

This list contains the certificates to be accepted for TLS secured connections (e.g. HTTPS, SIPS). You can add either individual endpoint certificates or a CA certificate if you want to accept all certificates issued by that CA.

Remove:	Remove the selected certificate.
Clear:	Remove all certificates from the trust list.
Details:	Click the name of a certificate to view its details.

Download: Download a single certificate by clicking the PEM- or DER-link, respectively.

Download all: Download the complete trust list as a PEM-encoded text file. You can upload that file to another box.

Upload: Select a local certificate file from your computer and press the Upload button to add it to the trust list. You can upload DER, PEM or PKCS#12 encoded certificates. PEM-files may contain multiple certificates. If you want to upload password encrypted certificates (PKCS#12 files only) you have to enter the password before clicking the upload button.

Rejected certificates

This list contains the certificate chains that were rejected before, while trying to establish a secure TLS connection. This happens for example if the certificate is expired or neither the certificate nor any of the issuing CAs is trusted. If one of the certificates should be trusted for future connections you can select and add it to the trust list, directly.

Trust: Add the selected certificates to the trust list and remove the corresponding chains from the rejected certificates.

Clear: Discard all rejected certificate chains.

Details: Click the name of a certificate to view its details.

Device certificate

The device certificate can be used by remote TLS endpoints to authenticate the identity of the device. In general this is not a single certificate but a chain containing the device certificate and the certificates of the intermediate CAs up to the root CA. A TLS connection can only be established if the remote endpoint trusts at least one of their certificates.

Trust: Add the selected certificates to the trust list.

Clear: This button is only displayed if a certificate was installed by the user, before. Click this button to discard the current device certificate and restore the standard certificate.

Renew: This button is only displayed if no certificate was installed by user, before. Click this button to renew the automatically generated standard certificate.

Details: Click the name of a certificate to view its details.

Download: Download a single certificate from the chain by clicking the PEM or DER-link, respectively.

Create new: Click this link to create a new self-singed certificate or certificate request (see below).

Upload: Select a local certificate file and press the "Upload" button. You can upload a single certificate corresponding to the private key of a previously created certificate request in PEM, DER or PKCS#12 format. Instead of that you can upload a complete certificate chain containing the corresponding private key as a PEM or PKCS#12 encoded text file, too. If you want to upload password encrypted certificates (PKCS#12 files only) you have to enter the password before clicking the upload button.

Creating a self-signed-certificate

Click the "Create new" link.

Type: Select "Self-signed certificate".

Key: Choose the bit strength of the key pair. Available bit-strengths are 1024, 2048 and 4096-bit. Optionally you can reuse the current key pair.

Validity: Select the Validity time in years.

Other naming options: There are some other optional naming parameters (Common Name, Organisational Unit, Organization, Locality, State or Province, Country, up to three DNS Names, up to two IP Addresses). You can use them to describe the role of the device within your installation, for example.

Signing request

A certificate signing request contains a public key and an identity. While the corresponding private key is kept secret, the request is being sent to a CA. It will issue an appropriate certificate for the public key after it verified the identity.

Details: Click the name of the signing request to view its details.

Download: Download the signing request by clicking the PEM- or DER-link, respectively.

Remove: Discard the current signing request and the corresponding private key. As an implication certificates for that key cannot be installed, any more.

Creating a certificate signing request

Click the "Create new" link at the device certificate section.

Type:	Select "Signing request".
Key:	Choose the bit strength of the key pair. Available bit-strengths are 1024, 2048 and 4096-bit. Optionally you can reuse the current key pair.
Common Name:	The common name should match with the name of the device. For example, if you access the web interface of the device with https://IP152-6a-52-60, the common name should be "IP152-6a-52-60" or "00-50-c2-6a-52-60".
Other naming options:	There are some other optional naming parameters (Organisational Unit, Organization, Locality, State or Province, Country, up to three DNS Names, up to two IP Addresses). You can use them to describe the role of the device within your installation, for example. Keep in mind that the CA signing the request can modify these parameters according to their policies.

Uploading the response certificate from a CA

See section about device certificate upload.

Application certificates

The application certificates are certificates for specific domains that are used by applications like SIP. The application uses the certificate that matches the own domain. So if you have a PBX with domain "example.com", SIP will fetch the certificate that has "example.com" as its common name.

Trust:	Add the selected certificates to the trust list.
Remove:	This button is only displayed if a certificate was installed by the user, before. Click this button to discard the current application certificate.
Details:	To see details of the certificate the name has to be clicked.
Download:	Download a single certificate from the chain by clicking the PEM or DER-link, respectively.
Create new:	Click this link to create a new self-singed certificate or certificate request (see below).

Upload: Select a local certificate file and press the "Upload" button. You can upload a single certificate corresponding to the private key of a previously created certificate request in PEM, DER or PKCS#12-format. Instead of that you can upload a complete certificate chain containing the corresponding private key as a PEM or PKCS#12 encoded text file, too. If you want to upload password encrypted certificates (PKCS#12 files only) you have to enter the password before clicking the upload button.

Creating a self-signed-certificate

Click the "Create new" link.

Type: Select "Self-signed certificate".

Key: Choose the bit strength of the key pair. Available bit-strengths are 1024, 2048 and 4096-bit. Optionally you can reuse the current key pair.

Validity: Select the Validity time in years.

Other naming options: There are some other optional naming parameters (Common Name, Organisational Unit, Organization, Locality, State or Province, Country, up to three DNS Names, up to two IP Addresses). You can use them to describe the role of the device within your installation, for example.

Signing request

A certificate signing request contains a public key and an identity. While the corresponding private key is kept secret, the request is being sent to a CA. It will issue an appropriate certificate for the public key after it verified the identity.

Details: Click the name of the signing request to view its details.

Download: Download the signing request by clicking the PEM- or DER-link, respectively.

Remove: Discard the current signing request and the corresponding private key. As an implication certificates for that key cannot be installed, any more.

Creating a certificate signing request

Click the "Create new" link at the device certificate section.

Type:	Select "Signing request".
Key:	Choose the bit strength of the key pair. Available bit-strengths are 1024, 2048 and 4096-bit. Optionally you can reuse the current key pair.
Common Name:	The common name should match with the name of the device. For example, if you access the web interface of the device with https://IP152-6a-52-60, the common name should be "IP152-6a-52-60" or "00-50-c2-6a-52-60".
Other naming options:	There are some other optional naming parameters (Organisational Unit, Organization, Locality, State or Province, Country, up to three DNS Names, up to two IP Addresses). You can use them to describe the role of the device within your installation, for example. Keep in mind that the CA signing the request can modify these parameters according to their policies.

Uploading the response certificate from a CA

See section about application certificate upload.

4.4 Main Menu ETH0

4.4.1 Menu Link

This is an option for setting the Ethernet connections. For every ETH interface, automatic settings, transfer speeds (10Mbit/s, 100Mbit/s), full duplex (fdx) or half duplex (hdx) can be defined in various combinations. The PC-Link LAN connection can be blocked. At telephone with a single LAN module the PC link is always disabled. With State= the actual state and with Autoneg= the actual configured mode of the interface will be shown.

In the most cases auto is the best choice for the link setup.

The MDI mode (permutation of receive and transmit) will be selected automatically with the ResistTel IP2 / IP152. Only with the ExResistTel IP2 / IP154 it is possible to setup the MDI mode.

Link	Transfer rate	Duplex Mode	MDI Mode
auto	10/100 Mbit/s (automatic)	full duplex / half duplex (automatic)	(automatic)
10m-hdx	10 Mbit/s	half duplex	(automatic)
10m-fdx	10 Mbit/s	full duplex	(automatic)
100m-hdx	100 Mbit/s	half duplex	(automatic)
100m-fdx	100 Mbit/s	full duplex	(automatic)
10m-mdi-hdx	10 Mbit/s	half duplex	mdi
10m-mdi-fdx	10 Mbit/s	full duplex	mdi
100m-mdi-hdx	100 Mbit/s	half duplex	mdi
100m-mdi-fdx	100 Mbit/s	full duplex	mdi
10m-mdix-hdx	10 Mbit/s	half duplex	mdi-x
10m-mdix-fdx	10 Mbit/s	full duplex	mdi-x
100m-mdix-hdx	100 Mbit/s	half duplex	mdi-x
100m-mdix-fdx	100 Mbit/s	full duplex	mdi-x

Table 17: Link Setups

4.4.2 Menu VLAN

In this menu further general settings are made. In the switch, the ETH packages sent by the device can be prioritised on the second level. To do this, the packages have to be marked correspondingly upon sending. This function must be supported by the used switch.

ID	If the editing field VLAN ID is empty, the value 0 is assumed. The VLAN ID with the value 0 switches off the QoS (Quality of Service) after 802.1Q.
Priority – RTP Data	Should your switch on the gateway port be configured on another VLAN ID, you must input the same value here, in order for the prioritising („Priority") of the Ethernet packages to work. Here, the priority of the VLAN ID for voice data is given in values from zero to seven.

Priority – Signaling	Should your switch on the gateway port be configured on another VLAN ID, you must input the same value here, in order for the prioritising („Priority") of the Ethernet packages to work. Here, the priority of the VLAN ID for signalling data is given in values from zero to seven. By default the priority for signalling is the same as the priority for voice data.

4.4.3 Menu 802.1X

EAP-MD5:

User	User
Password	Password

The State will be displayed also.

4.4.4 Menu Statistics

Via the submenu Statistics you get an overview of all sent (tx) and received (rx) data packages regarding the LAN Link, PC link and CPU Link interface:

tx-good	The number of successfully sent packages.
tx-unicast	The number of successfully sent Unicast packages.
tx-broadcast	The number of successfully sent Broadcast packages.
tx-multicast	The number of successfully sent Multicast packages.
tx-deferred	The number of deferred packages.

tx-collision	The number of colliding packages (max. 16).
tx-excesscol	The number of colliding packages (if tx-collision > 16).
tx-latecol	The number of colliding packages that need too much time to be transmitted. If a collision has been registered after the 512th. Bit of the frame that was to be transmitted, has been reached, a late collision is output.
rx-good	The number of successfully received packages.
rx-unicast	The number of successfully received Unicast packages.
rx-broadcast	The number of successfully received Broadcast packages.
rx-multicast	The number of successfully received Multicast packages.
rx-64	The total number of received packages with max. 64 bytes.
rx-64-127	The total number of received packages with more than 64 to 127 bytes.
rx-128-255	The total number of received packages between 128 and 255 bytes.
rx-256-511	The total number of sent packages between 256 and 511 bytes.
rx-512-1023	The total number of sent and received packages between 512 and 1023 bytes.

rx-1024	The total number of received packages with 1024 bytes.
rx-err	The number of received errors.
rx-dropped-err	The number of Dropped-Error upon reception of data packages.
rx-queue-overrun	The number of Queue-Overrun-Error upon reception of data packages.
rx-crc-err	The number of received CRC checksum errors.
rx-align-err	The number of alignment errors (false driver, defective cable) upon reception of data packages.
rx-too-short	The number of too small data packages during transfer.
rx-too-long	The number of too big data packages during transfer.

Using the link Clear deletes the statistical values.

4.5 Main Menu IP4

In this area,

- general settings of the Internet protocol can be made.
- the VPN protocol PPTP, the DSL protocol PPPoE and the address conversion according to NAT can be configured.

Changing these settings requires the consent of the network administrator.

4.5.1 Menu General

4.5.1.1 Submenu Settings

The TOS (Type of Service) byte inside the IP header is used for prioritization of packets inside the network. The device allows some packets to be marked as higher priority. The TOS values for this purpose are configured here.

TOS priority – RTP Data	If your router is able to set priorities on the basis of the „type of service" (TOS) field, this function can be used for speech packets. By this speech data will be served with priority. The value to be entered here must be aligned with the value of the network router. The value of 0xb8 is default.
TOS priority – Signalling	If your router is able to set priorities on the basis of the „type of service" (TOS) field, this function can be used for signalling packets. By this signalling data will be served with priority. The value to be entered here must be aligned with the value of the network router. The value of 0x68 is default.

☞ **Note**

You may enter the values hexadecimal, octal or decimal. The entries 0x10, 020 and 16 are equivalent. Please note, however, that the value for the TOS field should be identically set on all devices. ☜

Port Ranges	• First UDP-RTP port, Number of ports: These values define, in which area the negotiation of the RTP port shall take place. This is useful if the network is secured by a firewall and only certain ports are to be opened for telephony. As soon as the routers support prioritisation via port number, the port settings can also be used to influence the priority in the network. • First UDP-NAT port, Number of ports: If the VoIP telephone works as a DSL Router, and the internal network works with unroutable IP addresses, Network Address Translation (NAT) is used. With this setting, the NAT service can be limited to certain IP ports.
Local Networks	Here you can declare IP addresses or address ranges to be part of the *local network*. This configuration influences the coder selection process on VOIP endpoints like telephones and physical Gateway interfaces. (See chapter 4.7.1.1 on page 226)
Private Networks	Here you can declare IP addresses or address ranges to be part of the *private network*.

4.5.1.2 Submenu Routing

Here, the routing table of the telephone's current IP configuration is displayed. The table serves error analysis purposes for the administrator of the IP network.

The following parameters are shown in every line:

- Destination Network: IP Address of the Destination Network
- Network Mask: Network mask
- Gateway: IP Address of the next gateways
- Interface: Name of the used interface

- State: State of the interface

4.5.2 Menu ETH0

4.5.2.1 Submenu DHCP

DHCP enables a dynamic management of the IP parameters for a net. A DHCP server manages a pool of addresses and general settings. The VoIP telephones may be used both as DHCP servers and as DHCP clients. Usually, the VoIP telephone is configured as a DHCP client, whereas the DHCP server is available in the network. These settings are automatically assigned to the DHCP client. In the configuration interface of the VoIP telephones, the automatically accepted values are input behind the input templates and therefore do not need to be changed. The device can also be operated with locally and permanently set IP addresses. In this case, the mode must be set to disabled.

Mode	• disabled • client • server • automatic

Mode client:

Selected Server only	Use of specific leases only.
Wait for selected Server	Time to wait for a lease from selected DHCP server before accepting a lease from another server (in seconds).
Server Identifier	Value of manufacturer specific option 250 sent by the server and expected by the client (can be left empty)
Hostname	Hostname to be sent to the server (up to 63 alphanumeric ASCII characters and dashes, case independent)

Mode server:

Probe Address before dynamic Assignment	• disabled • ARP • PING
Reserved and same Vendor Clients only	Use of specific leases only.
Server Identifier	Value of manufacturer specific option 250 sent by the server and expected by the client (can be left empty)

When the telephone is working in DHCP client mode the parameters of the current lease are displayed.

Item	Description
Current Lease from	IP address of the DHCP server
IP Address	IP address of the telephone
Network Mask	Network mask of the telephone
Default Gateway	IP address of the default gateway
TOS Priority	Type of service priority
IP Routing	IP routing
DNS Server 1	IP address of the domain name server 1
DNS Server 2	IP address of the domain name server 2
Domain Name	Domain Name
SYSLOG Server	IP address of the SYSLOG server
TFTP Server	IP address of the trivial file transfer protocol server
Time Server 1	IP address of the first time server
Time Server 2	IP address of the second time server
Timezone String	Timezone string
WINS Server	IP address of the Windows Internet Naming Service server
Node Type	Node Type
Primary Gatekeeper	IP address of the primary gatekeeper
Secondary Gatekeeper	IP address of the secondary gatekeeper
Coder	Name of the coder
Gatekeeper Identifier	Gatekeeper identifier

Item	Description
Dial Tones	Dial tones • 0 – EUROPE-PBX • 1 – EUROPE-PUBLIC • 2 – US • 3 – UK • 4 – ITALY-PBX • 5 – ITALY-PUBLIC • 6 – CZECH-PBX • 7 – CZECH-PUBLIC • 8 – SWEDEN • 9 – FRANCE • 10 – SWISS • 11 – BELGIUM • 12 – NETHERLANDS • 13 – NORWAY • 14 – DENMARK • 15 – GERMANY • 16 – SPAIN • 17 – FINLAND • 18 – AUSTRIA • 19 – IRLAND • 20 – AUSTRALIA • 21 – NEWZEALAND • 22 – MALAYSIA • 23 – TURKEY • 34 – RUSSIA • 35 – SOUTH AFRICA • 36 – BRAZIL
Enblock Dialling Timeout	Enblock dialling timeout
Faststart [0/1]	Faststart option • 0 – disabled • 1 – enabled
Tunneling [0/1]	Tunneling option • 0 – disabled • 1 – enabled
Local Networks	Local Networks

Item	Description
Language	Language of the display of the terminal • ger – German • eng – English • frn – French • dut – Dutch • ita – Italian • swe – Swedish • esp – Spanish • dan – Danish • nor – Norwegian • fin – Finnish • cze – Czech • est – Estonian • por – Portuguese • lat – Latvian • cro – Croatian • pol – Polish
Dialling Location	Dialling location
AM/PM Clock [0/1]	Presentation of the clock • 0 – 24h • 1 – 12h AM/PM
LDAP Directory	LDAP directory
Update Interval [min]	Update interval in minutes
Update Server URL	Update server URL
802.1Q VLAN ID	802.1Q VLAN ID
802.1p VLAN Priority	802.1p VLAN Priority

Caution

The DHCP Automatic Mode should not be used for ‚normal' operation, as an involuntary restart would switch the operating mode.

4.5.2.2 Submenu IP

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

IP Address	The IP-Adresse of the network adapter.

Network Mask	The subnet mask of the network adapter.
Default Gateway	The IP address of the gateway, accepting all IP packages, which do not belong to your own network and are defined by an IP route.
DNS Server	The IP address of the server for the name resolution.
Alternate DNS Server	The IP address of the alternate server for the name resolution.
Proxy ARP	If this switch is set, the telephone responds to ARP requests for all addresses, for which a route has been entered, e.g. for sub-nets via VPN.
Check ARP	Treats a change of MAC address for a cached IP address as ARP poisoning attack.
Broadcast IP Multicasts	Sends IP multicast packets via MAC broadcasts
Static IP Routes:	Manual extensions of the IP routing table. • Network Destination (Zieladresse) • Network Mask (Netzwerk Maske) • Gateway

4.5.2.3 Submenu NAT

In this menu, you make the NAT settings.

Include Interface in NAT	If under IP/ NAT the switch ‚Enable NAT' is set, NAT can be switched on separately for each ETH interface.
Exclude Address / Exclude Mask	Here, certain address areas can be excluded from NAT. In case of one's own official IP address this makes sense for instance if devices in a DMZ (demilitarised zone) are configured on these addresses.

4.5.2.4 Submenu DHCP Server

If ‚Server' mode has been set as the DHCP mode in sub-menu DHCP, the DHCP server can be configured.

All options marked with a ‚*' are manufacturer specific options.

Common DHCP parameter:

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

Address Ranges:

First Address	The IP address, which constitutes the beginning of the address area (e.g.: 192.168.1.100).
Last Address	The IP address, which constitutes the end of the address area (e.g.: 192.168.1.110)

It can be entered more than one address area.

Offer Parameters:

Network Mask	The corresponding network mask regarding the IP address
Default Gateway	The standard-router (e.g.: 192.168.1.1).
TOS Priority	The Type-Of-Service (TOS) value for voice packages.
IP Routing	There is the possibility to add statistic IP routes. These must be input in the form of Address:Mask:Gateway. The elements must be separated from each other by a colon. By ending a route with a ,;', more routes can be added.
DNS Server 1	The primary DNS server address
DNS Server 2	The secondary DNS server address
Domain Name	Domain name that client should use when resolving hostnames via DMS (aka primary DNS prefix)
SYSLOG Server	The SYSLOG server address
TFTP Server	The TFTP server address (based on FTP)
Time Server 1	The first time server address
Time Server 2	The second time server address

Timezone String	Here, new time zones according to IEEE-POSIX standard can be defined and added to the devices by means of a certain character string (e.g.: CET-1CEST-2,M3.5.0/2,M10.5.0/3).
WINS Server	The WINS server address.
Node Type	NETBIOS over TCP/IP name resolution method (e.g. 2 for P-node)
Primary Gatekeeper	The primary gatekeeper IP address. (It will be used for all protocols (H323/SIP/TSIP/SIPS).)
Secondary Gatekeeper	The secondary gatekeeper IP address. (It will be used for all protocols (H323/SIP/TSIP/SIPS).)
Coder	Coder-preference for VoIP telephones. In addition to the preference for the general coder, the preference for the local network coder can be specified here. G729A,60/G711A,30 for example defines G729A as the general coder and G711A as the local network coder. The format is: <General Coder Preference>,<Framesize[ms]>/ <Local Network Code>,<Framesize[ms]>
Gatekeeper Identifier	The VoIP gatekeeper or the gatekeeper ID for VoIP-telephones.

Dial Tones	The dial tone transmitted by VoIP telephones as standard dial tone: • 0 – EUROPE-PBX • 1 – EUROPE-PUBLIC • 2 – US • 3 – UK • 4 – ITALY-PBX • 5 – ITALY-PUBLIC • 6 – CZECH-PBX • 7 – CZECH-PUBLIC • 8 – SWEDEN • 9 – FRANCE • 10 – SWISS • 11 – BELGIUM • 12 – NETHERLANDS • 13 – NORWAY • 14 – DENMARK • 15 – GERMANY • 16 – SPAIN • 17 – FINLAND • 18 – AUSTRIA • 19 – IRLAND • 20 – AUSTRALIA • 21 – NEWZEALAND • 22 – MALAYSIA • 23 – TURKEY • 34 – RUSSIA • 35 – SOUTH AFRICA • 36 – BRAZIL
Enblock Dialling Timeout [s]	Turns on the block dialling for VoIP telephones. Delay in seconds.
Faststart [0|1]	Using the option Faststart [0|1], you can turn the H.323 Faststart procedure on/off. If this option is not defined the default (on) applies. • 0 – disabled • 1 – enabled

Tunneling [0|1]	Using the option Tunnelling [0|1], you can turn the H.245 Tunnelling procedure on/off. If this option is not defined the default (on) applies. • 0 – disabled • 1 – enabled
Local Networks	List of networks where local coder applies (comma separated address:mask pairs, e.g. 127.0.0.0:255.255.255.0,192.168.0.0;255.255.255.0)
Language	For all VoIP telephones, which receive their IP addresses via DHCP, the language defined here is set as their standard language. • ger – German • eng – English • frn – French • dut – Dutch • ita – Italian • swe – Swedish • esp – Spanish • dan – Danish • nor – Norwegian • fin – Finnish • cze – Czech • est – Estonian • por – Portuguese • lat – Latvian • cro – Croatian • pol – Polish

Dialing Location	Defines the various PBX access numbers on VoIP telephones for directory access. This character string must include /cc-, /ac-, /ntp-, /itp-, /col- and /pbx options. Such a character string may look as follows: „/cc 49 /ac 208 /ntp 0 /itp 00 /col 0 /pbx 7“. Options: • /cc – country code • /ac – area code • /ntp – national line (carrier specific) • /itp – international line (carrier specific) • /col – external prefix (pbx specific) • /pbx – root numbers (pbx specific)
AM/PM Clock [0|1]	Activates / deactivates the English time format for VoIP telephones. German time format is displayed as standard: „dd.mm.yy hh:mm, 24 hour-clocks“. If a 1 is input in this field, the English time format „mm/dd hh:mm xm, 12-hour am/pm clock“ is displayed.
LDAP Directory	To allocate a functioning LDAP configuration to all VoIP devices integrated via DHCP, a configuration character string can be entered in the LDAP Directory field. You obtain this configuration character string by executing the following command in the browser of a configured device: "<IP-Adresse of the VoIP device>/!mod cmd PHONEDIR0 ldap-config". When this command has been executed, a configuration character string is output in the browser, which you copy and paste into the LDAP Directory field of the DHCP server. In this way, all further devices are given a correct LDAP configuration.
Update Interval [min]	All devices participating via DHCP receive the value that is entered here, in the Interval [min] field of the Update server.
Update Server URL	All devices participating via DHCP receive the value that is entered here, in the URL field of the Update server.

802.1Q VLAN ID	The configuration at the switch must be observed for setting the VLAN ID. An empty 802.1q VLAN ID field (16 bit) assumes the value 0. The VLAN ID with the value 0 switches QoS (Quality of Service) off according to 802.1q ab. If the switch at the port to the device happens to be configured to a different VLAN ID, the same value must be specified here to allow a prioritisation from the Ethernet. To be able to distinguish between the VLANs, the Ethernet packet is extended by 4 bytes, of which 12 bits are intended for the inclusion of the VLAN ID, making 4094 VLANs possible (VLAN ID 0 and 4095 are reserved or invalid).
802.1p VLAN Priority	In the 802.1p VLAN Priority field (3 bit), the associated VLAN priority level (a value between 0 and 7) can be specified, in order that voice data is given priority forwarding, for example.

Note

A device cannot work as a NTP Server. Information transmitted to other devices via DHCP, in these devices cannot be overwritten by a local configuration.

4.5.2.5 Submenu DHCP Leases

VoIP devices that have used this interface to fetch an IP address of the embedded DHCP server, are displayed here.

- Clicking once on the Type dynamic of a displayed lease enables you to change the dynamic lease into a reserved lease and at the same time to define a host name or release the lease.

- Clicking once on the Type reserved of a displayed lease enables you to release the reserved lease.

In addition, in chapter Reserve IP Address, you have the possibility to assign a certain IP address to a certain MAC address. In the Cleanup chapter assigned DHCP leases can be deleted again.

- Clicking once on Clear dynamic leases deletes all dynamically assigned leases.

- Clicking once on Clear reserved leases deletes all reserved leases.
- Clicking once on Clear all leases deletes all assigned leases.

IP Address	The assigned IP address of the DHCP lease.
MAC Address	The MAC address of the participating VoIP device.
Acknowledged	The date on which the DHCP lease was assigned.
Expires	The date on which the DHCP lease will expire.
Type	The type of DHCP lease. Dynamic or Reserved.
Host name	The host name of the participating VoIP device.

Furthermore IP addresses can be reserved for special MAC addresses. The fields IP address and MAC address have to be specified. A host name can be specified optionally. An IP address out of the range can be reserved activating the button Allow Out Of Range. To complete the reservation the button **Reserve** has to be pressed.

4.5.3 Menu PPP

4.5.3.1 Submenu Config

Here, you set the parameters for the DSL and VPN connections. A list of all possible PPP interfaces with their respective Name (if configured) and the state (up/down/etc) is displayed here. The PPP interfaces may be PPP over ISDN, PPP over Ethernet (PPPoE, used for DSL connections), or PPTP (VPN).

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

Enable	The connection via the interface is activated.

Connection port	• None • PPPOE: A connection for the DSL provider is established. ➢ DSL Provider (Access Concentrator): Access password preset by the DSL provider • PPTP: A connection to the company is established. ➢ Server Address: IP-address of the PPTP server ➢ Route to Interface: Interface, via which this connection shall be established. ▪ none ▪ ETH0 ▪ PPP0 ▪ PPP1 ▪ PPP2 ▪ PPP3 ➢ Enable Encryption: Encryption according to Microsoft Packed to Packed encryption (MPPE). This is recommended if the distant end has been provided by a product of certain companies. ➢ Stateless Operation: The costs per package of encryption are strongly dependant on the agreed transfer mode (stateless/ stateful). The „stateless mode" is less prone to packet loss, but requires, on the other hand, a new calculation of the key for each packet. In case of packet loss, the „stateful mode" requires a resynchronisation between sender and receiver. On the other hand, the key is calculated anew only every 256 packets.

	➢ 40Bit: Key length 40 bits for data encryption. ➢ 128Bit: Key length 128 bits for data encryption.
Descriptive name	The name of the interface
Bandwidth (kBit/s)	Limits the transfer speed of the connection (PPTP and PPPOE) to the value to be entered here.
Maximum transfer unit (Bytes)	Here, the maximum size of the IP packet is limited. The default MTU values are: • PPPoE - 1492 • PPTP – 1436
IP address for remote party	If the distant end does not assign an IP address, here you may define your own IP address in the remote IP net.
Automatic dial after boot	Immediately after booting, attempts are made to establish the connection.
Restart Time (hour:min)	Time of day when the connection should be restarted to overcome the 24-hour provider disconnect
Allow inbound connections	Allows requests for inbound connections from the remote IP net.
No DNS on this interface	DNS server configurations are ignored.
Exclude interface from NAT	The Network Translation is executed as long as this IP address does not appear.

Adapt to Cisco PPP peers	Try the Adapt to Cisco PPP peers option, if a Cisco router is used at the remote location and problems arise in the transmission of voice data.
Authentication	• Outbound: Combination of user name and password stored at the distant end for connection authentication. • Inbound: This option is required only if the switch "Allow inbound connections" has been set. The authentication of the distant end is preset, in order for the connection request to be accepted.
Always keep Routes active	To force connections to a private network over this interface the routes to be kept active in routing table even if the interface is down.
IP Routes	Further required IP routes for the newly established connection.

4.5.3.2 Submenu State

The state of all telephone's DSL and VPN connections are displayed. It is also possible to shut down the connections manually and re-establish them.

Interface	PPP0 to PPP3
Address	IP-address of the connection
Type	PPTP for VPN or PPPoE for DSL
State	up, down, connecting, disconnecting, disable, idle

Since	Here, the time is given, since when the connection has been active.
Action	• enable • disable • connect: Manual establishment of the connection • clear: Manual disconnection • info: further information
Name	Your name for the connection.

The function Info below the menu item Action can be used to fetch the following information:

Interface	Interface name
Name	Name of the connection
Address	IP address
Type	PPPoE / PPTP
State	Up / down / idle (state active or inactive) since date / time
Bandwidth	Bandwidth
Maximum Transfer Unit	Maximum Transfer Unit

Remote User	Remote User
Remote Peer	Remote Peer
Remote Address	Remote IP Address
Local User	Local User
Local Address	Local IP Address
Primary DNS	Primary DNS Server
Secondary DNS	Secondary DNS Server
Last Disconnect Cause	Last Disconnect Cause

4.5.4 Menu NAT

4.5.4.1 Submenu General

If the device is used as a router, it is possible to connect IP terminals from the network with a non-public address to the public Internet. For this, **NAT** (Network Address Translation) is necessary. Additional configuration is required on the different IP interfaces (e.g. ETH, PPP, etc.) to define on which interfaces the public and on which interfaces the private network is accessed.

Enable NAT	The Network Address Translation for SIP and non-VoIP will be activated.

Note

This function is necessary only if the VoIP telephone simultaneously is a DSL router.

Further settings serve the inbound connections.

Default forward destination	Standard IP address for inbound connections
Port specific forwardings	Here, in order to address several internal targets, various port numbers are assigned to IP addresses of the internal network. • Protocol: UDP/TCP • Port: IP-Port • Address: IP-Address • Int. Port (optional)

4.5.4.2 Submenu H.323

The telephone is capable of connecting IP network terminals having non-public addresses with the public Internet. This requires a "Network Address Translation" (NAT). The necessary parameters for H.323 connections of this configuration can be set here.

Enable H.323-NAT	The Network Address Translation for the H.323 protocol is activated.

Note

This function becomes necessary only if the VoIP telephone simultaneously is a DSL router, and if, in case of at least one registration, the H.323 protocol is used.

Require authentication for inbound RAS	A checked checkbox requires H.323 authentication.
H.225 / RAS destination	IP address of the server in the private network, to which incoming H.225/RAS messages are routed.
H.225 / Signalling destination	IP address of the server in the private network, to which incoming H.225/signalling messages are routed.

All registered users (Registered Clients) and the currently active calls (Active Calls) are still being displayed.

4.6 Main Menu IP6

The default local network IPv6 address is assembled as follows:

64-bit prefix: fe80:0000:0000:0000/64

The EUI-64 part of the IPv6 address will be derived from the MAC address of the device:

Die MAC address for this example is: 00:50:C2:6A:50:27.

		0	8	16	24	32	40	48	
		00	**50**	**C2**	**6A**	**51**	**27**		
		00000000	10010000	11000010	01101010	10010000	00100111		
		Organizationally Unique Identifier (OUI)			**Device Identifier**				
	0	8	16	24	32	40	48	56	64
1. Split MAC Address	00000000	10010000	11000010			01101010	10010001	00100111	
2. Add "FFFE" bit pattern to middle 16 bits	00000000	10010000	11000010	11111111	11111110	01101010	10010001	00100111	
3. Change bit 7 to 1	00000010	10010000	11000010	11111111	11111110	01101010	10010001	00100111	
Modified EUI-64 identifier in hexadecimal notation	**02**	**50**	**C2**	**FF**	**FE**	**6A**	**51**	**27**	
IPv6 Identifier in colon hexadecimal notation	**0250:C2FF:FE6A:5127**								

Figure 193: Converting IEEE MAC addresses to IPv6 modified EUI-64 Identifiers

Die complete local default network address for this example is:

fe80:0000:0000:0000:0250:C2FF:FE6A:5127

4.6.1 Menu General

4.6.1.1 Submenu Routing

Here, the routing table of the telephone's current IP configuration is displayed. The table serves error analysis purposes for the administrator of the IP network.

The following parameters are shown in every line:

- Destination Network: IPv6 Address of the Destination Network
- Gateway: IPv6 Address of the next gateway
- Interface: Name of the used interface
    - LOCAL
    - ETH0
- State: State of the interface
    - up
- Flag
    - none
    - P

4.6.2 Menu ETH0

4.6.2.1 Submenü IP6

The manual IPv6 configuration settings are effective if the address configuration is set to static. Right to the input field always the stored setups will be displayed.

Address Configuration	• Automatic • Static
IP6 Address	IPv6 address of the telephone (128 bit)
Prefix	Number of bits of the prefix
Default Gateway	The IPv6 address of the gateway taking all IP packets not belonging to the own network and being defined with a route.
Router Interface	Interface is router. Replies Router Solicitations with Router Advertisements, publishes routes and forwards packets.
Proxy ND	Replies to Proxy Neighbour Discovery requests if for required IP6 address an active route exists. Such addresses will appear 'local' to the queuing device.
Static IP6 Routes:	Manuel extensions of the IPv6 routing table • Destination • Gateway

4.6.2.2 Submenu Address

In a table the available IPv6 addresses are displayed. An item has the following parameter:

Address	IPv6 address

Scope	• 0x1 • 0x2 • 0xe
Type	• mcast (multicast address) • linklocal (link local address) • mcast/solicit (multicast/neighbour solicitation) • global (global address)
State	• <empty entry> • valid-preferred
Preferred	• infinite
Valid	• infinite
Flag	• none • E (EUI64) • M (manual) • P (router)

4.6.2.3 Submenu Router

In a table the received Router Advertisements are displayed. An item has the following parameter:

Received	Received

Address	IPv6 Address
Prefix	Prefix of an IPv6 Address
Valid	Valid
Preferred	Preferred
Hoplimit	Hop limit, the number of network segments on which the packet is allowed to travel before being discard by a router. The hop limit is set by the sending host and is used to prevent packets from endless circulation on an IPv6 internetwork. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop limit is 0.
R.Lifetime	The router lifetime is a 16 bit integer value, describing the time in seconds a router should remain in the default router list. The maximum value is 18,2 hours. A value of 0 indicates that the router is no default router and should not be stored in the default router list.
Reachable	Reachable
Retrans.	Retransmission
MTU	Maximum Transmission Unit
Flag	

4.6.3 Menu 6to4

4.6.3.1 Submenu Config

The IPv6 to IPv4 interfaces can be configured here. In a table the following parameter will be displayed:

Interface	• 6TO4-00 • 6TO4-01
Name	Name

Clicking on an interface, a new window will be displayed.

The following input fields are available for an interface:

Enabled	enabled
Descriptive Name	name of the interfaces
Destination IP4 Address	IPv4 destination address
Source IP4 Address	IPv4 source address

Additional static IPv6 routes can be entered consisting of the following parameters:

Destination	IPv6 destination address
Gateway	IPv6 gateway address

After entering a route it is necessary to click at the OK button to take over the data. The data will be taken over and the window will be closed. Wit the next call of the same interface, there will be the possibility to enter an additional IPv6 route.

4.6.3.2 Submenu State

A table with the main parameters and states of the IPv6ToIPv4 interfaces will be displayed.

For each interface the following parameter will be displayed:

Interface	• 6TO4-00 • 6TO4-01
Name	Name of the interface
Destination	IPv4 destination address
Source	IPv4 source address
State	• Down • Up
Route	All IPv6 destination addresses

4.7 Main Menu Phone

4.7.1 Menus User-1 to User-6

The telephone has been designed for multiple registrations. Up to six different registrations can be stored in one VoIP telephone. Each registration must be configured in a separate item of the main menu. (User-1 to User-6)

4.7.1.1 Submenu General

Here the parameters are input for logging into the PBX. These parameters are preset by the administrator of the telephone system.

Enable	Here the registration (user) will be enabled. Registration 1 is always enabled.

First, the required protocol must be chosen for registration. You have the choice between the protocols H323, SIP, TSIP and. SIPS. The corresponding parameters are automatically adapted to the selected protocol.

Protocol H323:

Primary Gatekeeper Address	Here, the IP address is input, under which the first responsible gatekeeper can be reached.
Secondary Gatekeeper Address	If the first gatekeeper cannot be reached, for security purposes there should be another gatekeeper in the network. The IP address of this gatekeeper should be entered here.

☞ **Note**

If no gatekeeper address is defined and the protocol is set to H.323, then the telephone will search for a gatekeeper via the gatekeeper recovery. ☞

Gatekeeper Identifier	If several gatekeepers are to be active on one address, among these a certain gatekeeper is identified on the basis of the name that is to be entered here.
Number	Telephone numbers that are required for the registration are entered here.

Name	The name that is to be entered here is required for the registration only if the number has not been entered.
Local Endpoint Address	If several IP addresses are configured on this VoIP telephone, this option enables you to specify the IP address, on the basis of which the logon at the gatekeeper should follow.

☞	**Note** Because the VoIP telephone has preset the local IP address on the basis of the IP routing table, the value is required only in exceptional cases.	☞

Protocols SIP, TSIP, SIPS:

Domain	The domain of the provider, which can be found after the ‚@' of the URI, can be entered instead of the IP address. The default port for the registration of the protocols SIP and TSIP is 5060 and fort he protocol SIPS 5061. If this port shall be changed, the items Primary/ Secondary Server Address should be left empty and in this field should be entered IP Address:Port Number.

Note

If the protocol SIPS is selected, the domain name of the registration of the telephone must be the same as the parameter CN or Subject Alternative Name of the device certificate of the PBX.

If this is not the case, then you have to get a certificate accordingly or if the security requests or not so high you can generate a certificate by yourself. This certificate must be installed at the PBX and if necessary in the trust list of the telephone.

Furthermore there is a possibility to suppress this check with the SIPS protocol option 'No Certificate Check' (see chapter 4.11.45 on page 371).

If there are any problems with the protocol SIPS, then these values must be verified with the web interface of the telephone.

CGPN	The calling party number to be used on outgoing calls.
User ID	The User ID (number or name) corresponding to the part in front of the @ in the URI, should be entered here.
Proxy	IP address or domain name, under which the responsible SIP server can be reached.
Alternative Proxy	If the first SIP server cannot be reached, for security purposes there should be another one in the network. The IP address or domain name of the alternative SIP server can be entered here.
STUN Server	The IP address or domain name must be configured, if the telephone uses a non-public IP address, whereas the server, however, can be reached under a public IP address. The value is given by the SIP provider or administrator.

☞	**Note** If a domain name is defined, a DNS server must be configured and must be reachable. The DNS server must be able to solve the name.	☜

The following authorisation parameters can be adjusted independently of the protocol. These parameters are automatically negotiated when a connection is established. A change is necessary only if the gatekeeper / server makes certain demands regarding the connection protocol.

Username	(Only for protocol SIP, TSIP and SIPS) In some SIP registrations, authorising a separate user name is required. In all other cases, the field should be left empty.
Password	The registration requires a password, which can be agreed upon in this option.
Retype	This is a security question for the password.

The following options are in depended of the protocol:

Dial Tones	In some countries, the dial tones vary. Here, the preset are defined corresponding to the specific country and area of operation (PBX, public network, etc.). • 0 – EUROPE-PBX • 1 – EUROPE-PUBLIC • 2 – US • 3 – UK • 4 – ITALY-PBX • 5 – ITALY-PUBLIC • 6 – CZECH-PBX

	• 7 – CZECH-PUBLIC • 8 – SWEDEN • 9 – FRANCE • 10 – SWISS • 11 – BELGIUM • 12 – NETHERLANDS • 13 – NORWAY • 14 – DENMARK • 15 – GERMANY • 16 – SPAIN • 17 – FINLAND • 18 – AUSTRIA • 19 – IRLAND • 20 – AUSTRALIA • 21 – NEWSEALAND • 22 – MALAYSIA • 23 – TURKEY • 34 – RUSSIA • 35 – SOUTH AFRICA • 36 – BRAZIL

Enblock dialing timeout [s]	The VoIP telephone supports single digit dialling. This means that the digits are being sent consecutively, until the number is complete, after which the connection is automatically established. If the exchange or telephone system does not support single digit dialling, entering a time value in this field can switch the dialling procedure to block dialling. Then, after each digit entry, the time is measured. Only after the time is expired, all currently entered digits are sent en bloc in order to establish the connection. After entering all digits, the waiting time after the last entered digit can be cut by entering the digit #. The before entered calling number (without the digit #) will be dialled immediately. If this parameter is set, then the digit # can't be used as part of the calling number.
General Coder Preference	The protocols for the speech compression (for external calls) are listed in this parameter. Here, you can set the desired coder. You can choose between: • G711A (ISDN Europe) • G711u (ISDN North of America, Japan) • G729A
Framesize [ms]	For General Coder Preference: The package sizes are automatically negotiated with 60 ms. This parameter enables the determination of another RTP package size.
Silence compression	For General Coder Preference: Taking the VoIP telephone as the starting point, in case of silence (no conversation), no packages are sent.

Exclusive	For General Coder Preference: This parameter allows no negotiation, but accepts only the preset parameters.
Local Network Coder	The protocols for the speech compression (for calls in local networks (internal calls)) are listed in this parameter. Here, you can set the desired coder. You can choose between: • G711A (ISDN Europe) • G711u (ISDN North of America, Japan) • G729A
Framesize [ms]	For Local Network Coder: The package sizes are automatically negotiated with 30 ms. This parameter enables the determination of another RTP package size.
Silence compression	For Local Network Coder: Taking the VoIP telephone as the starting point, in case of silence (no conversation), no packages are sent.

Secure RTP	Selection of the encrypted speech data • <empty item> (no encryption) • AES128/32 (AES encryption, key length 128 bit, 32 bit SHA1 Hash message) • AES128/80 (AES encryption, key length 128 bit, 80 bit SHA1 Hash message) • AES192/32 (AES encryption, key length 192 bit, 32 bit SHA1 Hash message) • AES192/80 (AES encryption, key length 192 bit, 80 bit SHA1 Hash message) • AES256/32 (AES encryption, key length 256 bit, 32 bit SHA1 Hash message) • AES256/80 (AES encryption, key length 256 bit, 80 bit SHA1 Hash message)
No DTMF Detection	DTMF tones are sent in-band through the media channel but not as separate signalling messages.

SIP Interop Tweaks (only Protocols SIP, TSIP und SIPS):

Proposed Registration Interval [s]	Proposed registration interval in seconds
Accept INVITE's from Anywhere	Accept invite's from anywhere
Put Consultation Call on Hold before Transfer	Put consultation call on hold before transfer

Before configuring the second or following registrations, the corresponding registration should be made possible through 'enable'. By deactivating ‚enable', the complete registration can be cancelled, whereby the loss of the parameters is ruled out.

Note

If a device is updated from an older software version and is configured to one of the protocols SIP, TSIP or SIPS or the protocol is changed from H323 to SIP, TSIP or SIPS and neither proxy nor alternate proxy are configured, then the at gatekeeper address configured IP address will be used for the registration at a SIP server.

If the gatekeeper or alternate gatekeeper address will be sent via DHCP to the device, then this address will be used independent of the configuration of the gatekeeper in the device and independent of the selected protocol.

If a gatekeeper address is defined as domain name via DHCP, then this is not working with the protocol H323 and not working with devices with older software versions.

4.7.1.2 Submenu Preferences

Here you can make individual settings for the user.

Language	The dialog language for the telephone display. • German (Deutsch) • English (English) • French (Francaise) • Dutch (Nederlands) • Italian (Italiano) • Spanish (Espanol) • Swedish (Svenska) • Danish (Dansk) • Norwegian (Norsk) • Finnish (Suomi) • Czech (Cestina) • Estonian (Eesti) • Portuguese (Portugues) • Latvian (Latvieou) • Croatian (Hrvatski) • Polish (Polski)
Time Format	The date and time format that can be found in the bottom line of the telephone display. • dd.mm.yy hh:mm • mm/dd hh:mm AM/PM

Call Waiting	In case of an inbound second call, there are different Call Waiting signals: • enabled – default tone: • enabled – beep once: a short notification tone occurs • enabled – silent: no notification tone, visible in the display only • disabled: no notification
Hide own Number	Telephone number suppression for outbound calls
Enable Call Intrusion	The Call Intrusion feature is enabled.

Announcement Calls	The Announcement Call feature is configured here.
	• Incoming
	  ○ **Reject**: Block inbound announcement calls.
	  ○ **Reject, if busy**: Block inbound announcement calls, if busy.
	  ○ **Micro On**: Turn on microphone for incoming announcement calls.
	  ○ **Audible Signal Off**:
	  ○ **Treat any Call as Announcement**: Every incoming called is automatically connected in hands free mode with switched off microphone, if the muting isn't cancelled with "Micro On".
	  This feature makes it possible to make announcement calls from telephones, which don't have the needed function keys.
	  Usefully, a registration will be used with a special number for such calls.
	• Outgoing
	  ○ **Allow:** Enable announcement sending

Ring Tones	For internal and external inbound calls, returned calls, offered calls, announcement calls, multicast announcement calls, messages and do not disturb calls various ringing tones, speeds and volumes can be set. The ringing tones are listed under „Administration / Phone / Ring Tones" (Refer chapter 4.7.2 on page 271) can be played back on the telephone, and in addition, more ringing tones can be downloaded. The speeds can be changed for the standard tones only. For announcement calls, multicast announcement calls, messages and do not disturb calls the duration can be selected. For announcement calls, multicast announcement calls and messages the ring tones will be played only, if the option Play Configured Ring Melody before Automatically Connecting an Announcement Call is set at Administration/Phone/Preferences.
Ring Filter	For five separately entered telephone numbers (e.g. VIP numbers), further special ringing tones can be defined. • Number: Incoming telephone number the ringing tone can be assigned to. • Name: The incoming names can be assigned to the ringing tone instead of the telephone number. • Type: It is possible to further specify the filter. ➢ any: all possible targets are evaluated ➢ external: During evaluation of the filter, only calls from external senders are considered. ➢ group: Here, especially in case of diverted calls the number of the call diversion for the filter is used, and not the sender information. • Volume: The volume of a defined ringing tone can be determined in 11 steps. • Melody: Here, you select the name of the melody to be played.

Do Not Disturb	In case of the Do Not Disturb feature, you can set the response and the type of call.
	• Action
	  ○ do not ring: The telephone does not ring.
	  ○ ring once: The telephone is ringing once.
	  ○ reject call (busy): Reject the inbound call using a busy signal.
	  ○ ignore call (no response): ignore the call.
	  ○ out of office (ignore call and send absence message)
	• Apply to
	  ○ any call (for any call)
	  ○ external calls (for external calls only)
	  ○ internal calls (for internal calls only)

Message Text	The out of office message can be entered here (only if action is set to out off office).

Favorite Diversions	Three different call diversions can be set. Here, the telephone numbers and names can be set. Call diversions must be set on the device.
	
	• Always: All calls are diverted.
	  ○ Number: Telephone number the incoming call can be diverted to.
	  ○ Name: As an alternative to the telephone number, you can enter the name the call should be diverted to.
	
	• Busy: If busy, the incoming call is diverted.
	  ○ Number: Telephone number the incoming call can be diverted to.
	  ○ Name: As an alternative to the telephone number, you can enter the name the call should be diverted to.
	
	• No Response: If the incoming call after a certain amount of time is not answered, the call will be diverted.
	  ○ Number: Telephone number the incoming call is diverted to.
	  ○ Name: As an alternative to the telephone number, you can enter the name the call should be diverted to.

4.7.1.3 Submenu Call-Lists

The list of inbound and outbound calls can be stored on your own telephone. This option can be enabled activating Enabled.

4.7.1.4 Submenu Directories

This menu lists the three cases, in which the telephone can access telephone books.

Local Enable	A private telephone book can be created and used on the device itself.
PBX Enable	Furthermore, all users of the PBX can be made available as telephone book entries. The feature must be supported by the current PBX. • **Use TLS**: The connection to the PBX will be a scrambled TLS connection. • **Username:** User name required for login, stored at the PBX. • **Password + Retype**: The password corresponding to the user name.
External LDPA Server Enable	In addition, an external database may be used as a telephone book via the LDPA protocol. You can enter the LDPA access parameters for the external telephone book here. • **Server:** IP address of the LDAP server • **Port:** Fitting port to the IP address • **Username:** User name for authentication at the LDAP server • **Password + Retype:** The password that fits the user name.

The following parameters are required for searching within the external database.
For further details, please contact the administrator of the external database.

- **Search base**
- **Mode: basic, paged results, virtual list views**

- **Object Filter**
- **Sort Results (by 1st LDAP name attribute)**
- **Name Attributes**
- **Number Attributes**
- **H323 ID Attribute**
- **Hold Server Connection (default 5 seconds)**

Dialing Location	In order to convert the telephone numbers extracted from the databases to telephone numbers than can be dialled, the parameters of your own connection must be made known. • **Country Code:** Own country code without preplaced digits or special characters • **Area Code:** own area code / prefixes • **National Line (carrier specific):** Digit sequence to obtain a national line • **International Line (carrier specific):** Digit sequence to obtain an international line • **External Line (pbx specific):** Digit sequence to obtain a line of a PBX. • **Subscriber Numbers (pbx specific):** For the conversion of completely available, internal numbers, you can enter the telephone number stem here, which shall be omitted for internal dialling of the telephone number.

4.7.1.5 Submenu Function-Keys

The following functions can be assigned to function-keys. On a telephone with a 21 key keypad, you have 10 function keys. To get the function keys (F1 – F10) you have to press the key # for more than a second (shift function) and than to press a digit key (1 – 9, 0). You don't have a lamp or a display field in the phone display for any function-key.

On a telephone with additional input lines, you can connect additional keys. Depending on the configuration of the additional input lines up to 10 further function-keys will be available.

- <empty item>
- Dial
- Partner
- Park
- Pickup
- Message Waiting
- Call Forwarding
- Join Group
- Search Directory
- Enable Registration
- Activate Registration
- Do Not Disturb
- Call Waiting
- Hide Own Number
- Transfer
- Redirect
- Lock
- Headset
- Hot Desking
- Create Registration
- Delete Registration

- Switch
- Recording
- Boolean Object
- Presence
- Prepare Override
- Toggle
- Message
- Spare

4.7.1.5.1 Function Keys General

General setup of a function key:

Disable Modification on Phone	With activation of this option this function key will be locked for modification on the phone.

In general, there are two different kinds of function keys, which can take on the conditions 'idle state' or 'active state', respectively:

1. Function keys that are assigned to the telephone display, can be defined with the parameters Text or Icon, according to the particular state.

Text	Here, you enter the text to be shown in the display beside the function key. The text can be freely chosen and may consist of 20 characters per function key.
Icon	Alternatively, an icon (a symbol) can be shown in the display. The assignment of graphics to names is described in the following table „Icon Definition"

2. Function keys with an LED indicator can be assigned to the states:

    - off
    - blink
    - flicker
    - on

Symbol	Icon	Symbol	Icon
	empty item		Headset
	Key		Loudspeaker
	Divert		Bell-crossed
	List		Bell-white
	Letter		Bell-black
	Letter-black		Onhook
	Sunglasses		Offhook
	Glasses		Mask- white
	Cup-op-coffee		Mask- black
	Handset-rope		Smiley
	Handset-flat		Face
	Handset-right		Right-arrow
	Handset-left		Callback

Figure 194: Icons

For programming a function-key a new sub-window will be opened. On the bottom of each sub-window there will be different buttons:

OK Button:

The data in the sub-window will be sent to the telephone and the sub-window will be closed.

Cancel Button:

The sub-window will be closed without sending the data in the sub-window to the telephone.

Apply Button:

The data in the sub-window will be sent to the telephone and the sub-window will be kept open.

4.7.1.5.2 Delete Function Key (<empty item>)

A function key can de deleted by selecting by selecting the type to the empty item. Afterwards a security question appears to delete the function key. The question has to be answered with OK to delete the function key. With Cancel it will be aborted to delete the function key.

4.7.1.5.3 Function Key Short Dial

This function enables the user to assign a number to a function key in such a way that the function key can be used to call a distant end directly.

The following configurable parameters are at the user's disposal:

Number	Remote party number and/or DTMF digits. A comma (,) can be used to insert a 300ms pause between the digits. This is useful e.g. for destinations accepting DTMF after connect. If the destination shall be stored as IP address, the IP address has to be entered into the field name und the field number has to be empty.
Name	Remote party name (H323 ID).

Prepare	This is a set option, under which the connection is not immediately established, but which serves as dialling preparation in the sense that the number can be completed by further digits. Only as a consequence of subsequent actions, like picking up the receiver or turning on the enabling device, the number is dialled.
Announcement	Set up an announcement call, i.e. a call which should be automatically accepted by the called phone. This checkmark is only effective if **Allow Outgoing** for Announcement Calls is checked on the **Phone->User-x->Preferences** page of the registration. Further **Reject Incoming for Announcement Calls** must not be checked on the **Phone->User-x->Preferences** page of the called phone.
Send in Active Call	Send the digits configured under `Number´ as DTMF digits if there is an existing connection already. If the phone is idle set up a call as usual.
Send as Control Call	Set up a control call to a special PBX object, for example to control special voice mail features. For a control call no media channel is established.

4.7.1.5.4 Function Key Partner

The partner function is subdivided into three states.

Idle	In this idle state, the key performs direct dialling.
Alerting	This state indicates that the partner telephone rings, and you can use this key to answer the call (pick-up).
Busy	In case the line is busy, the function key indicates the partner state only.

In „Partner Identification", the partner telephone is defined with the corresponding number and name.

Caution

The PBX must support the feature, both telephones must be in a common group, and the partner functions must be enabled.

Note

The described functions can only be used if both users (the assigning and the assignee) belong to the same group. The same group is selected in the PBX.

Additional the following options are selectable.

Number	Number for partner identification
Name	Name for partner identification
Partner Type	• Default • Executive • Secretary
Subscribe for Dialog Info	Subscribe for Dialog Info
Subscribe for Presence	Subscribe for Presence

Perform Intrusion if Partner is busy	Send Intrusion call to busy partner. When this feature is active, you can select the type of the call. • Not active • Conference • Silent Monitoring
Hide calling Party in alerting State	Hide calling party in alerting state
Hide calling Party in ringback State	Hide calling Party in ring back state
Show connected Party in busy State	Show connected party in busy state
Do not pick up an alerting Call	Do not pick up an alerting call
Audible Signal after alerting [sec]	Delay for audible signal after alerting in seconds

4.7.1.5.5 Function Key Park

This function can be used to park a call. The following parameter can be selected:

Number	The number of the PBX object to be used (Trunk Line, Waiting Queue ..., for a Trunk Line the number should be specified).
Name	The name of the PBX object to be used (must be left empty if a number is specified).

Position	The park position associated with this key. Usually 0 for the first Park key, 1 for the second and so on.
Trunk Line	Trunk line
Hide parked Party	Do not display the parked party of a call (by default both the parked and the active party are displayed)
Hide Foreign Connections	Do not display foreign connections
Audible Signal after parking [sec]	An audible signal is triggered if any of the monitored calls is parked longer than the given number of seconds.

4.7.1.5.6 Function Key Pickup

Within a group, an incoming call can be picked up by a participant, whereby the telephone number is shown in the display. If several participants of the group are being called, a list of calls is generated, enabling the participants to choose in advance which call to pick up.

Hide calling Party	Hide calling party
Audible Signal after alerting [sec]	Delay for audible signal after alerting in seconds

4.7.1.5.7 Function Key Message Waiting

In order to get into the Message Center, you need the access data, which are defined on the basis of the telephone number and the name. Optionally you can append your own number to the message center account number.

If no messages are present, you may play back old messages (state 0) or for instance rephrase the announcement. In state 1 you may listen to the new messages.

Number	Calling number of the message center
Name	Name of the message center
Append Own Number	Append own calling number to the dialled number
Global	Broadcast MWI to all registrations on the same gatekeeper. This function is used when the voicebox of other registrations is monitored for MWIs. To monitor the MWI of another registration, you need a second registration for the respective user at the phone. This second registration needs also a MWI - function key. The 'Global Flag' must be activated on this second registration MWI - key. By this when MWI - message is received, the 'Global Flag' will ensure that the status change is communicated and displayed also at the first (main) registration.
DTMF	Send DTMF tones as configured for the registration (Default), via signalling messages (Outband) or as in band tones (Inband). • Default • Outband • Inband

4.7.1.5.8 Function Key Call Forwarding

This function allows incoming calls to be diverted. Four active states (1 – 4) with different destinations can be configured (for example, mobile phone, voicemail), which are offered in succession. In each of these states, the following options can be used. In state 0 the function call forwarding is inactive:

Apply 'Always' Setting Only	The setting is applied for a permanent call diversion only.

In each of these active states, the following options can be used:

Always	This indicates a permanent call diversion.
Busy	The call diversion is activated if one's own telephone is busy.
No Response	The call diversion is activated after a delay, e.g. four rings.

4.7.1.5.9 Function Key Join Group

Using this function, a user can log on or off the call distribution of a collective line group. For registration the name will be necessary for the group identification.

Group Identification:

Name	Name of the group identification

4.7.1.5.10 Function Key Search Directory

This function can be used for searching for entries in the telephone book. For searching parameters can be selected:

- Combined Directories: All subscribers combined from the three next search criteria.
- Local Directory: All subscribers stored in your IP telephone.
- PBX Directory: All subscribers of the telephone system you are registered with.
- External Directory: All subscribers connected on an external database via the LDAP protocol.

4.7.1.5.11 Function Key Enable Registration

Using this function, a user (registration) is enabled or locked. If the user was the active user, the previous user automatically becomes the active user.

You can specify an "active user". Outgoing calls are made under the user's parameters, and the function keys are transferred to a different IP telephone if necessary. The IP telephone allows up to six registrations, which do not have to be available at the same time. With the "Enable registration" function, you can enable the registrations already created. With the "Set target registration active" switch, the newly enabled registrations are also activated.

The following parameters are selectable:

Registration Identifier	Numeric configuration identifier of the target registration (1..6)
Set Target Registration active	The target registration shall become the active registration when enabled.

4.7.1.5.12 Function Key Activate Registration

With this function, the defined registration is activated under "Registration identifier". The currently active registration is set to inactive. If you have turned on the "Disable current registration" switch, the registration previously active is deregistered.

☝	**Tip** When the new registration has become active after use, the settings of the new registration are also valid.	☝

Registration Identifier	Numeric configuration identifier of the target registration (1..6)
Disable current Registration	Disable the current registration when activating the actual target registration.

Activate Next Enabled Registration	Sets the next enabled registration to the active registration. Otherwise the last active registration will become the active registration again.

4.7.1.5.13 Function Key Do not Disturb

The Do Not Disturb function can be controlled via a function key. You can choose between the states 'On' and 'Off'.

Action	Under Action the Do not Disturb variant can be selected. • default • do not ring • reject call (busy) • ignore call (no response) • out of office (ignore call and send absence message)
Apply to	Under Apply to the kind of call to be treated by the feature can be selected. • default • any call • external calls • internal calls

4.7.1.5.14 Function Key Call Waiting

If a call is already active, an incoming call can be treated in different ways, depending on the current state. The state can be determined by the function key.

State 0	If the Call Waiting function is deactivated, the second caller hears a busy signal.
State 1	If the ‚Call Waiting' function is activated, the call is shown in the display, and a short signalling tone can be heard by the person who is being called. The person who is being called, may then • End the call, in order to answer the new call, • Put the active call on hold, in order to switch to the new call, or • Reject the call.

4.7.1.5.15 Function Key Hide Own Number

Transmitting one's own number can be temporarily suppressed by means of this function.

- State 0 = Telephone number is transmitted
- State 1 = Telephone number is suppressed

4.7.1.5.16 Function Key Transfer

In case of a new incoming call during an already active call, the new call must be answered (switch active call using the 'R' key). During the two established calls, the ‚Transfer' function can be used to connect the two callers with each other, and to place one's own VoIP telephone in idle mode.

4.7.1.5.17 Function Key Redirect

This function puts two options at your disposal:

1. Using this key, you may divert an incoming call to the configured number.
2. If during a call, a second call occurs, this function can be used to divert the active caller, in order to answer the new call.

Number	The number to be called.
Name	The name to be called.
Redirect Active Call	If this checkmark is set the active call is redirected. By default the first waiting call (if any) is redirected.

☞ **Note**

If both *Number* and *Name* are left blank a dialog will pop up each time the function key is pressed. After the address has been entered the Redirection is started by pressing the redial key. ☜

4.7.1.5.18 Function Key Lock

This function can be used to lock the telephone. A setup of the functions to be able to be locked can be configured at Menu Protect (see chapter 4.7.5 on page 275).

The PIN can be configured respectively changed:

- "Menu"
- "Phone Setup"
- "Change PIN"

In the as-delivered condition, no PIN is stored.

4.7.1.5.19 Function Key Headset

In order to control the telephone when a headset is connected, a key, depending on the particular VoIP telephone, works as a hook switch:

State 0	• Headset control off
State 1	• Headset control on

Furthermore the mode can be configured.

Mode	• Enable (The headset can be released or locked.) • Control (The headset can be controlled (lift off, hang up).)

4.7.1.5.20 Function Key Hot Desking

If different participants often log on using a certain telephone, the function Hot Desking can be used to obtain the access data upon each logon. If the state changes to state 0, the co-user is logged off again.

User Config Stored at PBX	**Attention**: this configuration option can be used only, if the PBX supports this option. The function "User Config stored at PBX" should be used if the registration that activates the hotdesking, stores its config in the PBX. Without this button the configuration of the second user (user executing the hotdesking) is modified and a 'Delete Registration' button is inserted at the position of the previous hotdesking button. To prevent this, you must set the "User Config stored at PBX" option and configure manually an additional 'Delete Registration' button at the user executing the hotdesking. If the stored config contains itself a 'Hot Desking' key with 'User Config Stored at PBX' checked this key works as a 'Delete Registration' key in a hot desking registration.

4.7.1.5.21 Function Key Create Registration

In the Active state, a further user is logged on for the telephone. According to this, the logon can take place

- in the same telephone system,
- in another telephone system, or
- directly at an IP telephony provider

The protocols H323 or SIP can be used for this purpose. The allocation of the parameters in the Active State can be obtained from the particular provider of the system. The option "set active" is used to activate the new registrations.

☞	**Note** You can determine an 'active user'. The outbound calls are conducted under his parameters, and the function keys are, if necessary, applied on another VoIP telephone.	☞

First, the required protocol must be chosen for registration. You have the choice between the protocols H323, SIP, TSIP and SIPS. The corresponding parameters are automatically adapted to the selected protocol.

Protocol H323:

Gatekeeper Address	This is the IP address, under which the PBX or the responsible gatekeeper can be reached.
Gatekeeper Identifier	If several gatekeepers are to be active on one address, among these a certain gatekeeper is identified on the basis of the name that is to be entered here.
Number	Telephone numbers that are required for the registration are entered here.

Name	The name that is to be entered here is required for the registration only if the number has not been entered.
Password	The registration requires a password, which can be agreed upon in this option.
Retype	This is a security question for the password.

Protocol SIP, TSIP, SIPS:

Domain	The domain of the provider, which can be found after the ‚@' of the URI, can be entered instead of the IP address.
User ID	In this protocol, registration requires a user ID, which corresponds to the part before the @ of the URI.
Username	In some SIP registrations, authorising a separate user name is required. In all other cases, the field should be left empty.
Password	The registration requires a password, which can be agreed upon in this option.
Retype	This is a security question for the password.
Proxy	IP address or domain name, under which the responsible SIP server can be reached.
STUN Server	The IP address or domain name must be configured, if the telephone uses a non-public IP address, whereas the server, however, can be reached under a public IP address. The value is given by the SIP provider or administrator.

☞	**Note** If a domain name is defined, a DNS server must be defined and reachable. The DNS server must be able to resolve the name.	☜

The following parameters can be adjusted independently of the protocol. These parameters are automatically negotiated when a connection is established. A change is necessary only if the gatekeeper/server makes certain demands regarding the connection protocol.

General Coder	The protocols for the speech compression are listed in this parameter. The desired general coder can be selected: One of the following coder can be selected: • G711A (ISDN Europe) • G711u (ISDN North of America, Japan) • G729A
Framesize [ms]	For General Coder: The package sizes are automatically negotiated with 60 ms. This parameter enables the determination of another RTP package size.
Silence compression	For General Coder: Taking the VoIP telephone as the starting point, in case of silence (no conversation), no packages are sent. On the other side, noise is played back.
Exclusive	For General Coder: This parameter allows no negotiation, but accepts only the preset parameters.

Local Coder	The protocols for the speech compression in the local network are listed in this parameter. The desired local coder can be selected: One of the following coder can be selected: • G711A (ISDN Europe) • G711u (ISDN North of America, Japan) • G729A
Framesize [ms]	For Local Coder: The package sizes are automatically negotiated with 30 ms. This parameter enables the determination of another RTP package size.
Silence compression	For Local Coder: Taking the VoIP telephone as the starting point, in case of silence (no conversation), no packages are sent. On the other side, noise is played back.

Secure RTP	Selection of the speech data encryption: • <empty item> (no encryption) • AES128/32 (AES encryption, key length 128 bit, 32 bit SHA1 Hash message) • AES128/80 (AES encryption, key length 128 bit, 80 bit SHA1 Hash message) • AES192/32 (AES encryption, key length 192 bit, 32 bit SHA1 Hash message) • AES192/80 (AES encryption, key length 192 bit, 80 bit SHA1 Hash message) • AES256/32 (AES encryption, key length 256 bit, 32 bit SHA1 Hash message) • AES256/80 (AES encryption, key length 256 bit, 80 bit SHA1 Hash message)
Set Active	Following registration, this registration is set as the active registration.

4.7.1.5.22 Function Key Delete Registration

The still active co-user, in this option is deregistered, and the previous user thus automatically restored to the state of active user.

4.7.1.5.23 Function Key Switch

Once several users have been registered, this function can be used to the switch to another user as the active user.

If the new registration has become active after use, the function key assignment of the new registration also applies. It therefore makes sense to configure a deregistration on this key in the user's configuration.

Under Action the following parameter can be selected:

Protocol H323:

Gatekeeper Address	This is the IP address, under which the PBX or the responsible gatekeeper can be reached.
Gatekeeper Identifier	If several gatekeepers are to be active on one address, among these a certain gatekeeper is identified on the basis of the name that is to be entered here.
Number	Telephone numbers that are required for the registration are entered here.
Name	The name that is to be entered here is required for the registration only if the number has not been entered.

Protocol SIP, TSIP, SIPS:

Domain	The domain of the provider, which can be found after the ‚@' of the URI, can be entered instead of the IP address.
User ID	In this protocol, registration requires a user ID, which corresponds to the part before the @ of the URI.
Proxy	IP address or domain name, under which the responsible SIP server can be reached.

All protocols:

Disable Active Registration	Disable active registration

4.7.1.5.24 Function Key Recording

This function key can activate or deactivate the recording function.

4.7.1.5.25 Function Key Boolean Object

This function monitors the state of the addressed Boolean Object in the PBX. A Boolean Object as seen by the user is in one of four states:

Automatic off state	The automatic mode FALSE rule applies.
Automatic on state	The automatic mode TRUE rule applies.
Manual override off state	The manual override FALSE rule applies (automatic mode rules are disabled).
Manual override on state	The manual override TRUE rule applies (automatic mode rules are disabled).

How a state is indicated at the phone is configured under the respective topic.

The identification will be done with calling number and name.

Number	Number
Name	Name

Toggle State	If this checkmark is set, the key operates as a toggle key. Each keystroke switches from the current state of the addressed Boolean Object to the next state in the sequence Automatic *Off/On State / Manual Override Off State / Manual Override On State*. **Note: Toggling works only if a number is configured for the Boolean Object.** If this checkmark is not set, pressing the key sets up a connection to the Boolean Object. The state of the Boolean Object can be changed then by entering DTMF codes. DTMF codes: 0 - Clear Manual Override, i.e. switch to the automatic mode rule according to current time of day. 11 - Manual Override On, i.e. apply the manual override TRUE rule. 10 - Manual Override Off, i.e. apply the manual override FALSE rule.

☞	**Note** This function will only work if the monitoring user (i.e. the user configuring the key) shares a group with the addressed Boolean Object and this group is selected under "Group indications" in the PBX User Object of the monitoring user.	☜

4.7.1.5.26 Function Key Presence

This function key can activate or deactivate the presence state.

By subsequent pressing this function-key, someone toggles own presence activity until desired activity reached.

This function key is a handy shortcut for a long navigation way through main menu: main menu, user settings, presence, toggle activity, menu, menu.

☞	**Note** The presence publishing is done with a 2 second delay after reaching the final presence activity. This delay is to avoid unnecessary signaling traffic to PBX and all presence subscribers.	☞

4.7.1.5.27 Function Key Prepare Override

Thi7s function key is used to prepare a call with some override options and to complete the number or the name with further digits or letters. Dialing is started by lifting the handset or pressing the speaker or the headset key:

Number	Remote party number. A comma (**,**) can be used to insert a 300ms pause between the digits. This is useful e.g. for destinations accepting DTMF after connect.
Name	Remote party name (H323 ID).
Dial Immediately	Dial immediately with the given parameters.
Announcement	Announcement Call

Override	• None: No Override Options • Caller: The default calling party number and name are overridden by *Caller Number* and *Caller Name*. • Diversion: The call is sent directly to the given *Number* and *Name* ignoring any diversions set by the called party.
Caller Number	Overriding calling party number (If override is set to caller.).
Caller Name	Overriding calling party name (If override is set to caller.).

If the key is pressed when...

- the phone is idle and *Dial* is checked, then a call is set up immediately even if both *Number* and *Name* are empty.
- the phone is idle and *Dial* is NOT checked, then the indirect dialing menu is opened. The menu footline indicates the kind of override (*CO* - Caller Override, *DO* - Diversion Override).
- the indirect dialing menu is active (opened by this or any other key), then a call with the given override parameters is set up to the target entered in the menu.
- the phone went just off hook and no digits were entered so far, then the call is restarted with the given parameters.
- the phone went just off hook and some digits were entered already, then the key is ignored.
- there is ONE connected call, then a second call is set up.
- there is more than one call, then the key is ignored.

4.7.1.5.28 Function Key Toggle

With this function-key it is possible to toggle between two states.

State 0:

Number	Call number

State 1:

Number	Call number

Aktion:

Toggle on Press and Release	Toggle state on pressing and releasing the key.

This function key will be used to send alternative DTMF sequences during an active call, to realize a Push to Talk key.

With pressing the key the configured DTMF digits in the current state will be transmitted and the state will switched to the alternative state.

If there is no existing active call, then the key will be ignored.

State 0 – Number

DTMF digits to be send, if the key will be pressed in the state 0.

State 1 – Number

DTMF digits to be send, if the key will be pressed in the state 1.

Toggle on Press and Release

Execute the state 0 action with pressing the key and execute state 1 action with releasing the key.

4.7.1.5.29 Function Key Message

With this function a prepared message can be stored at a function-key.

Destination	Destination of the message
Text	Message text

4.7.1.5.30 Function Key Spare

With this function-key a key position can be reserved for administrative purposes.

4.7.1.6 Submenu Recording

In order to record telephone conversations, you need to start a conference, in which the recording device can be included, if necessary.

There are four kinds of recording:

- Off: Recording is disabled.
- Manual: In this mode, recording takes place on the request of the participant. By pressing the Repeat key, recording is activated and also deactivated.
- Transparent: This mode activates recording throughout the conference and cannot be interrupted by the participant.
- Optional: This mode starts recording automatically for each call, but recording can be stopped if the participants requests it.

Tip

The „Optional" mode should be used if, at the beginning of a conversation, it is unclear whether or not recording is necessary.

Number	Here, the telephone number is entered, during which the recording device can be reached.

Name	Alternatively, the H323 name of the recording device can be entered.
External Calls Only	With this option, the recording function can be limited to calls from outside of one's own telephone system.
Function Key Control Only	With this option, the recording function can be controlled with a function key only.

Call Data:

The recording call from the phone to the recording device is a straight fresh call with the recording phones telephone number as calling line id. However, the remote party number (that is, the party the agent is talking to) will be sent with this call as diverting number (H.450 information in H.323 and Diversion**:** header in SIP, respectively). Please note that when the agent does consultation calls while recording, the recorded stream always follows the active call. The changing remote party numbers are not notified in the recording call.

The diversion info sent in the recording call will indicate an incoming call as *diversion user busy* and an outgoing call as *diversion-no-answer*.

4.7.1.7 Submenu Reset

With this function the user specific configuration can be rested. Therefore the option Reset User Specific Configuration has to be activated and the ok button must be clicked.

4.7.2 Menu Ring-Tones

In this submenu, up to 26 ringing tones in RTTTL format (Ringing Tones Text Transfer Language) can be downloaded to the VoIP telephone. Other formats are not supported.

In order to download a ringing tone, the text based and RTTTL compatible content of the new ringing tone is entered in the 'RTTTL String' field, and then confirmed through the button 'Add'.

Pressing the hyperlinks 'piano', 'mezzo' and 'forte' plays back the particular ringing tones on the phone, from quiet (piano) to loud (forte). The link "stop" serves to stops playing a ringing tone. The link 'delete' in the 'Action' column serves to delete a ringing tone. The already installed ringing tones are also displayed.

The preinstalled ringing tones can't be deleted.

In the case of subsequently downloaded ringing tones, it is not possible to alter the playback speed via the device menu.

Tip

The name of the ringing tone is already contained in the RTTTL format and is automatically displayed in the 'Title' column. In order to alter the name of the ringing tone, you can open the RTTTL file using an ASCII editor, and edit the name.

4.7.3 Menu Direct-Dialing

If Direct-Dialling is turned on, and the telephone receiver is lifted or the loudspeaker key is pressed, an entered direct dial number is dialled. All keys of the VoIP telephone, except the Menu key, are locked after the autodial timeout.

Enable	Enable the direct-dialling feature
Destination Number	Telephone number, which is dialled directly upon lifting the receiver.
Destination Name	The name can be assigned to the direct call destination instead of the telephone number.
Autodial Timeout [s]	Delay in seconds before dialling, default: 0 seconds (immediately)

☞	**Note** If the direct dial is active and the delay is set to 0 seconds, then after the try to enter digits in the idle state the following error message will be displayed: keyboard locked! Also with active direct dial no inquiry calls can be made.	☞

4.7.4 Menu Preferences

Preferred settings:

Background Image	Background Image (PNG-File) (Only for telephones with colour displays)
No Call Transfer on Hook-On	No call transfer on hook-on.
No Local Conference Tone	No local conference tone.
No Local Intrusion Tone	No local intrusion tone.
No Local Dial Tone	Suppress the dial tone usually played after call setup until the first digit is called.
Swap Internal/External Ring Tone Pattern	In some countries the ring tone timing patterns for internal/external calls need to be swapped to meet country defaults. If at an (optional) relay the option 'Alert Ringing Pattern' is selected, then at Device/Relays the Option 'Swap Internal/External Relay Ring Tone Pattern' has to be selected too (see chapter 4.8.4 on page 288).

Display Name on Pickup/Partner Key	Display the H323-ID of the calling party instead of the number. Usually only internal calls provide the H323-ID (the 'Name' in a PBX user object)
Keep Calling Party Info on Pickup Key	Truncate the called party info instead of the calling party info.
Display Alerting Partners on Pickup Key	Display alerting partners on pickup key.
Hide Display Info from ISDN Provider	Do not display the text some ISDN Providers may send via info indications bearing a display info element.
Start Outbound Call on Electronic Hook Switch (EHS) Signal	Start outbound call on electronic hook switch (EHS) signal.
Play Configured Ring Melody before Automatically Connecting an Announcement Call	Play configured ring melody before automatically Connecting an announcement or multicast-announcement call.
Route Automatically Connected Inbound Calls to Headset (if enabled)	Route automatically connected inbound calls (announcement, multicast-announcement) to headset instead to speakerphone when headset is enabled.
Connect Automatic Redialled Call with Microphone Switched Off	Connect automatic redialled call with microphone switched off.
Use Headset like a Handset Ignore Hookswitch Signals	Use headset like a handset, Ignore hookswitch signals.

Use Newline/OK Key as Headset Key	Use newline/OK key as headset key.

4.7.5 Menu Protect

Configuration is possible not only using the interface of the web browser, but partly also using the VoIP telephone directly. This configuration can also be password protected or completely hidden.

If according to a parameter a bit mask is to be entered, so all for this parameter relevant desired masks have to be added as a hexadecimal number and afterwards the sum has to be entered into the input field.

Protect Configuration at Phone	Password protected changes of the administrative configuration at the phone.
Hide Complete Configuration at Phone	Do not display the configuration at the phone. The administrative configuration can be changed only via the WEB interface. The Main Menu displays Call Lists, Directories, Messages and Administration items only. The "Administration" menu displays version info only.
Hide Administration Configuration at Phone	Do not display the administrative configuration at the phone. The administrative configuration can be changed only via the WEB interface. The "Administration" menu displays version info only.
Fine grained Function Hiding	Bit mask to selectively hide phone configuration menus and screen.

The following functions can be hided:

Name	Wert	Beschreibung
PHONE_HIDE_ADMIN_INFO_MAC	0x01000000	Hide serial/MAC from admin->info screen
PHONE_HIDE_ADMIN_CONFIG	0x10000000	Hide config entries from admin-menu (keep admin-info only)
PHONE_HIDE_MM_ADMIN	0x08000000	hide admin entry from main-menu
PHONE_HIDE_MM_USER_LIST	0x20000000	hide user-list entry from main-menu
PHONE_HIDE_MM_PHONE_SETTINGS	0x40000000	hide phone-settings entry from main-menu
PHONE_HIDE_MM_USER_SETTINGS	0x80000000	hide user-settings entry from main-menu
PHONE_HIDE_US_PREFERENCES	0x00000100	hide preferences from user-list
PHONE_HIDE_US_RING_MELODY	0x00000200	hide ring melody from user-list
PHONE_HIDE_US_FUNCTION_KEYS	0x00000800	hide function keys entry from user-list
PHONE_HIDE_US_REGISTRATION	0x00001000	hide registration entry from user-list
PHONE_HIDE_PS_BGIMAGE	0x00000001	hide background-image entry from phone-settings menu

The mask defined under "Fine grained Function Hiding" (/hide-mask) is applied when the phone is in normal mode. The default for this mask is 0x00000000.

Hide private Call Information	Show only calls from/to the currently active registration in call lists.
Numbers for Emergency Calls	Comma separated list of numbers (including any necessary prefix) permitted to call when the phone is locked. An empty list means that no calls are permitted when the phone is locked. (white list)
Prefixes for External Calls	Comma separated list of prefixes not permitted to dial when the phone is disabled for external calls via lock mask.

Fine grained Function Locking	Bit mask to selectively disable certain functions when the phone is not locked.
Functions to lock via PIN	Bit mask to define the functions disabled when the phone is locked by PIN, by default everything except emergency calls.

Currently the following functions can be disabled:

name	value	description
PHONE_LOCK_DIAL_EXT	0x00000001	disable external call if not on white list
PHONE_LOCK_DIAL_INT	0x00000002	disable internal call if not on white list
PHONE_LOCK_DIAL_QUERY	0x00000004	disable directory search on outbound calls
PHONE_LOCK_DIAL_HISTORY	0x00000008	disable outbound call list access
PHONE_LOCK_RING_EXT	0x00000010	ignore (but log) inbound external calls
PHONE_LOCK_RING_INT	0x00000020	ignore (but log) inbound internal
PHONE_LOCK_RING_QUERY	0x00000040	disable directory search on inbound calls
PHONE_LOCK_RING_HISTORY	0x00000080	disable inbound call list access
PHONE_LOCK_CALL_COMPLETION	0x00000100	disable call completion
PHONE_LOCK_CALL_TRANSFER	0x00000200	disable call transfer
PHONE_LOCK_CALL_BROKING	0x00000400	disable handling of multiple calls
PHONE_LOCK_CALL_CONFERENCE	0x00000800	disable conference
PHONE_LOCK_CALL_DIVERSION	0x00001000	disable call diversion

name	value	description
PHONE_LOCK_CALL_REDIAL	0x00002000	disable automatic dialling if call completion is not locked at all
PHONE_LOCK_MSG_SEND	0x00004000	disable sending messages
PHONE_LOCK_MSG_RECV	0x00008000	disable receiving messages
PHONE_LOCK_FKEYS	0x00020000	disable function keys
PHONE_LOCK_MENU	0x00040000	disable any menu
PHONE_LOCK_DND	0x00080000	disable Do Not Disturb via mute key, function key and menu
PHONE_LOCK_DIRECTORY	0x00200000	disable directory access
PHONE_LOCK_PHONE_SETUP	0x00400000	disable phone setup functions: direct dial, lock phone, change pin
PHONE_LOCK_USER_LIST	0x00800000	disable user list functions: activate, function keys
PHONE_LOCK_REMOTE_CONTROL	0x01000000	disable remote control of phone
PHONE_LOCK_DIVERSION_OVERRIDE	0x04000000	disable diversion override for outbound calls
PHONE_LOCK_KEY_INFO	0x20000000	do not display function key labels or lamps
PHONE_LOCK_CALL_INFO	0x40000000	do not display missed calls and active diversions
PHONE_LOCK_USAGE	0x80000000	restrict phone access to emergency use

The mask defined under "Fine grained Function Locking" (/lock-mask) is applied when the phone is in normal mode. The default for this mask is 0x00000000.

The mask defined under "Functions to lock via PIN" (/pinlock-mask) is applied when the phone is locked with a PIN entered in the corresponding menu. The default for this mask is 0x9FFFFFBF:

- Outbound calls are restricted according to white list; an empty white list disables any outbound call.
- Inbound calls are ignored, but logged in the call list.
- Function keys are deactivated.
- Missed calls are displayed.
- Active diversions are not displayed (this is currently not controlled by the pinlock-mask, but by the pinlocked state itself, thus this cannot be changed in current version but it will be in following versions).

The white list is a comma separated list of numbers, including any necessary prefix.

The prefix list is a comma separated list of prefixes identifying external calls, in the most simple case this list may contain only a '0'.

The same information can be entered by config uploading the following command line:

```
config change PHONE USER /lock-mask <mask> /pinlock-mask
<mask> /whitelist-e164 <numbers> /external-e164 <prefixes>
```

<table>
<tr><td rowspan="2">Function keys not modifiable on the phone</td><td colspan="3">Type of function keys that the configuration could not be displayed and not be modified at the phone.

List of the function key types:</td></tr>
<tr><td>function key type</td><td>bit</td><td>value</td></tr>
<tr><td></td><td>not defined</td><td></td><td></td></tr>
<tr><td></td><td>Dial</td><td>1</td><td>0x00000002</td></tr>
<tr><td></td><td>Call Forwarding</td><td>2</td><td>0x00000004</td></tr>
<tr><td></td><td>Lock</td><td>3</td><td>0x00000008</td></tr>
<tr><td></td><td>Do Not Disturb</td><td>4</td><td>0x00000010</td></tr>
<tr><td></td><td>Call Waiting</td><td>5</td><td>0x00000020</td></tr>
<tr><td></td><td>Hide Own Number</td><td>6</td><td>0x00000040</td></tr>
<tr><td></td><td>Headset</td><td>7</td><td>0x00000080</td></tr>
<tr><td></td><td>Partner</td><td>8</td><td>0x00000100</td></tr>
<tr><td></td><td>Pickup</td><td>9</td><td>0x00000200</td></tr>
<tr><td></td><td>Create Registration</td><td>10</td><td>0x00000400</td></tr>
<tr><td></td><td>Delete Registration</td><td>11</td><td>0x00000800</td></tr>
<tr><td></td><td>Switch</td><td>12</td><td>0x00001000</td></tr>
<tr><td></td><td>Hot Desking</td><td>13</td><td>0x00002000</td></tr>
<tr><td></td><td>Message Waiting</td><td>14</td><td>0x00004000</td></tr>
<tr><td></td><td>Transfer</td><td>15</td><td>0x00008000</td></tr>
<tr><td></td><td>Redirect</td><td>16</td><td>0x00010000</td></tr>
</table>

	Park	17	0x00020000
	Enable Registration	18	0x00040000
	Activate Registration	19	0x00080000
	Join Group	20	0x00100000
	Search Directory	21	0x00200000
	Boolean Object	22	0x00400000
	Recording	23	0x00800000
	Presence	24	0x01000000
	Prepare Override	25	0x02000000
	Toggle	26	0x04000000
	Message	27	0x08000000
	Spare	28	0x10000000
	The default value fort he input field is: 0x00000000. For the function key types to lock is the OR logic interconnection of the values of the function key types has to be entered. Keys not programmed can be programmed always, but cannot be modified afterwards.		

4.7.6 Menu State

4.7.6.1 Submenu Registrations

Here it becomes clear, which users are currently registered at the VoIP telephone.

Id	Running numbering
State	• **up:** User registration was successful • **disabled:** The accordant registration is configured but not enabled. • **timeout:** Due to the expiration of the time limit during the logon procedure, the user was not logged on. • **rejected:** User registration was rejected • **unauthorized:** User logon was declined in view of missing or incorrect password.

Number	Calling number of the user
Name	Name of the registration
Gatekeeper Address	IP address of the gatekeeper that received the registration.
Gatekeeper Identifier	ID of the gatekeeper that accepted the registration.
Gatekeeper Instance	• **primary:** The registration will be carried out at the primary gatekeeper. • **secondary:** The registration will be carried out at the secondary gatekeeper
Protocol	VoIP Protocol H.323, SIP, TSIP or SIPS
Active	Shows which user is actively registered on the VoIP telephone.

If more than one registration is registered successfully, then another registration can be selected as the active registration. With clicking the OK button the active registration can be switched over.

4.7.6.2 Submenu Calls

In this submenu all active connections of the phone will be displayed.

In the table the following parameter will be displayed.

Protocol	• **H323:** • **SIP:** • **TSIP:** • **SIPS:** There will be additional information, weather the call is local (**LOCAL**) or external (**EXTERNAL**).
Number	Calling number of the used registration.
Name	Name of the used registration.
Media	Used codec of the own side
Addr	IP address : port number of the own side
Dir	• **>>:** outgoing established call • **<<:** incoming established call
Number	Calling number of the opposite side
Name	Name of the opposite side
Media	Used codec of the opposite side
Addr	IP address : port number of the opposite side

State	State of the connection • **calling:** The connection will be set up • **altering:** The opposite phone is ringing • **ringing:** The phone is ringing • **connected:** Connection is active • **closing:** Connection will be closed
Action	• **drop:** With clicking on existing connections can be cancelled • **dial:** If the phone is in idle state, then with clicking on an input window will be opened, in which a calling number can be entered. After clicking on the button dial in the input window the phone dials the entered number as if someone has entered the number at the phone keypad. • **accept:** With clicking on an incoming call will be accepted • **reject:** With clicking on an incoming call will be rejected

4.7.6.3 Submenu DHCP-Options

The DHCP options cannot be shown if the telephone is operating in the DHCP client mode. A list with the option, the ID and the value will be shown.

Here are shown additional Information about the DHCP-Options:

Details:

This device supports auto configuration via standard DHCP options.

They additionally support some manufacture specific options to effect some VoIP specific configuration.

Some of them are generic; some of them are specific to phone devices.

System Requirements:

To use vendor specific DHCP options, a DHCP server that supports such options is required.

Most popular DHCP server implementations such as the Microsoft Windows DHCP service and the Linux dhcpd do so.

Configuration:

For the DHCP server to support vendor specific options, the options must be made known to the server.

Consult the accompanying documentation which comes with your DHCP server implementation how to do this.

Supported Options:

name	data type	array	code	meaning	how to code
H323 gatekeeper	IP address	Yes	200	Defines the IP address of both the primary and the alternate gatekeeper for the device. This is only required, if gatekeeper discovery is not feasible.	This is an array of IP addresses. Put the primary gatekeepers IP into the first entry, the alternate gatekeepers IP into the second entry. Further entries are ignored.
H323 gatekeeper id	String	No	201	The gatekeeper id of the gatekeeper the device likes to register with. Usually required only if several gatekeepers are running and a particular one must be chosen during gatekeeper discovery	Type the gatekeeper id as configured in the gateway or PBX configuration into the string field.
POSIX TZ	String	No	202	Defines both the time zone and the daylight saving time information.	Enter the correct TZ string into the string field as you would configure it in the devices configuration applet. This option is in fact identical to the standard DHCP option number 88 (TZ). However, various DHCP servers do not support this option, so it is provided as a redundant vendor specific option. If your DHCP server supports option 88, the vendor specific option is not needed.

name	data type	array	code	meaning	how to code
Default coder	String	No	203	Defines the preferred coders for H.245 coder negotiation, as well as the packet size when sending RTP packets and the use of CNG and VAD.	This string option must contain the value of the "/coder" option in the phone configuration file, e.g. **G729A,40,sec**. After a "/" the value of the "/lcoder" option can be added to this string. **G729A,60/G711A,30** for example defines G729A as the general coder and G711A as the coder to be used in networks considered local.
Language	String	No	204	Defines the user interface language	This string must contain the value of the **/lang** option in the phone configuration file, e.g. **eng**
Location	String	No	205	Defines the various PBX access numbers (country code etc.) for the device.	This string must contain the **/cc**, **/ac**, **/ntp**, **/itp**, **/col** and **/pbx** options in the phone configuration file, e.g. **/cc 49 /ac 208 /ntp 0 /itp 00 /col 0 /pbx 7** (althought, to save bytes, you may omit the **/**-es)
VLAN ID	Word (16bit)	No	206	The 802.1q VLAN ID for traffic sent and received by the device	Enter the numerical ID into the 16bit edit field
VLAN Priority	Byte (8bit)	No	207	The 802.1p VLAN priority for traffic sent by the device	Enter the numerical priority into the 8bit edit field
TOS Bits	String	No	208	The value for the IP TOS field in the IP header of voice traffic sent by the device	Enter the numerical TOS (Type of Service) into the string field. You may prefix with **0x** to specify hexadecimal numbers (or **0** to specify octal numbers)
Enbloc dialling	Byte (8bit)	No	209	The number of seconds dialled digits are kept in the phone before they are sent en-bloc to the gatekeeper	Enter the number of seconds into the 8bit edit field. A value of **0** indicates that en-bloc dialling is turned off and digits are sent to the gatekeeper as they are dialled
Dialtone type	Byte (8bit)	No	210	The type of dialtone to generate locally	Enter the numeric dialtone type (e.g. **0** - german PBX, **1** – german PSTN, **2** – US)
Faststart	Byte (8bit)	No	211	Disable/Enable the H245 faststart procedure	To disable enter **0**, otherwise enter **1** into the 8bit edit field
H245-Tunnelling	Byte (8bit)	No	212	Disable/Enable H245 tunneling	To disable enter **0**, otherwise enter **1** into the 8bit edit field
Clock Type	Byte (8bit)	No	213	Define format of date and time display	Enter the numeric clock type (**0** – *dd.mm.yy hh:mm*, 24 hour clock; **1** – *mm/dd hh:mm xm*, 12 hour am/pm clock)

name	data type	array	code	meaning	how to code
Static Routes	String	No	214	Static routes to be added to the routes already defined in the device configuration	The string (max 127 characters) must contain comma separated route definitions in the form *address*:***mask***:***gateway*** *address*, *mask* and *gateway* are expected in dotted decimal notation, mask (but not the colon) can be left off in a host route
Update URL	String	No	215	URL to retrieve update commands from. This is identical to the /url option parameter of the UP1 module	Complete URL as in **http://192.168.0.10/file.txt** . No symbolic host names are supported
Update Poll Interval	Word (16bit)	No	216	Standard poll interval in minutes. This is identical to the **/poll** option parameter of the UP1 module	Interval in minutes
LDAP directory	String	No	217	Defines the various Parameters required to access an LDAP directory	
Local Networks	String	No	218	Defines the networks to be considered local in coder negotiation.	This string option must contain a list of networks in form of comma separated "Address:Mask" pairs, for example **192.168.1.0:255.255.255.0, 192.168.2.0:255.255.255.0**.

The option (202) is in fact identical to the standard DHCP option number 88 (TZ). However, various DHCP servers do not support this option, so it is provided as a redundant vendor specific option. If your DHCP server supports option 88, the vendor specific option is not needed.

4.8 Main Menu Device

4.8.1 Menu Info

In this area some information about the telephone are displayed.

DRAM cashed	The available cashed DRAM memory of the telephone. Behind **free** the still available cashed DRAM memory is displayed.

DRAM uncashed	The available not cashed DRAM memory of the telephone. Behind **free** the still available not cashed DRAM memory is displayed.
ISRAM	The available ISRAM memory of the telephone. Behind **free** the still available ISRAM memory is displayed..
FLASH	The available FLASH memory of the telephone.
Default Language	The language of the user interface of the phone after a reset to factory default.

4.8.2 Menu Temperature

Every 5 seconds you will be displayed the actual values of the following temperatures. This feature is only available for the telephone ResistTel IP2 / IP152.

Temperature	Actual temperature of the printed board inside the phone.
Temp HYST	If the temperature of the printed board inside the phone is below this value the heater of the display will be switched on.
Temp OS	If the temperature of the printed board inside the phone is above this value the heater of the display will be switched off.

4.8.3 Menu LAN-Interface

In the submenu LAN-interface the type of the build in LAN interface module inside the phone will be shown. This can be one the following types:

- 1 port
- 2 port switch

4.8.4 Menu Monitoring

The monitoring allows the remote testing of the electro acoustic converters (microphone, speaker) of the telephone.

Each test will be executed with one microphone and one speaker. Inside of the telephone two speakers for ringing respectively hands free mode, a microphone for hands free mode and a speaker and a microphone for the handset are mounted. Therefore the following three tests variants are available:

- Test handset. For the handset test the speaker and the microphone of the handset will be used.
- Test hands free / speaker 1: For the test the speaker 1 and the hands free microphone will be used.
- Test hands free / speaker 2: For the test the speaker 2 and the hands free microphone will be used.

4.8.4.1 Submenu Info

In the submenu Info the actual state of the telephone, the results of the last complete monitoring tests and the last state of the monitoring tests can be seen. All shown parameter will be refreshed every 5 minutes.

In the chapter phone the following information will be displayed:

Phone State	Call state of then telephone: • idle (The telephone is in idle state) • busy (The telephone is in busy state (call state, alerting state, calling state).
Phone State since	The duration since the last change of the state will be displayed in the format 1d 2h 23m 45s (days, hours, minutes, seconds).
Hook State	State of the hook switch: • on • off

Hook State since	The duration since the last change of the state will be displayed in the format 1d 2h 23m 45s (days, hours, minutes, seconds).

In each of the sections to the different tests the information will be displayed.

Note

The information for each test will be conserved during a loss of the power or a restart of the telephone.

If a reset to factory default or an overwriting of the configuration with a file will be executed, then the stored results will be deleted or changed.

Last completed Test	Point of time (date, time) the last test was finished completely with a test result (ok, error). The point of time will be displayed only, if the actual time specification was available for the phone via a NTP sever.
Result	Result of the last complete test: • unknown (result after reset the configuration to factory default) • ok • too much noise • handset missing / microphone error • handset error • handsfree / speaker 1/2 error • handsfree / speaker 1/2 overload error
Last Test	Point of time (date, time) of the last test. The point of time will be displayed only, if the actual time specification was available for the phone via a NTP sever.

Last Test State	State of the last test. Zustand des letzten Tests • idle (result after reset the configuration to factory default) • pending • started • aborted • complete

☞	**Note** If the test will be executed in a very noisy environment, then the amplifiers and the A/D converters will be overloaded totally. This error can't be always differentiated from other errors. Such errors will be displayed as overload errors.	☜

4.8.4.2 Submenu Test

With the submenu Test the tests can be started, test properties selected and adjusted to the environment of the telephone.

Test Environment	With this parameter the tests can be adjusted to the environment noise level. • Normal • Noisy

In a low noise measuring room some measurements have been done with a pink noise background noise. The maximal level for the pink noise background noise and the characteristic parameter of the tests can be seen in the following table.

With the adjustment noisy environment the test tone will be send out with a higher level for a longer duration. If the telephone will be accessed by a call (alerting, hook off, hands free mode) during sending the test tone, then the test will be aborted immediately. If the telephone will be accessed by a call or other requests (e. g. HTTP accesses) during the interpretation, then the time for the interpretation will be extended.

Test Environment	Normal	Noisy
Background Noise Pink Noise	68 dB	76 dB
Test Tone Duration	Ca. 9,5 Seconds	Ca. 34 Seconds
Time for Interpretation	Min. 22 Seconds	Min. 98 Seconds

To start to tests the following tests and options can be selected.

Repeat Test with 'Too much Noise Error' automatically	With this option tests with the error message,'Too much Noise Error' will be repeated maximal three times automatically.
Check Handset	Test Handset
Check Handsfree / Speaker 1	Test Handsfree / Speaker 1
Check Handsfree / Speaker 2	Test Handsfree / Speaker 2

The selected tests and test options will be accepted by clicking on the 'OK' button. At the page Info the tests will be displayed as 'started' respectively 'pending'.

If more than one test is selected, then the test will be executed one after the other. A test will be started, after the telephone will be in idle state for at least a minute.

During the handset test the handset may be not in the on hook position. If the handset is off hook and the phone is not in idle state, then you should look at the calling state at the web page Phone/State/Calls in detail. If the handset is in off hook position for more than a minute (see Device/Monitoring/Info web page) and the telephone is in the state 'calling' or 'closing', then you can assume, that the handset is in off hook position without having a call. With clicking at 'drop' the telephone can be set to the idle state. After a waiting period of a minute the first pending test will be started.

If a test will be aborted by an incoming or outgoing call or a restart of the phone, then the test will be repeated after an idle time of the telephone of at least a minute.

4.8.5 Menu Relays

In the submenu relays the function of the optional build in relay module can be configured. Without build in relay module the setup is without interest.

For both relays the following setups can be selected:

Disabled	Relay disabled
Alert-on	The relay is active, if the phone is in the ringing state.
Alert Ringing Pattern	The relay is switching in the rhythm of the default ringing signals for internal, external and returned calls.
Phone not idle	The relay is active, if the phone is not in the idle state. (If the disconnect key is pressed during lift off handset, the phone is in the idle state again, in face of lift off handset.)
Phone not idle or Handset lift off	The relay is active, if the phone is not in the idle state or the handset is lifted off.
DTMF Control on/off	The relay can be switched on or off during a call by the dialogue partner by configured DTMF signs. After the end of the call the relay will be switch off in every case. The remote controlling of the relay by DTMF signs is possible only, if the DTMF signs are broadcasted with signalling (RFC2833). If the same DTMF character is configured for switching on and off, then the relay will change the state with every received configured DTMF character.
DTMF Control Pulse	The relay can be switched on during a call by the dialogue partner by a configured DTMF sign for a configured duration. The remote activation of the relay with a DTMF sign is possible only, if the DTMF sign is broadcasted with signalling (RFC2833).

Registration Info	The relay will be switched active, if all with registration options selected registrations are marked as enabled at Phone/User-x/General (with x=1…6) and have the state up. At least one registration must be selected with the registration options.
Registration Alert	The relay will be switched active, if at least one the with registration options selected registrations is marked as enabled at Phone/User-x/General (with x=1…6) and has not the state up.

If the relays are set to Alert on or Alert Ringing Pattern, then the setup possibilities Alerting Options are enabled.

No internal Calls	The Relay will not be switched with internal calls.
No external Calls	The Relay will not be switched with external calls.
No returned Calls	The Relay will not be switched with returned calls.
No offered Calls	The Relay will not be switched with offered calls.

If a relay is set to DTMF Control on/off, then the setup control options DTMF Control on and DTMF Control off are enabled.

If a relays is set to DTMF-control-pulse, then the setup control options DTMF Control on and Pulse Duration [ms] are enabled.

DTMF Control on	DTMF character to switch the relay on.
DTMF Control off	DTMF character to switch the relay on. If DTMF Control on and DTMF Control off are sat to the same character, then the state of the relay will toggle with every received configured character.
Pulse Duration [ms]	Duration in ms, the relay will be switched on before it will be reset to the idle state automatically.

If a relay is set to Registration Info or Registration Alert, then the setup control options Registration Options are enabled.

Registration	Description
active	The registration at Phone/State/Registrations as active marked will be used for controlling the relay.
1	Registration 1
2	Registration 2
3	Registration 3
4	Registration 4
5	Registration 5
6	Registration 6

Additional setup possibilities:

Swap Internal/External Relay Ring Tone Pattern	If at Administration/Phone/Preferences (see chapter 4.7.4 on page 288) the option Swap Internal/External Ring Tone Pattern is activated, this option for the relay control should be activated too.

4.8.6 Menu Keypad

With the menu keypad the following setups are available:

External push buttons can be connected at the voltaic separated inputs. The push buttons must be suited for an electrical loading of 60 V DC, 3 mA. All inputs have a common zero potential.

For each line the operating mode can be programmed separately.

disabled	disabled
Function Key, press Fx	Function key, with pressing the key the function key Fx will be executed.
Function Key, release Fy	Function key, with releasing the key the function key Fy will be executed.
Function Key, press Fx – release Fy	Function key, with pressing the key the function key Fx and with releasing the function key Fy will be executed.

☞ **Note**

The function keys must be programmed for each used registration at Phone/User-x/Function-Keys.

Only the telephone ResistTel IP2 / IP152 has voltaic separated input lines. ☜

Caution

With using the voltaic separated input lines the input voltage must be 21.5 V – 57 V DC if using an external power supply.

The following Options are only available for phones with an illuminated keypad.

Incoming Call Alert Blinking Period [ticks]	Blinking period of an illuminated keypad during an incoming call. 1 Tick corresponds to a period of 40 ms. (25 Ticks ≙ 1 Hz). With an empty field, the keypad will not blink during incoming calls.
Registration Alert Blinking Period [ticks]	Blinking period of an illuminated keypad during a registration alarm. 1 Tick corresponds to a period of 40 ms. (25 Ticks ≙ 1 Hz). With an empty field, the keypad will not blink during a registration alarm. A registration alarm will become active, if at least one of at registration options marked registrations is marked at Phone/User-x/General (with x=1…6) as enabled and the state is not up.

Registration Options

Registration	Description
active	The registration at Phone/State/Registrations as active marked will be used for controlling the relay.
1	Registration 1
2	Registration 2
3	Registration 3

4	Registration 4
5	Registration 5
6	Registration 6

4.8.7 Menu Extended-Preferences

The menu Extended-Preferences has the following possibilities for setup:

H323: No Faststart Protocol Option	The on default enabled protocol option faststart can be disabled by checking the box.
H323: No H245 Tunneling Protocol Option	The on default enabled protocol option tunneling can be disabled by checking the box.
No Extended fast Connect Protocol Option	The on default enabled protocol option extended fast connect can be disabled by checking the box.
Show IP Address of Caller	With the protocol option show IP address of caller the IP address of the caller with a suppressed calling number will be displayed. This function is only available for the protocol H.323.

SIP/TSIP/SIPS: Gatekeeper Port	With the protocol option gatekeeper port, the port number for the gatekeeper/registrar can be defined. The default port number is: • protocol H323: 1720 • protocol SIP: 5060 • protocol TSIP: 5060 • protocol SIPS: 5061 Input: • 0: Default port number, if this is the primary registration otherwise wildcard port number (0) • 65535: Wildcard port number • 1 – 65534: Defined port number
Local Music on Hold off	With the protocol option local MoH off the local acknowledgement tone can be suppressed, if the PBX sends no MoH.
Do not Prefer E164-Number	Do not Prefer the E164 number, if the E164 number and the H323-ID (name) are available.
Do not Propagate Name Identification	Do not propagate the name identification to the application layer.

4.9 Main Menu Services

4.9.1 Menu HTTP

4.9.1.1 Submenu Server

Here, the access parameters of the web configuration are set. It is possible to protect the configuration in an easy way.

Force HTTPS	Allow only HTTPS sessions. HTTP requests are redirected to HTTPS requests. On the first request after enabling this feature some browsers may not accept redirection of the XSL file, in this case the reload button of the browser helps.
Disable HTTP basic authentication:	For HTTP basic and digest authentication is supported by the device. With basic authentication the password is transmitted as clear text, which is a security risk if someone can listen to this communication. Digest authentication only transmits a hash code of the password which is of no use for a listener. To avoid the vulnerability of the basic authentication it can be disabled, but some applications may not support the digest authentication, which in turn do not work anymore if basic authentication is disabled.
Password protect all HTTP pages	Apart from the start page Configuration/General/Info, all areas of the user interface are password protected. If this checkmark is set all pages are password protected.
Port	As default port 80 is used for HTTP. With this field it can be changed to any other value (e.g. 8080).
HTTPS-Port	As default port 443 is used for HTTPS. With this field it can be changed to any other value.
Allowed stations	Access to the device can be restricted to a particular network (for example, 192.168.0.0 / 255.255.0.0) or to a particular host (for example, 192.168.0.23 / 255.255.255.255).

The following is a line for line list of the active HTTP/HTTPS sessions with the parameters:

- From (IP-Address)

- Protocol
- To (Application)
- Uptime
- Idle
- Requests

4.9.1.2 Submenu Client

Some files that the device must access via HTTP (update commands (Refer to chapter 4.9.3 beginning on page 304), MoH, announcements, voicemail, etc.) may be located in a password-protected area. A list of URLs with the respective user names and passwords can be configured. The URLs in the list usually specify only the path to a file (or a part of it). The longest match of the list defines the user name and the password used for authentication required when establishing a connection.

Note

As soon as a line is completed, the entry fields for the next parameter appear.

Entry fields in a line:

- URL
- User
- Password

Proxy Servers:

	Host	Port
HTTP Proxy	Proxy server used for HTTP requests	Port for the HTTP Proxy Server

HTTPS Tunnel Proxy	Proxy server used for HTTPS requests	Port for the HTTPS Proxy Server

No Proxy Server for:

Input parameter of a line:

- Address
- Mask

☞	**Note** As soon as a No Proxy Server for line is completed and transferred with clicking ok, the input fields for the next line will appear.

Domain Suffix:

Input parameter of a line:

- Domain Suffix (Networks and domains which can be accessed without using a proxy server.)

☞	**Note** As soon as a Domain Suffix line is completed and transferred with clicking ok, the input fields for the next line will appear.

4.9.2 Menu NTP

The device can synchronize its internal date/time to an NTP server using the SNTP protocol. Without synchronization to an NTP server the internal date/time is reset to January 1st, 1970 0:00 after each restart.

As NTP servers only deliver UTC time (corresponds to Greenwich Mean Time), and due to their operating principle cannot deliver any information about daylight saving time, in order to calculate the local time either a rule (POSIX conformable) must be entered.

Configuration:

Entry field	Description
Time Server 1	The IP-Adresse of the first time server
Time Server 2	The IP-Adresse of the second time server
Interval [min]	The time interval (in minutes) at which the device tries to synchronise with the time server.
Timezone	Select the time zone in which the device is located. • Other • Europe – Central European Time (UTC + 1) • Europe – East European Time (UTC + 2) • Europe – West European Time (UTC) • USA – Alaska Time (UTC - 9) • USA – Aleutian Islands (UTC - 10) • USA – Arizona (UTC - 7) • USA – Atlantic Time (UTC - 4) • USA – Central Time (UTC - 6) • USA – Eastern Time (UTC - 5) • USA – Hawaii (UTC - 10) • USA – Indiana (UTC - 5) • USA – Mountain Time (UTC - 5)

Entry field	Description
	• USA – Pacific Time (UTC - 8)
String	If the timezone to be used is not one of the predefined timezones, it can be configured with a string in accordance with the IEEE POSIX standard.

Timezone Configuration String

Time services always provide the coordinated world time UTC (Universal Time Coordinated), which corresponds to GMT (Greenwich Mean Time), not however the correct time zone and summer time. It is therefore possible to specify the time difference between the time zone and the world time in the String field. The difference from the time zone GMT+1 (Central European time zone) is 60 minutes. A further 60 minutes has to be added with summer time, adding up to a total difference of 120 minutes. In this case, however, you must adjust the time difference manually when switching from winter to summer time and vice versa.

If a so-called timezone string was entered in the String field, the device can make the switch from summer to winter time automatically. The name of the time zone, the name of the summer time zone and their respective differences in time compared to the UTC and the time switch points are encoded in this field.

There are various formats for the specification of this string. These formats are defined by the IEEE POSIX standard. POSIX timezone strings have the following format (optional parts in square brackets):

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

Std stands for the time zone (for example, CET for Central European Time or MET for Middle European Time).

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

Dst stands for the summer time zone (for example, CEST for Central European Summer Time or MEST for Middle European Summer Time).

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

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

Example

The Central European time zone is specified **CET-1CEST-2,M3.5.0/2,M10.5.0/3**:

CET (Central European Time) - offset -1

CEST (Central European Summer Time) - offset -2

Switch to Summer Time at 3(March), 5(last week of the month), 0(Sunday)/at 2:00

Switch to Standard Time at 10(October), 5(last week of the month), 0(Sunday)/at 3:00

Display field

- Current Server: IP address of the current time server
- Last sync: Time of last synchronisation

4.9.3 Menu Update

On this page the VoIP telephone can be configured to poll an update server (a normal web server). A file pointed to by an URL is read from the update server and executed. This is an efficient mechanism to keep a large number of devices up to date.

Entry field	Description		
Command File URL	An URL, for example http://192.168.0.1/update/script-ip150.txt, is pointing to a file whose commands are executed. If the URL ends with a slash '/', for example http://192.168.0.1/update/, the device is adding the file name update-ipxxx.htm automatically, deduced from the device short name (for example update-ip150.htm). These placeholders may be used e.g. to address a device-specific directory (http://192.168.1.2/update/#h/script.txt) or to generate HTTP-GET parameters (http://192.168.0.1/update/script.php?mac=#m). Some standard parameters are always appended to the query part of the URL:		
	name	value	example
	ver	human readable version information	6.00 dvl-sr1 IP150[07-60600.03], Bootcode[145], HW[104]
	BOOT	last serial for **boot** command	145
	PROT	last serial for **prot** command	07-6060003
	BMC	last serial for **bmc** command	
	CFG	last serial for **cfg** command	
	SCFG		

	CHECK	last serial for **check** command	20070511-01
	CFG-BACKUP-NUM	last backup number for **scfg** command	
	If access to the command file requires authentication, it must be configured within the HTTP-Client of the device.		
Interval [min]	An interval (in minutes) at which the file is re-read and executed. To restrict the update to certain hours (e.g. only during the night), there are mechanisms within the available commands to restrict the execution of the commands. The polling of the command file cannot be restricted.		

The **Current Update Serials** section shows the values of the variables set after last successful execution of the associated command. These values are provided as standard parameters in the query part of the URL

Name	Command	Description
BOOT	boot	With the boot command, the boot code is updated.
PROT	prot	To initiate a firmware update.
BMC	bmc	The bmc command allows you to update the burst mode controller' firmware.
CFG	cfg	
SCFG	scfg	

Name	Command	Description
CHECK	check	In most cases, however, the maintenance file should be executed not every time as soon as it is received, but once only. Assuming that a secure configuration is to be loaded onto several devices, it is best, if this is done from one device. This can be achieved with the check command.
CFG-BACKUP-NUM	scfg	If the UP0 interface is being used, then the device configuration can be stored on a Web server.

4.9.3.1 Configuration of the Update-Server

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

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

There are two modules in the device which work in tandem. The first is known as "UP0" and actually executes the upload and download of configuration information as well as the update of the firmware. UP0 is controlled by commands as detailed below. The second module is known as "UP1". It serves to poll a given website for changed configuration information. If certain conditions are met, UP1 will issue commands to UP0 to perform the requested updates.

4.9.3.1.1 System Requirements

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

4.9.3.1.2 Installation

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

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

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

4.9.3.1.3 Configuration

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

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

If the URL happens to end with a '/', then a standard file name based on the product description is used. If, for example, the URL is http://1.2.3.4/configs/ , then it is extended in the case of an IP150 as follows: http://1.2.3.4/configs/update-ip150.htm. The product name is specified in the first line in chapter "Configuration/General/Info". The file extension is irrelevant here. The extension *.txt or *.htm or no file extension at all is possible. In relation to URL specifications note, that some Web servers differentiate between upper case and lower case letters.

4.9.3.1.4 Running Maintenance

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

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

4.9.3.1.5 Maintenance Commands

Additional commands implemented specially for the update server are available. The maintenance file is executed every time (depending on the interval set), as soon as it is received.

4.9.3.1.6 Check Command

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

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

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

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

- **ireset**: Resets the device as soon as it is not being actively used.
- **reset**: Resets the device immediately.
- **iresetn**: Resets the device as soon as it is not being actively used and a reset is required.
- **resetn**: Resets the device immediately if a reset is required.
- **ser**: no-op

4.9.3.1.7 Times Command

Often, configuration changes shall be made only during certain times (e.g. non-working hours). This can be achieved using the times command:

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

The times command will check the current time against <hours>. If it does not match this restriction, any further processing of the command file is cancelled. <hours> is a comma separated list of hours. Only those hours listed are considered valid times for execution of the command file.

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

will allow command executions only between 12:00 and 12:59 and 22:00 and 4:59 local time (on a 24h clock). Note that if the device has no time set (yet), all command executions will be cancelled.

If the /initial parameter is set, then no commands will be executed within the first <minutes> minutes after the device has been booted. This is done to avoid firmware download and flashing when installing devices.

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

will suppress any command file processing within the first six minutes after each boot of the device. If /initial is set, for new devices (or those that have been reset to factory settings), the command file will be retrieved even if it normally would be suppressed by the /allow parameter. This allows new devices to retrieve a site specific standard configuration quickly.

4.9.3.1.8 Prot Command

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

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

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

If the <url> parameter ends with a slash ('/'), a standard firmware file name is appended to the URL depending on the product description (for example, IP152.bin for an IP system).

```
mod cmd UP0 prot http://192.168.0.10/firm/ip152.bin ireset 04-
5656
```

The command

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

determines whether the firmware version 04-5656 was already installed. If this is not the case, the current firmware is downloaded from the address 192.168.0.10/firm/ip152.bin, the UPDATE/PROT internal variable is overwritten with 04-5656 and, finally, the device is reset as soon at it is not being actively used.

4.9.3.1.9 Boot Command

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

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

The command

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

determines whether the boot code version 205 was already installed. If this is not the case, the current boot code is downloaded from the address 192.168.0.10/firm/boot152.bin, the UPDATE/BOOT internal variable is overwritten with the version number of the downloaded boot code (205) and, finally, the device is reset as soon as it is not being actively used.

Since V6.00 sr2-hotfix3 the commands "reboot" and "ireboot" are available and should be used to reset the device after boot code update to activate it. The system is run down the same way as with "reset" and "ireset" but finally a watchdog restart is forced instead of a soft restart.

4.9.3.1.10 BMC Command (only for DECT Devices)

With the bmc command, the DECT radio code (aka burst mode controller firmware or BMC code) is updated and this is done in the same way as with the prot command.

```
mod cmd UP0 bmc <url> <final-command> <build-serial>
```

The name of the file to use must be given explicitly here (the file name appended to an <url> parameter ending with a slash ('/') has no ".bin" suffix like the delivered file).
The command

```
mod cmd UP0 bmc http://192.168.0.10/firm/ccfp1200.bin ireset
PCS04fd
```

determines whether the DECT radio code PCS04fd was already installed. If this is not the case, the current DECT radio code is downloaded from the address 192.168.0.10/firm/ccfp1200.bin, the UPDATE/BMC internal variable is overwritten with PCS04fd and, finally, the device is reset as soon at it is not being actively used.

4.9.3.1.11 SCFG Command

```
mod cmd UP0  scfg <url> [<final-command> <save-serial> [
/force <hours> ]]
```

This will cause the device to upload its current configuration to <url>. This will be done using an HTTP PUT command. <url> must be writable thus. Within <url>, some meta character strings are replaced as follows:

Sequence	Replacement	Example
#F	kernel build number	09-7030014
#fn	first n digits of kernel build number after the dash	70300
#B	boot code build number	09-7030012
#H	hardware build number	102
#h	device hardware ID	IP152-03-0d-f0
#n	device name	RadioOne
#m	MAC address of the device	00-50-c2-6a-50-01
#d	current date and time	20051010-170130
#bn	rolling backup index	3
#i	(one of) the local ip-address(es)	192.168.0.1
#N	network (that is, IP address with host bits set to 0)	192.168.0.0
#t	device type	IP152
##	escapes a hash mark	#

This meta character strings are available in the URL of SCFG command and in the Update Server URL only.

The rolling backup index loops over 0 .. n-1 for each backup and can only be used once in an update script. That means more than one SCFG command in a script with a usage of the rolling backup index will overlap and produce unexpected results.

Beginning with V7.00 the optional Parameters <final-command>, <save-serial> and /force <hours> will be recognized.

<final-command> defines the command to be executed after successful completion of scfg (typically no-op is used).

<save-serial> is compared to the UPDATE/SCFG variable. If it is not equal, the command is started. If it is equal and /force is not specified the command is skipped, otherwise /force is evaluated.

/force <hours> specifies the number of hours after which scfg is executed again even if <save-serial> has not changed.

```
mod cmd UP0  scfg http://192.168.0.10/configs/saved/#h#b5.txt
no-op WEEKLY /force 168
```

will save the device configuration once per week with a backlog of 5 weeks.

4.9.3.1.12 CFG command

A configuration file may be loaded using the CFG command:

```
mod cmd UP0 cfg <url> <final-command> <serial>
```

The file will be read, all configuration commands in there executed and a final config write appended. Please note that no activation will be done implicitly. Thus, you will likely either use reset as <final-command> or use ser and have a config activate and iresetn follow.

4.9.3.1.13 Common Problems

The update tab will show the update client status. Common error message include:

- not polled. The client has not (yet) polled the command script. This is probably because the script is polled the first time only *after* the interval has expired.
- failed (401). The client has no sufficient access right to read the command script from the HTTP server.
- failed (404). The update command script does not exist. You probably misspelled the path or name.
- failed (502). Might indicate problems with a proxy server on the far end. However, the HTTP client currently generates 502 for badly formed URLs also (e.g. `http:172.31.2.3/drive/cf0/update/update-all.txt`). Please note that URLs must not contain host names.

Generally, numeric error codes in parentheses (such as failed (401)) are taken from the last HTTP error code received by the update client. More about HTTP error codes can be found in the German and English Wikipedia.

4.9.4 Menu Logging

Log Server:

Due to the fact that VoIP telephones only have a limited memory, the necessary logging can be stored in other devices. Here, you set the protocol and the parameters for accessing the external storage destination. Three procedures are at your disposal for storing these data. The actual configured values are displayed next to the input fields.

Type: Off	Logging is disabled.
Type: TCP	The entries are written to a TCP connection. The other end of the TCP connection is then responsible for the further evaluation of the entries. • If the TCP connection shall be automatically established, you enter the target IP address under „Address". • In „Port", you enter the TCP port number of the connection.
Type: SYSLOG	The entries are reported to a syslog server in the network. This takes care of the further evaluation or storage. • Enter the syslog IP address under „Address". • Choose the syslog report category in „Class". The syslog class is a numeric value between 0 and 7.

Type: HTTP /
Type: HTTPS
	The entries are transmitted to a web server for further processing. Every single entry is transferred to the web server as form data in the HTTP GET format.
	
	• Enter the web server's IP address under „Address".
	
	• In „Port", you enter the HTTP/HTTPS port number of the connection.
	
	• In „Method" you select the access method. The following methods are selectable:
	
	  ○ Standard
	
	  ○ External (GET)
	
	  ○ External (POST)
	
	• In the web server, at „Path", you enter the relative URL of the form software. This is only for use with the methods External (GET) and External (POST).
	
	The device will make a HTTP/HTTPS GET request to the Web server on the entered URL, followed by the URL-encoded syslog entry. If, for example, a page named /cdr/cdrwrite.asp with a form that expects the log message in parameter msg exists on a Web server, then the value /cdr/cdrwrite.asp is entered. The device will then make a GET /cdr/cdrwrite.asp?event=syslog&msg=logmsg request to the Web server.

Type: REMOTE-AP / Type: REMOTE-AP-S	The logs are transmitted to the REMOTE-AP (Remote Linux Application Platform) Server. With REMOTE-AP-S a scrambled transmission will be used. • In the Address field, you enter the IP address of the REMOTE-AP-Servers. • In the Port field, you specify the port to which the REMOTE-AP connection is set up.

Alarm and Event Forward Server:

Type	Type of the alarm and event forward server can be selected: • off • HTTP • HTTPS • REMOTE-AP • REMOTE-AP-S
Address	The address of a HTTP/HTTPS or REMOTE-AP/ REMOTE-AP-S server to forward alarms and faults to.
Port	IP port of the HTTP/HTTPS or REMOTE-AP/ REMOTE-AP-S server, defaults to 80 for HTTP and 443 for HTTPS.
Method	Access method for the HTTP/HTTPS server. Standard External (GET) External (POST)
Path	The Request-URI to send in the HTTP/HTTPS request, e. g. '/log/fault.asp'. Current config yields ". This is valid only for the methods External (GET) and External (POST)

Local Alarm and Event Queues:

Memory Queue Entries	Maximum number of faults and alarms to hold in volatile memory (DRAM), default: 100.
Persistent Queue Entries	Maximum number of alarms to keep in flash memory, default: 50.

4.9.5 Menu SNMP

The VoIP device allows the operating state to be monitored using **SNMP** (Simple Network Management Protocol with version 1.0). Standard MIB II and a manufacturer-specific MIB (Management Information Base) are supported. The phone uses the standard Ports for SNMP, UDP Port 161 and UDP Port 162 for SNMP traps, and they are not changeable. The information is only available to be read (Commands GET and TRAP).

Community	If the standard community name „public" is not being used, a different community name can be entered in this field.
Device Name	For more detailed information, a device name can be specified here for the SNMP agent.
Contact	As can a contact person (Contact).
Location	As can a location (Location).
Authentication Trap	Access via SNMP is only possible if the correct community name is entered. If this check box is checked, a trap is generated in the case of access with an incorrect community name.
Trap Destinations	Destinations for trap messages also have to be defined if the device is to trigger the traps defined in the manufacturer-specific MIB.

Allowed networks	To increase security, access to the device can be restricted by restricting SNMP access to a defined list of computers or IP address ranges. The List is restricted to 5 entries. To disable SNMP access completely just enter *0.0.0.0* as *Address* and *255.255.255.255* as *Mask*.

4.9.6 Menu Telnet

Using this switch, the configuration can also be allowed for the Telnet protocol.

The device can be configured with commands such as reset, config change UP1 /url <http url> /poll <secs>, for example.

All Admin Accounts can have access via Telnet. Viewer accounts do not have access; also Kerberos Accounts do not have access (as the Password is send unencrypted via Telnet).

4.9.7 Menu DNS

4.9.7.1 Supported DNS Resource Records Types

Type	Value (decimal)	RFC	Description	Function
A	1	1035	Address Record	Returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host, but also used for DNSBLs, storing subnet masks in RFC 1101, etc.
AAAA	28	3596	IPv6 Address Record	Returns a 128-bit IPv6 address, most commonly used to map hostnames to an IP address of the host.
CNAME	5	1035	Canonical Name Record	Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name.
MX	15	1035	Mail Exchange Record	Maps a domain name to a list of message transfer agents for that domain
NAPTR	35	3403	Naming Authority Pointer	Allows regular expression based rewriting of domain names which can then be used as URIs, further domain names to lookups, etc.
NS	2	1035	Name Server Record	Delegates a DNS zone to use the given authoritative name servers.
PTR	12	1035	Pointer Record	Pointer to a canonical name. Unlike a CNAME, DNS processing does *NOT* proceed, just the name is returned. The most common use is for implementing reverse DNS lookups, but other uses include such things as DNS-SD.

Type	Value (decimal)	RFC	Description	Function
SOA	6	1035	Start of Authority Record	Specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.
SRV	33	2782	Service Locator	Generalized service location record, used for newer protocols instead of creating protocol-specific records such as MX.

4.9.7.2 Submenu Hosts

A local database of static DNS resource records can be administrated. This might be useful in *SIP Federation* scenarios or for training purposes.

The records provided in this database are used by the local DNS client to resolve local requests, prior to ask a configured DNS server.

In case the device is used as DNS relay, the relay functionality is not affected by this records.

Local Resource Records	The local database of static DNS resource records is going to be displayed here.
New Resource Record	A new resource record can be added: • Select the desired type of resource record from the drop-down list. • Complete the resource record and click on **OK**.

Possible Status/Error texts are:

Status/Error Text	Description
Success/0	Standard DNS success response
Format Error/1	Standard DNS error response
Server Failure/2	Standard DNS error response
NXDOMAIN/Name Error/3	Standard DNS error response
Not Implemented/4	Standard DNS error response
Refused/5	Standard DNS error response

Local Timeout/16	Local proprietary error response • A timeout maximum was exceeded
Local Error/17	Local proprietary error response • The box's DNS configuration is empty or wrong. • The user's input for a DNS query may not be acceptable.

Below Local Resource Records the local DNS host are listed. Each line begins with the type (SRV, AAAA, A). The additional parameters correspond to the parameters at the input of new resource records.

Furthermore additional DNS host can be inserted below New Resource Record.

Type A: DNS Host with the following parameters:

Parameter	Description
Name	Hostname, e. g.: gateway.example.com
IP Address	IP Version 4 Address

Type AAAA: DNS Host with the following parameters:

Parameter	Description
Name	Hostname, e. g.: gateway.example.com
IP Address	IP Version 6 Address

Type SRV: (Service) DNS Host with the following parameters:

Parameter	Description
Name	Name (service + protocol + domain), e. g.: _sip._udp.example.com
Target	Destination host name, e. g.: gateway.example.com
Port	UDP/TCP port number
Priority	Priority
Weight	Weight

4.9.7.3 Submenu Query

Two parameters can be entered at the left side.

Parameter	Description
Domain Name	Domain name, to be searched for.
Type of Resource Record	Resource Record Type • A (Address Record) • NS (Name Server Record) • CNAME (Canonical Name Record) • SOA (Start of Authority Record) • PTR (Pointer Record)

	• MX (Mail Exchange Record) • AAAA (IPv6 Address Record) • SRV (Service Locator) • NAPTR (Naming Authority Pointer)

The search can be started by clicking on.

The error code of the search will be displayed in the first line at the right side

Error code	Description
0	Success
16	Local Timeout
17	Local Error

Below there are three areas:

- Answer Section
- Name Server Section
- Additional Records Section

The located records of the search will be displayed accordingly.

4.10 Main Menu Maintenance

4.10.1 Menu Diagnostics

4.10.1.1 Submenu Logging

Here, various protocols or actions can be selected to appear in syslog. The logged information is output through the 'syslog' link.

Selectable Options:

- TCP
- TCP6
- PPP
- H.323 Registrations
- SIP/UDP Registrations
- SIP/TCP Registrations
- SIP/TLS Registrations
- H.323 NAT
- Administration

4.10.1.2 Submenu Tracing

Here, various protocols or actions can be selected to appear in Trace Buffer. This information is output through the 'trace (buffer)' link. This information can be viewed through the link 'trace (continuous)', too, but through this link, all information is updated continuously.

Selectable Options:

- H.323 Signalling
- SIP/UDP Signalling
- SIP/TCP Signalling
- SIP/TLS Signalling
- NAT
- H.323 NAT
- Phone
- HTTP Client
- All TCP/UDP Traffic
- All TCP6/UDP6/ICMP6 Traffic
- Enable RPCAP (Wireshark: rpcap://<ip-address>/trace (copy to clipboard, IE only)

4.10.1.3 Submenu Alarms

In a list all happened alarms are displayed.

The following parameters are displayed in a row.

Time	
Code	
Severity	
Remote	
Source	
Description	

Clicking on the code of an alarm opens a window, showing the alarm in detail as follows:

Time	
Type	
Code	
Severity	
Source	
Description	
Registration	
Protocol	
Number	
Name	
AOR	registration account
Comment	

With the button Mark respectively Unmark an alarm message can be marked respectively unmarked.

Marked alarms are displayed with an orange, unmarked alarms are displayed with a grey code.

4.10.1.4 Submenu Events

In a list all happened events are displayed.

The following parameters are displayed in a row.

Time	Date and time
Type	Type • Alarm • Error • Alarm cleared • Alarm timed out
Code	
Severity	Severity • none • Major • Critical • Indeterminate
Remote	
Source	
Description	

The list can be deleted with the link **Clear** and can be stored in a text file on a pc with the link **Save**.

Clicking on the code of an event opens a window, showing the event in detail as follows:

Time	Date and time
Type	Type • Alarm • Error • Alarm cleared • Alarm timed out
Code	
Severity	Severity • none • Major • Critical • Indeterminate
Source	
Description	
Registration	ID <1..6>

Protocol	• H323 • SIP • TSIP • SIPS
Call	Number:Name → Number:Name
Number	
Name	
AOR	Account of registration
Response code	
Comment	
H.323	H.323 name
Media	<IP address>:<port> ↔ <IP address>:<port>
Type	Coder

With the button Mark respectively Unmark an event message can be marked respectively unmarked.

Marked events are displayed with an orange, unmarked events are displayed with a grey code.

Description of the used (error-)codes of the alarms and events.

Code	Name	Description
0x00010000	Gateway	Faults of the group Gateway
0x00010001	Gateway: Interface Down	This is an alarm which is generated, if a physical interface which is configured to be up gets down. This can be the case for ISDN interfaces configured as Point-to-Point. ISDN interfaces configured as Point-to-Multipoint are not expected to be up all the time.
0x00010002	Gateway: Registration down	This is an alarm which is generated if a configured outgoing registration is down.
0x00010003	Gateway: Protocol Error	The gateway process receives a call clearing with cause code 'Protocol Error'. This can be an indication for an interoperation problem with some other equipment.
0x00020000	PBX	Faults of the group PBX
0x00020002	PBX: Error	You have configured an obsolete pickup prefix. Pickup can be configured with the DTMF Feature Object. You have to configure a zero length string to pickup prefix to remove the alarm and the text box will then disappear.

Code	Name	Description
0x00020003	PBX: Error	An external transfer was attempted even if not allowed. The calls to be transferred were disconnected instead. External Transfer can be enabled using the 'PBX/General/Enable External Transfer' checkmark.
0x00030000	DECT	Faults of the group DECT
0x00040000	Phone	Faults of the group Phone
0x00050000	RTP	Faults of the group RTP
0x00050001	RTP: No Media Data received	No RTP packets from remote side were received on a connected call. This problem points to either a NAT problem (private RTP address was given to remote side) or a general signalling problem (media negotiation).
0x00050002	RTP: Excessive Loss of Data	This event is generated if in a period of 10s more than approximately 3% packet loss was detected.
0x00050003	RTP: Wrong Payload Type	RTP packet with wrong payload type has been received. Caused by signalling/negotiation problems (interoperability). An endpoint sends RTP packets with a payload type other than negotiated.
0x00050004	RTP: STUN failed	STUN failed

Code	Name	Description
0x00050005	RTP: SRTP Authority failed	SRTP Authority failed
0x00050006	RTP: SRTCP Authority failed	SRTCP Authority failed
0x00060000	H323	Faults of the group H323
0x00060001	H323: Unexpected Message	A message was received, which was not expected by the protocol in this state. This could be caused by network problems or by incompatible equipment.
0x00060002	H323: Status Inquiry	H323: Status Inquiry
0x00060003	H323: Signalling TCP failed	The signalling transport connection could not be established. This usually means the destination (IP) is not reachable. Check network connectivity.
0x00060004	H323: Signaling Timeout	A signaling timer expired. The reason for this could be a network problem or an interop problem.
0x00070000	SIP	Faults of the group SIP
0x00070001	SIP: NAT Discovery failed	NAT Discovery failed
0x00070002	SIP: STUN failed	STUN failed

Code	Name	Description
0x00070003	SIP: Overload	The SIP protocol stack reached its build-in memory allocation limit. The total number message allocation is limited to be saved against denial-of-service attacks. Under normal working conditions the limit should not be reached.
0x00070004	SIP: Coder mismatch	Coder mismatch
0x00070005	SIP: Media Config failed	Media configuration failed
0x00070006	SIP: DNS failed	DNS failed
0x00080000	Webmedia	Faults of the group Webmedia
0x00080001	Webmedia: Invalid URL	Invalid URL
0x00080001	Webmedia: Invalid coder in URL	Invalid coder in URL
0x00080002	Webmedia: Coder missing in URL	Coder missing in URL
0x00090000	CF Card	Faults of the group CF Card
0x00090001	CF Card: Error	The cluster chain of a file or a directory is broken. This can be caused by removing the card without unmounting it before. Be sure to run chkdsk.

Code	Name	Description
0x00090002	CF Card: Error	The next cluster of a file or a directory is out of range. This error should not occur. Be sure to run chkdsk.
0x00090003	CF Card: Error	The underlying driver returned no data. This can be caused by an invalid cluster or if the card was removed while operations are performed on it. Be sure to run chkdsk.
0x00090004	CF Card: Error	The card is full. You can buy a bigger one or delete some unnecessary files.
0x00090005	CF Card: Error	The card is unformatted or formatted with an unknown format. Be sure to format it with fat32.
0x00090006	CF Card: Error	The card has a wrong disk format. The needed format is fat32. Be sure to format it.
0x000a0000	ISDN Interface	Faults of the group ISDN Interface
0x000a0001	ISDN Interface: Error	Signalling error reported by ISDN interfaces: A broadcast packet was received on a point-to-point interface, which should not happen. This indicates that there is a configuration mismatch point-to-point/point-to-multipoint.
0x000b0000	CMD	Faults of the group CMD

Code	Name	Description
0x000b0001	CMD: Unexpected Restart	The system was restarted because of watchdog, trap or by pressing the reset button. This event is generated 60s after the restart.
0x000c0000	Security	Faults of the group Security
0x000c0100	TLS Alert Local	Faults of the subgroup Security/TLS Alert Local
0x000c0100	TLS Alert Local: Close Notify	Close Notify
0x000c010a	TLS Alert Local: Unexpected Message	Unexpected Message
0x000c0114	TLS Alert Local: Bad Record MAC	Bad Record MAC
0x000c0115	TLS Alert Local: Decryption Failed	Decryption Failed
0x000c0116	TLS Alert Local: Record Overflow	Record Overflow
0x000c011e	TLS Alert Local: Decompression Failure	Decompression Failure
0x000c0128	TLS Alert Local: Handshake Failure	Handshake Failure

Code	Name	Description
0x000c0129	TLS Alert Local: SSL no Certificate	SSL no Certificate
0x000c012a	TLS Alert Local: Bad Certificate	Bad Certificate
0x000c012b	TLS Alert Local: Unsupported Certificate	Unsupported Certificate
0x000c012c	TLS Alert Local: Certificate Revoked	Certificate Revoked
0x000c012d	TLS Alert Local: Certificate Expired	Certificate Expired
0x000c012e	TLS Alert Local: Certificate Unknown	Certificate Unknown
0x000c012f	TLS Alert Local: Illegal Parameter	Illegal Parameter
0x000c0130	TLS Alert Local: Unknown CA	A TLS connection could not be established because the CA of the remote certificate is not trusted. Check the rejected certificates for details.
0x000c0131	TLS Alert Local: Access Denied	Access Denied

Code	Name	Description
0x000c0132	TLS Alert Local: Decode Error	Decode Error
0x000c0133	TLS Alert Local: Decrypt Error	Decrypt Error
0x000c013c	TLS Alert Local: Export Restriction	Export Restriction
0x000c0146	TLS Alert Local: Protocol Version	Protocol Version
0x000c0147	TLS Alert Local: Insufficient Security	Insufficient Security
0x000c0150	TLS Alert Local: Internal Error	Internal Error
0x000c015a	TLS Alert Local: User Cancelled	User Cancelled
0x000c0164	TLS Alert Local: No Renegotiation	No Renegotiation
0x000c0200	TLS Alert Remote	Faults of the subgroup Security/TLS Alert Remote
0x000c0200	TLS Alert Remote: Close Notify	Close Notify

Code	Name	Description
0x000c020a	TLS Alert Remote: Unexpected Message	Unexpected Message
0x000c0214	TLS Alert Remote: Bad Record MAC	Bad Record MAC
0x000c0215	TLS Alert Remote: Decryption Failed	Decryption Failed
0x000c0216	TLS Alert Remote: Record Overflow	Record Overflow
0x000c021e	TLS Alert Remote: Decompression Failure	Decompression Failure
0x000c0228	TLS Alert Remote: Handshake Failure	Handshake Failure
0x000c0229	TLS Alert Remote: SSL no Certificate	SSL no Certificate
0x000c022a	TLS Alert Remote: Bad Certificate	Bad Certificate
0x000c022b	TLS Alert Remote: Unsupported Certificate	Unsupported Certificate
0x000c022c	TLS Alert Remote: Certificate Revoked	Certificate Revoked

Code	Name	Description
0x000c022d	TLS Alert Remote: Certificate Expired	Certificate Expired
0x000c022e	TLS Alert Remote: Certificate Unknown	Certificate Unknown
0x000c022f	TLS Alert Remote: Illegal Parameter	Illegal Parameter
0x000c0230	TLS Alert Remote: Unknown CA	A TLS connection could not be established because the remote party does not trust the CA of the certificate of this device.
0x000c0231	TLS Alert Remote: Access Denied	Access Denied
0x000c0232	TLS Alert Remote: Decode Error	Decode Error
0x000c0233	TLS Alert Remote: Decrypt Error	Decrypt Error
0x000c023c	TLS Alert Remote: Export Restriction	Export Restriction
0x000c0246	TLS Alert Remote: Protocol Version	Protocol Version
0x000c0247	TLS Alert Remote: Insufficient Security	Insufficient Security

Code	Name	Description
0x000c0250	TLS Alert Remote: Internal Error	Internal Error
0x000c025a	TLS Alert Remote: User Cancelled	User Cancelled
0x000c0264	TLS Alert Remote: No Renegotiation	No Renegotiation
0x000c0400	Kerberos Client	Faults of the subgroup Security/Kerberos Client
0x000c0401	Kerberos Client: Server not found	Kerberos Server not found
0x000c0402	Kerberos Client: User not found	User not found at Kerberos Server
0x000c0403	Kerberos Client: Service not found	Service not found
0x000c0403	Kerberos Client: Host unknown to Kerberos Server	The host account of the device has been deleted on the Kerberos server. Join the Kerberos realm again.
0x000c0404	Kerberos Client: Wrong Password	Wrong Password
0x000c0405	Kerberos Client: Not Authorized	Not Authorized

Code	Name	Description
0x000c0406	Kerberos Client: Server Down (Timeout)	The device did not get a response from the Kerberos server. Make sure that the Kerberos server is up and its address is well configured on the devices.
0x000c0406	Kerberos Client: Server unreachable	Server not reachable
0x000c0407	Kerberos: Cross-realm trust not configured	The user tried to log-in with a user account from a Kerberos realm that does not trust or is not trusted by the realm of the device.
0x000c0407	Kerberos: Cross-realm Password Mismatch	The password for the cross-realm trust is not the same on both of the Kerberos servers.
0x000c0407	Kerberos Client: Cross-realm failed	Cross-realm failed
0x000c0500	Kerberos Server	Faults of the subgroup Security/Kerberos Server
0x000c1000	X509 Alarm	Faults of the subgroup Security/X509 Alarm
0x000c1000	TLS: Error	Certificate validation is disabled until system time is set.
0x000d0000	Fax	Faults of the group Fax

Code	Name	Description
0x000d0001	Fax: Bad signal quality	This event is generated if the fax modem in the gateway receives a distorted analog fax signal. The fax demodulator generates an eye pattern from the fax signal that shows amplitude and phase. The quality of the eye pattern is the EQM, a value between 0 (good) and 15 (bad). Values from 10 to 15 generate this event. Changing the fax transmit level or the receive level of the analogue interface (if present) should improve the EQM.
0x000d0002	Fax: Clock offset too large	Clock offset too large
0x000d0003	Fax: Loss of data	More than 5 lost T.38 packets. Indicates a network problem.
0x000d0004	Fax: Missing Page Confirmation	Indicates one fax page was not acknowledged. This can be happen if the fax modems get out of synchronization, e.g. if slips on an ISDN interface occur during fax transmission.
0x000d0005	Fax: General Error	Indicates a problem in the T.30 or the T.38 protocol or a timing problem (incompatible fax devices, end to end delay to high).
0x000e0000	RFP	Faults of the group RFP
0x000f0000	Environment	Faults of the group Environment

Code	Name	Description
0x00100000	DECT Synchronization	Faults of the group DECT Synchronisation
0x00110000	Network	Faults of the group Network
0x00110001	Network: Interface down	Interface is down
0x00110002	Network: Interface unconfigured	Interface is not configured
0x00110003	Network: DHCP timeout	DHCP timeout
0x00110019	Network: UDP RTP port configuration error	UDP RTP port configuration error
0x0011001a	Network: UDP NAT port configuration error	UDP NAT port configuration error
0x0011001b	Network: TCP NAT port configuration error	TCP NAT port configuration error
0x0011001c	Network: RT0 misconfigured	RT0 configured not correctly
0x0011001d	Network: RT1 misconfigured	RT1 configured not correctly
0x0011001e	Network: RT2 misconfigured	RT2 configured not correctly

Code	Name	Description
0x0011001f	Network: RT3 misconfigured	RT3 configured not correctly
0x00110040	Network: IP checksum error	IP checksum error
0x00110041	Network: ARP poisoning	ARP poisoning
0x00110046	Network: TCP NAT ports exhausted	TCP NAT ports exhausted
0x00110047	Network: TCP ports exhausted	TCP ports exhausted
0x00110048	Network: TCP checksum	TCP checksum
0x00110049	Network: TCP bind error	Local error. TCP socket was trying to bind itself to a specific local port number. The port number was found to be in use by some other socket.
0x00110050	Network: UDP RTP ports exhausted	UDP RTP ports exhausted
0x00110051	Network: UDP ports exhausted	UDP ports exhausted

Code	Name	Description
0x00110052	Network: UDP checksum	UDP checksum
0x00110053	Network: UDP bind error	Local error. UDP socket was trying to bind itself to a specific local port number. The port number was found to be in use by some other socket.
0x0011005a	Network Route Error: no route	No route
0x0011005b	Network Route Error: No route through interface (Interface down)	The IP routing process failed to deliver a packet explicitly directed to a specific network interface. The network interface was either down or disabled. Packets directed to a specific network interface are used for example by DHCP (UDP) and by PPTP Tunnels (TCP/GRE). If this error is reported for UDP broadcast packets rather often it usually indicates that DHCP client mode is configured for the interface but the interface is not connected to a network or disabled. In this case the DHCP mode should be changed to disabled.
0x0011005c	Network Route Error: Interface unconfigured	Interface not configured
0x0011005d	Network Route Error: Interface no gateway	Interface is no gateway

Code	Name	Description
0x0011005e	Network Route Error: Interface loop	Interface loop
0x00120000	Box	Faults of the group Box
0x00120001	Memory: Error	This alarm indicates that there is less then 200000 bytes of memory available for allocation.
0x00130000	Flashman	Faults of the group Flash Programming
0x00130001	Flashman: Upload Error	Error during upload or save of data.
0x00140000	DECTPROT	Faults of the group DECTPROT
0x00150000	DECTCLU	Faults of the group DECTCLU
0x00160000	WLAN	Faults of the group WLAN
0x00160001	WLAN: Low Battery	The power of the battery is to low. Load or exchange battery.
0x00190000	Provision	Faults of the group Provision
0x001a0000	Unite	Faults of the group Unite

4.10.1.5 Submenu Counters

Here the desired counters can be selected.

CPU	Processor load (main)
MEM	Memory load
ETH0	Network traffic load

4.10.1.6 Submenu Config-Show

Here, the current configuration of the telephone is output in text format.

4.10.1.7 Submenu Ping

It is possible to execute a **ping** towards a particular destination host (IP address), since for test purposes it is often necessary to execute a ping command directly from the VoIP device. This makes it possible to check whether a network address (telephone, PBX, VoIP provider, etc.) is accessible. If the remote address is accessible, *Reply from <host>* is displayed. If the remote address is not accessible, *Request timed out* is displayed.

4.10.1.8 Submenu Traceroute

The Traceroute tool allows you to see how packets travel in the IP network. It shows the path taken by packets between this device and any other given remote host (IP address).

You get an ordered list of hosts (IP addresses) with the measured round trip time.

4.10.2 Menu Upload

4.10.2.1 Submenu Config

☞	**Note** Before loading the configuration again, the name and the password of the default administrators must be set to the values during save of the configuration.	☜

Here, the configurations previously saved in Menu Download Submenu Config (Refer to chapter 4.10.3.1 on page 350), are input again.

- In the field 'File', you enter the path and the file name of the configuration file you want to upload. Alternative the path and the file name can be searched and selected with the search button. With clicking the upload button the file will be loaded.

4.10.2.2 Submenu Firmware

This function enables you to transfer a new firmware version, available from your dealer, to your VoIP telephone.

Below flash status the status of the checksum of the bootcode and the firmware will be displayed.

- In the field 'File', you enter the path and the file name of the firmware file you want to upload.

- During upload of the new firmware you receive a notification, under no circumstances to interrupt the upload. If the upload process is interrupted after all, the VoIP telephone under no circumstances should be turned off. Instead the procedure should be repeated, after the problem has been solved.

- Study the documentation included with the new version to find out if also a new boot firmware has to be downloaded. If this is the case, please note also the correct sequence of download for the bootcode and firmware updates (if applicable).

- The new firmware is not activated directly. You have to perform a reset in order to activate the new version.

After the successful update of the firmware, all browser and applet windows must be closed and the browser restarted. This is required because the new firmware may also contain new interface elements, which can only be activated in this manner.

4.10.2.3 Submenu Bootcode

This function enables you to transfer a new bootcode version to your VoIP telephone. New bootcode versions are available from your dealer.

Below flash status the status of the checksum of the bootcode and the firmware will be displayed.

- In the field 'File', you enter the path and the file name of the bootcode file you want to upload.

- During upload of the new bootcode you receive a notification, under no circumstances to interrupt the upload. If the upload process is interrupted after all, the VoIP telephone under no circumstances should be turned off. Instead the procedure should be repeated, after the problem has been solved.

- The new bootcode is not activated directly. In order to activate the new version, you have to turn off the VoIP telephone and turn it back on again.

Study the documentation included with the new version to find out if a new firmware has to be uploaded, too. If this is the case, please note also the correct sequence of upload for the bootcode and firmware updates (if applicable).

4.10.2.4 Submenu Directory

Here, the configurations previously saved in Menu Download Submenu Directory (Refer to chapter 4.10.3.2 on page 351), are input again.

For input of directory entries, you can select one of three modes.

Merge	The file will be added to the existing directory. Entries with identical names will be replaced.
Import	All imported entries will be deleted before input; manual created entries will be kept.
Replace	All existing entries will be deleted before input. This function will be suitable for input of saved directories.

In the field 'File', you enter the path and the file name of the directory file you want to upload.

The following columns in comma separated value (csv) format are expected:

Surname, first name, company, telephone number, H323 identifier, notes [,..optional]

4.10.2.5 Submenu DRAM

This function makes it possible to load the new firmware into the DRAM of your VoIP phone directly. In the field „Firmware File" the path and the file name of the firmware file has to be entered.

4.10.3 Menu Download

4.10.3.1 Submenu Config

This function allows **saving the current configuration** of the VoIP device.

The device hardware ID is a combination of the internal type of the telephone and the last three bytes of the MAC address, e. g.: **IP152-6a-5e-f7**.

When clicking the **download** or **download with standard password** link, a popup page opens, in which it can be specified whether to save the configuration file as a txt file or immediately open it with an editor. To modify the configuration of the device, the configuration has to be stored in a file on the PC.

In the configuration file passwords and pin codes are encrypted.

When clicking the **download** link the default file name to save the configuration is: complete-<device hardware ID>.txt. Passwords and pin codes are encrypted with the current password of the default administrator.

When clicking the **download with standard password** link the default file name to save the configuration is: standard-<device hardware ID>.txt. Passwords and pin codes are encrypted with the default password of the default administrator.

Later input of the saved configuration is possible over the Menu Upload Submenu Config (Refer to chapter 4.10.2.1 on page 348).

☞	**Note** Before loading the configuration again, the name of the default admin and the password must be set to the values during save of the configuration.	☜

4.10.3.2 Submenu Directory

This function allows saving **the complete directory** of the VoIP device. When clicking the **Download** link, a popup page opens, in which it can be specified whether to save the configuration file as a csv file or immediately displayed with the browser.

Later input of the saved directory is possible over the Menu Upload Submenu Directory (Refer to chapter 4.10.2.4 on page 349).

The format of the directory is defined in the chapter 4.11.36 page 368.

4.10.3.3 Submenu Firmware

In this submenu the firmware of the VoIP phone can be stored as a bin-file. With clicking on the link **download firmware (ip152.bin)** or **download firmware (IP152-6a-5e-f7-ip152.bin)** a popup window will be opened in which you can specify to store the file (on a PC) or to display the file with a program.

4.10.3.4 Submenu Bootcode

In this submenu the bootcode of the VoIP phone can be stored as a bin-file. With clicking on the link **download bootcode (boot152.bin)** or **download bootcode (IP152-6a-5e-f7-boot152.bin)** a popup window will be opened in which you can specify to store the file (on a PC) or to display the file with a program.

4.10.4 Menu Reset

4.10.4.1 Submenu Idle-Reset

Reset, as soon as the VoIP telephone is in idle mode, i.e. as soon as no conversation is taking place and no menu is open on the telephone.

4.10.4.2 Submenu Reset

After confirmation, the reset is executed immediately.

4.10.4.3 Submenu TFTP

A reset is executed, following which the telephone starts in a TFTP mode. Only by means of the software gwload will you be able to access the telephone through the TFTP mode.

Caution

Only the administrator, who has received training in the use of the 'gwload' tool, is user authorised.

4.10.4.4 Submenu Bootcode

In the bootmode the phone uses a leaned Version of the firmware (minifirmware) and can be administrated with the web interface in a limited manner.

4.10.5 Menu Tuning

The **Menu Tuning** is an optional menu, which is locked as default. The activation of the menu is described in Chapter 4.11.2 on page 356.

4.10.5.1 Submenu Tuning

This function supports to setup some protocol timers.

- Prioritized TCP Connection Keepalive
  - Packet Send Interval (TCP keepalive)
  - Max Missing Responses (TCP miss alive)
- RAS Gatekeeper Registration Keepalive

- Time to Live (RAS time to live)
- Max Retries (RAS retry count)
- Request Timeout (RAS request t.o.)
- Restart Timeout (RAS restart t.o.)

4.10.6 Menu Debug

The **Menu Debug** is an optional menu, which is locked as default. The activation of the menu is described in Chapter 4.11.2 on page 356.

4.10.6.1 Submenu Leaks

This function lists all currently used dynamic buffers.

4.10.6.2 Submenu Tracing

This function supports additional configurations, to setup the tracing in the telephone. Different protocols or actions can be selected to appear in the trace buffer. With the link "Trace (buffer)" the output of these information will be carried out. With the link "Trace (contiguous)" all information will be visible too, but with this link all information will be always updated.

- Group VOIP
  - H.323/RAS
  - H.323/H.225
  - H.323/H.245
  - SIP/UDP
  - SIP/TCP
  - SIP/TLS
- Group IP
  - PPP
  - PPTP

  - PPPoE
  - DHCP
  - TCP/UDP Traffic
  - TLS Plaintext
- Group HTTP
  - Client
  - Server
  - Servlets
  - Config Cmds
  - (verbose)
- Group Update
  - Polling
  - Execution
- Group Phone
  - Signalling
  - Directories
- Group Remote PCAP
  - Enable Wireshark rpcap://<IP-Adresse>/trace
  - Trace

4.11 Special Configuration

4.11.1 General

Many special configurations cannot be configured with the web interface.

4.11.1.1 Changing the Configuration using a PC with an Editor

An easy possibility to configure such options is to edit the configuration using a PC. The configuration of the phone has to be stored on a PC using the web interface of the phone. Then the configuration file has to be edited with a text editor. Most of the options have the format:

- /option

or

- /option <parameter>

Pay attention appending an option, that between the text "/option" and the text before it a space character will be inserted. Furthermore between the text "/option" and the text <parameter> a space character must be inserted. Sometimes the searched configuration line exists more than once. In this case the new option must be appended to the last according configuration line, better it should be appended to all according configuration lines. After storing of the configuration file, it must loaded using the web interface of the phone and the phone must be restarted. The configuration file is secured with a checksum. After editing and loading the configuration file it may happens, that an error message appears und the instruction to restart the phone is missing. The error message can be ignored, if there is no input error. The reset must be executed in all cases.

4.11.1.2 Changing the Configuration using the Address Line of a Browser

For changing the configuration using the address line of a browser the commands have to be entered as follows:

http://<IP-address>/!<command>

Important: Between the IP address of the phone and the commands, there must be a slash and an exclamation mark, exactly.

4.11.1.3 Changing the Configuration using Telnet

First the protocol telnet must be enabled fort he phone. Then it is possible to login into the phone. Username and password are the same as for the web access. The commands can be entered after the prompt directly.

4.11.1.4 Commands

The actual configuration can be read with Administration->Diagnostics->Config-Show via the web interface or with the command:

```
config show
```

If an option shall be appended to a configuration line only, then this can be done with the following command:

```
config add /option <parameter>
```

If an option shall be appended to a configuration line, this can be done with the following command also. Pay attention appending an option that between "/option" and the text before a space character must be entered. Furthermore between the text "/option" and the text <parameter> a space character must be inserted.

```
config change <existing configuration line> /option <parameter>
```

If an option shall be deleted or modified, this can be done with the following command. In the config change line the configuration line must be always complete. Missing options and parameters are deleted.

```
config change <new complete configuration line>
```

The config change or config add line must be followed by the following commands.

```
config write
```

```
config activate
```

A successful exercised command will be prompted with an ok.

Depending on the command there may be a request to restart the phone.

4.11.2 Additional Configuration Menus

Additional only for special cases necessary configuration menus are always locked as default. They can be activated via configuration and will appear in the web interface of the telephone or in the menu of the phone afterwards.

- Activation of the menu group Debug:

  Append to the configuration line "config change CPU" the option "/debug".

Afterwards in the web interface of the telephone below Maintenance the group Debug with the submenus Leaks and Tracing will appear.

- Activation of the menu group Tuning:

  Append to the configuration line "config change CPU" the option "/tuning".

  Afterwards in the web interface of the telephone below Maintenance the group Tuning with the submenu Tuning will appear.

  Furthermore in the menu of the phone below Administration the submenu Tuning will appear.

To take effort of the change of the configuration menu, a restart of the telephone and afterwards a refresh or new start of the browser on the PC must be executed.

4.11.3 Configuration for Direct Dialling of IP Addresses

Tip

With direct dialling of IP addresses it is possible to make call, but it is impossible to make inquiry calls.

The message "channel not free" appearing with lifting off the handset, has to be ignored.

4.11.3.1 Backup for Failure of the Gatekeeper

Every telephone that should be able direct dialling of IP addresses during the gatekeeper isn't reachable, is being configured like the following:

- It must be sure that the telephones always have the same IP address. For this purpose there are two possibilities:
  - In the DHCP server the allocation IP-address – MAC-address must be set to fixed.
  - The telephones must be operated with local set fixed IP-addresses. This solution should be preferred, because this is insensible to a malfunction of the DHCP server

- Registration 1 has to be configured as standalone registration, a registration without using a gatekeeper. Therefore the Primary Gatekeeper Address in "Registration 1/Registration" has to be configured to 0.0.0.0.

  The Name in "Registration 1/Registration" has to be configured with the local IP address with added telephone number, e.g. "192.168.0.3#22". This enables the possibility for recall in case of IP address direct dialling, too.

  The Protocol in "Registration 1/Registration" has to be configured to H.323.

- Registration 2 has to be configured as normal registration at a gatekeeper. The values (IP-address, telephone number have to be configured at "Registration 2/Registration".

- Registration 2 has to get access to the local directory. Therefore activate "Registration 2/Directories/Local/Enable". In the local directory the Calling numbers and the IP addresses for direct dialling can be stored. On disconnect of the gatekeeper you dial from directory without problems.

- Registration 2 becomes the active registration, this registration will be used to receive and transmit calls normally. The "Phone/Registrations[Id=2]/Active" has to be set.

4.11.3.2 Test Operation without a Gatekeeper

For test purposes a few telephones can be operated with a small infrastructure (a PoE switch only) without using a gatekeeper.

Every telephone that should be able of direct dialling of IP addresses is being configured like the following:

- The telephones will be operated with locally fixed configured IP addresses.

- .Registration 1 has to be configured as standalone registration, a registration without using a gatekeeper. Therefore the Primary Gatekeeper Address in "Phone/User-1/General" has to be configured to 0.0.0.0.

  The Protocol in "Registration 1/Registration" has to be configured to H.323.

4.11.4 Protocol Options 'Faststart', 'H.245 Tunneling' and 'Extended Fastconnect'

The protocol options 'Faststart', 'H.245 tunneling' and Extended Fastconnect are always active per default. These options can be changed only with the configuration parameter of a DHCP server (see chapter 4.7.6.3 on page 283), with editing and loading of the modified configuration file and restart of the phone or with the command sequence described in chapter 4.11.1.4 on page 356.

- To disable the protocol option faststart:

  Append to the configuration line "config change PHONE SIG" the option "/no-faststart".

- To disable the protocol option H.245 tunneling:

  Append to the configuration line "config change PHONE SIG" the option "/no-h245-tunneling".

- To disable the protocol option Extended Fastconnect:

  Append to the configuration line "config change PHONE SIG" the option "/no-efc".

4.11.5 Protocol Option 'SIP-Hold'

With the protocol option 'SIP-hold' it can be modified, how a connection will be put on hold.

With "/sip-hold <number>"

0 = "inactive"	With putting the connection into hold the PBX will be send an 'inactive'. (default)
1 = "sendonly"	With putting the connection into hold the PBX will be send a 'sendonly'.
2 = "sendonly with 0.0.0.0"	With putting the connection into hold the PBX will be send a 'sendonly' and the RTP address will be set to 0.0.0.0 .

Append to the configuration line "config change PHONE SIG" the option "/sip-hold <number>". Only the numbers 1 or 2 have to be configured. Number 0 (default) will be used, if nothing is configured.

4.11.6 Protocol Option 'Local MoH off'

With the protocol option 'Local MoH off' the local MoH acknowledgement tone can be suppressed, when the PBX is sending no MoH.

Append to the configuration line "config change PHONE SIG" the option "/local-moh-off".

4.11.7 Protocol Option 'No Dial Tone'

With the protocol option 'No Dial Tone' the dial tone can be suppressed.

Append to the configuration line "config change PHONE SIG" the option "/no-dial-tone".

4.11.8 Protocol Option 'Recording without Remote Party Info'

With the protocol option 'Recording without Remote Party Info' during recording of calls the information about the remote party can be suppressed.

Append to the configuration line "config change PHONE SIG" the option "/recording-without-remote-party-info".

4.11.9 Protocol Option 'Local Call Forward'

With the protocol option 'Local Call Forward' a call forward will be entered in the phone, but not inside the PBX. An incoming call will be redirected by the phone automatically. This feature is working only, if the phone is operating and reachable by the PBX.

The supplementary service is interesting, if the PBX doesn’t support the call forwarding or if one of the protocols SIP, TSIP or SIPS is used.

Append to the configuration line "config change PHONE SIG" the option "/local-cf".

There are the following possibilities to use this feature:

- If the protocol H.323 is in use, the call forward can be entered with the normal menu function.

- If one of the protocols SIP/TSIP/SIPS is in use, then with activated local call forward option the normally suppressed call forward item in the menu will appear to be used for the feature.

- A function key call forward has to be programmed. With the function key menu (at the phone or at the web interface) a call forward can be entered for different conditions (always, busy, no response) and for different states (1, 2, 3 or 4). With the function key one of the wanted states (0, no call forwarding), 1, 2, 3 or 4) can be selected.

4.11.10 Protocol Option 'Show IP'

With the protocol option 'Show IP' the IP address of a call with a suppressed calling number can be displayed alternatively.

Append to the configuration line "config change PHONE SIG" the option "/showip".

This feature is working with the protocol H.323 only.

4.11.11 Protocol Option 'Do not Prefer E164-Number'

With the protocol option 'Do not Prefer E164-Number' the preference of the E164 number can be suppressed, if the E164 number and the H323 ID are.

Append to the configuration line "config change PHONE SIG" the option "/no-e164-prefer".

4.11.12 Protocol Option 'Do not Propagate Name Identification'

With the protocol option 'Do not Propagate Name Identification' the propagation of the name identification to the application layer can be suppressed.

Append to the configuration line "config change PHONE SIG" the option "/no-name-id".

4.11.13 Protocol Option 'Keep Alive'

With the protocol option 'Keep Alive' the number of seconds between the keep alive messages. (Default 0 seconds, no keep alive messages)

Append to the configuration line "config change PHONE SIG" the option "/keep-alive <seconds>".

4.11.14 Protocol Option 'Gatekeeper Port'

With the protocol option 'Gatekeeper Port' the port number for the gatekeeper/registrar communication can be defined.

Append to the configuration line "config change PHONE SIG" the option "/gk-port <port number>".

Default port number:

protocol	default port number
H.323	1720
SIP	5060
TSIP	5060
SIPS	5061

0	standard port number, if primary registration, otherwise wildcard port number (0)
65535	wildcard port number (0)
1 - 65534	fixed port number

4.11.15 SIP / TSIP / SIPS Protocol Parameter 'Name-ID'

The SIP / TSIP / SIPS protocol-parameter 'name-id' will be administrated by the PBX normally. Name-id is the displayed name of a caller at the called phone. Some manufacturer don't administrate this parameter not with the PBX, the parameter from the calling phone will be transported transparently. For these special cases this parameter can be inserted or changed only with editing and following loading of the configuration file of the phone.

For the registration 1:

- Append in the configuration line "config change PHONE SIG" the option "/name-id <text>". For text you should enter the name to be displayed.

For the registration 2 – 6:

- In the configuration line `vars create PHONE/USER-REG/0000<n> p %3creg+prot=’` with <n> = registrationnumber – 1 before `+coder=’` the string `+name-id=’Text’` is to be inserted.

Example for the registration 2:

```
vars create PHONE/USER-REG/00001 p %3creg+prot=’SIP’+enblock=
’2’+gk-addr=’10.10.10.1’+alt-gk=’10.10.10.201’+name-id=
’Mustermann,Maximilian’+coder=G729,60+lcoder=’G729A,30’+e164=
’7004’+/%3e
```

4.11.16 SIP / TSIP / SIPS Protocol Option 'Force Silence Compression'

With the SIP / TSIP / SIPS protocol option 'Force Silence Compression' the silence compression (Stop of the RTP stream) can be forced, even when the remote party doesn't offer the feature in the protocol.

Append to the configuration line "config change <prot>" the option "/sc".

With <prot> = SIP, TSIP or SIPS.

4.11.17 SIP / TSIP / SIPS Protocol Option Get CDPM (Called Party Number) from Request-URI

With the SIP / TSIP / SIPS protocol option 'Get CDPM (Called Party Number) from Request-URI (even on registered interfaces)' the called number can be fetched from the request URI (even on registered interfaces).

Append to the configuration line "config change <prot>" the option "/get-cdpn-from-request-uri".

With <prot> = SIP, TSIP or SIPS.

4.11.18 SIP / TSIP / SIPS Protocol Option 'Remote Domain in From'

With the SIP / TSIP / SIPS protocol option 'Remote Domain in From' the remote domain can be fetched from the absence field of outgoing calls on non registered interfaces).

Append to the configuration line "config change <prot>" the option "/remote-domain-in-from".

With <prot> = SIP, TSIP or SIPS.

4.11.19 SIP / TSIP / SIPS Protocol Option 'No T38 in Initial Offer'

With the SIP / TSIP / SIPS protocol option 'No T38 in Initial Offer' the option T38 can be suppressed during call setup.

Append to the configuration line "config change <prot>" the option "/no-t38-in-initial-offer".

With <prot> = SIP, TSIP or SIPS.

4.11.20 SIP / TSIP / SIPS Protocol Option 'Take Sendonly as Inactive'

With the SIP / TSIP / SIPS protocol option 'Take Sendonly as Inactive' the reaction during inquiry call for the keyword sendonly will be the same as for the keyword inactive.

Append to the configuration line "config change <prot>" the option "/take-sendonly-as-inactive".

With <prot> = SIP, TSIP or SIPS.

4.11.21 SIP / TSIP / SIPS Protocol Option 'Hold Notify as Inactive'

With the SIP / TSIP / SIPS protocol option 'Take Hold Notify as Inactive' the reaction during inquiry call for the keyword hold-notify will be the same as for the keyword inactive .

Append to the configuration line "config change <prot>" the option "hold-notify-as-inactive".

With <prot> = SIP, TSIP or SIPS.

4.11.22 SIP / TSIP / SIPS Protocol Option 'No Receive only'

With the SIP / TSIP / SIPS protocol option 'No Receive only' the stopping of the RTP transmit stream will be suppressed.

Append to the configuration line "config change <prot>" the option "/no-recvonly".

With <prot> = SIP, TSIP or SIPS.

4.11.23 SIP / TSIP / SIPS Protocol Option 'Registration Redirect Support'

With the SIP / TSIP / SIPS protocol option 'Registration Redirect Support' the activation of a second registration will be suppressed.

Append to the configuration line "config change <prot>" the option "/reg-redirect-support ".

With <prot> = SIP, TSIP or SIPS.

4.11.24 SIP / TSIP / SIPS Protocol Option 'No HR Notify'

With the SIP / TSIP / SIPS protocol option 'No HR Notify' the Hold Notify and the Retrieve Notify signalling will be suppressed.

Append to the configuration line "config change <prot>" the option "/no-hr-notify".

With <prot> = SIP, TSIP or SIPS.

4.11.25 SIP / TSIP / SIPS Protocol Option 'Prefer Tel URI'

With the SIP / TSIP / SIPS protocol option Prefer Tel Uri the use of telephone URI's in stead of SIP URI's will be preferred.

Append to the configuration line "config change <prot>" the option "/prefer-tel-uri".

With <prot> = SIP, TSIP or SIPS.

4.11.26 SIP / TSIP / SIPS Protocol Option 'Prefer 'PAI'

With the SIP / TSIP / SIPS protocol option 'Prefer PAI' the use of PAI's (P-Asserted Identity) will be preferred.

Append to the configuration line "config change <prot>" the option "/prefer-pai".

With <prot> = SIP, TSIP or SIPS.

4.11.27 SIP / TSIP / SIPS Protocol Option 'Prefer PAI2'

With the SIP / TSIP / SIPS protocol option 'Prefer PAI2' the use of the second PAI (P-Asserted Identity) will be preferred.

Append to the configuration line "config change <prot>" the option "/prefer-pai2".

Mit <prot> = SIP, TSIP or SIPS.

4.11.28 SIP / TSIP / SIPS Protocol Option 'Force PAI'

With the SIP / TSIP / SIPS protocol option 'Force PAI' the use of PAI's (P-Asserted Identity) will be forced.

Append to the configuration line "config change <prot>" the option "/pai".

With <prot> = SIP, TSIP or SIPS.

4.11.29 SIP / TSIP / SIPS Protocol Option 'Force PPI'

With the SIP / TSIP / SIPS protocol option 'Force PPI' the use of PPI's (P-Preferred Identity) will be forced.

Append to the configuration line "config change <prot>" the option "/ppi".

With <prot> = SIP, TSIP or SIPS.

4.11.30 SIP / TSIP / SIPS Protocol Option 'Share Local Port'

With the SIP / TSIP / SIPS protocol option 'Share Local Port' the output socket will be bound to the same local port as the listening socket is bound to (Cisco connection reuse).

Append to the configuration line "config change <prot>" the option "/share-local-port".

With <prot> = SIP, TSIP or SIPS.

4.11.31 SIP / TSIP / SIPS Protocol Option 'No Diverting Name'

With the SIP / TSIP / SIPS protocol option 'No Diverting Name' the presentation of the redirected name will be suppressed.

Append to the configuration line "config change <prot>" the option "/no-diverting-name".

With <prot> = SIP, TSIP or SIPS.

4.11.32 SIP / TSIP / SIPS Protocol Option 'No User Parameter in From'

With the SIP / TSIP / SIPS protocol option 'No User Parameter in From' the takeover of user parameter out of the from line will be suppressed.

Append to the configuration line "config change <prot>" the option "/no-user-param-in-from".

With <prot> = SIP, TSIP or SIPS.

4.11.33 SIP / TSIP / SIPS Protocol Option 'No User Parameter in To'

With the SIP / TSIP / SIPS protocol option 'No User Parameter in To' the insertion of user parameter into the to line will be suppressed.

Append to the configuration line "config change <prot>" the option "/no-user-param-in-to".

With <prot> = SIP, TSIP or SIPS.

4.11.34 SIP / TSIP / SIPS Protocol Option 'Anonymize Host'

With the SIP / TSIP / SIPS protocol option 'Anonymize Host' the output of host information will be suppressed.

Append to the configuration line "config change <prot>" the option "/anonymize-host".

With <prot> = SIP, TSIP or SIPS.

4.11.35 SIP / TSIP / SIPS Protocol Option 'Cause 21 to 403'

With the SIP / TSIP / SIPS protocol option 'Cause 21 to 403' the cause 21 will be changed to cause 403.

Append to the configuration line "config change <prot>" the option "/cause-21-to-403".

With <prot> = SIP, TSIP or SIPS.

4.11.36 SIP / TSIP / SIPS Protocol Option No Application Rerouting

With the SIP / TSIP / SIPS protocol option 'No Application Rerouting' the rerouting will be suppressed.

Append to the configuration line "config change <prot>" the option "/no-app-rerouting".

With <prot> = SIP, TSIP or SIPS.

4.11.37 SIP / TSIP / SIPS Protocol Option 'No Alert Information'

With the SIP / TSIP / SIPS protocol option No Alert Information the alert information will be suppressed.

Append to the configuration line "config change <prot>" the option "/no-alert-info".

With <prot> = SIP, TSIP or SIPS.

4.11.38 SIP / TSIP / SIPS Protocol Option 'No MS Acceptedby'

With the SIP / TSIP / SIPS protocol option' 'No MS Acceptedby' the MS accepted by parameter will not be send in the reason header of a CANCEL message.

Append to the configuration line "config change <prot>" the option "/no-ms-acceptedby".

With <prot> = SIP, TSIP or SIPS.

4.11.39 SIP / TSIP / SIPS Protocol Option 'Keep Active Endpoints'

With the SIP / TSIP / SIPS protocol option 'Keep Active Endpoints' endpoints will not be refreshing their registration during a call.

Append to the configuration line "config change <prot>" the option "/keep-active-endpoints".

With <prot> = SIP, TSIP or SIPS.

4.11.40 SIP / TSIP / SIPS Protocol Option 'Take Zero Address for Hold'

With the SIP / TSIP / SIPS protocol option 'Take Zero Address for Hold' the parameter "c=IN IP4 0.0.0.0" will be taken as request for hold.

Append to the configuration line "config change <prot>" the option "/take-zero-address-for-hold".

With <prot> = SIP, TSIP or SIPS.

4.11.41 SIP / TSIP / SIPS Protocol Option 'Remove Calling Number Capability'

With the SIP / TSIP / SIPS protocol option 'Remove Calling Number Capability' the calling number capability for mediation server will be removed.

Append to the configuration line "config change <prot>" the option "/rem-cn-capability".

With <prot> = SIP, TSIP or SIPS.

4.11.42 SIP / TSIP / SIPS Protocol Option 'Send Confidential Access Level Header'

With the SIP / TSIP / SIPS protocol option 'Send Confidential Access Level Header' the confidential access level header will be send.

Append to the configuration line "config change <prot>" the option "/cal-header".

With <prot> = SIP, TSIP or SIPS.

4.11.43 SIP / TSIP / SIPS Protocol Option 'Fixed Contact Address'

With the SIP / TSIP / SIPS protocol option 'Fixed Contact Address' the re-calculation of the local URI ((RFC-3581 for symmetrical NAT) will be suppressed.

Append to the configuration line "config change <prot>" the option "/fixed-contact-address ".

With <prot> = SIP, TSIP or SIPS.

4.11.44 SIP / TSIP / SIPS Protocol Option 'Product ID Format'

With the SIP / TSIP / SIPS protocol option 'Product ID Format' the formatting of the product ID und the version information will selected.

Append to the configuration line "config change <prot>" the option "/product-id-format <format-number>".

With <prot> = SIP, TSIP or SIPS.

The product ID information will be sent in the parameter fields of the information elements e. g.: User-Agent or Server during registration or call control messages.

For the examples the following values are used:

field	description	example
<PDID>	product ID	`ResistTel IP2`
<PDIDwoSC>	product ID without special characters and without spaces	`ResistTelIP2`
<MVI>	main version information	`9.00 dvl`
<FWR>	firmware release	`9.061019`
<FWRwoSC>	firmware release without special characters	`9061019`
<BCR>	bootcode release	`9061019`
<HWV>	hardware version	`101`

format number	format `example`
0	(<PDID>/<MVI> [<FWR>/<BCR>/<HWV>]) `(ResistTel IP2/9.00 dvl [9.061019/9061019/101])`
1	<PDIDwoSC>x<FWRwoSC>x<HWV> `ResistTelIP2x9061019x101`

4.11.45 SIP / TSIP / SIPS Protocol Option 'Separate Encryption'

With the SIP / TSIP / SIPS protocol option 'Separate Encryption' the media encryption will be offered as separated media description.

Append to the configuration line "config change <prot>" the option "/separate-encryption".

With <prot> = SIP, TSIP or SIPS.

4.11.46 SIPS Protocol Option 'No Certificate Check'

With the SIPS protocol option 'No Certificate Check' with selected protocol SIPS the check, weather the domain parameter in the registration of the phone is equal with the CN or Subject Alternate Name value from the PBX device certificate during initializing the TLS connection, will be suppressed.

Append to the configuration line "config change SIPS" the option "/no-certificate-check".

4.11.47 SIPS Protocol Option 'TLS Unchecked'

With the SIPS protocol option 'TLS Unchecked' with selected protocol SIPS the check of the remote certificate establishing the TLS socket will be suppressed.

Append to the configuration line "config change SIPS" the option "/tls-unchecked".

4.11.48 Directory Items

The IP address directory should be prepared und uploaded for all concerned telephones. The upload can be done with the function Upload/Directory from the Web-page. With the Upload/Directory function it is possible to load a file written from Excel in the CSV format (Comma Separated Values) directly.

The delimiter between the values has to be a comma.

The rows of a table have to be interpreted as follows:

rows	description
A	surname
B	name
C	organisation
D	destination calling number
E	destination H323 name
F	remarks
G	flags
H	unused
I	do not disturb
J	ringing melody
K	ringing speed
L	ringing volume
M	origination calling number (standard active registration)
N	origination H323 name (standard active registration)

From the rows A, B und C the internal name will be put together. In the internal name the contents of the rows are separated with spaces.

Row D respectively E defines the address of the calling party.

In row G the value has to be set FLAG_IP for entries dialling IP addresses, otherwise the row can be cleared.

FLAG_IP describes, that the destination H323 name (row E) defines an IP address. During dialling of such a directory entry, it is checked that the active registration is connected with the gatekeeper. In this case to connection will be established with the gatekeeper, otherwise the connection will be established with the standalone registration.

4.11.49 RTTTL

RTTTL, Ringing Tones Text Transfer Language is an often used format for ringing tones of mobile telephones.

Technical details:

A ringing tone in the RTTTL format must have the following three parts, to be recognised by a ringing tone program: The name, the default values and the notes.

For example, a RTTTL ringing tone:

name of the ringing tone: d=4, o=5, b=108: 2a4, 2e, 2d#, 2b4, 2a4, 2c, 2d, 2a#4, 2e., e, 1f4, 1a4, 1d#, 2e., d, 2c., b4, 1a4, 1p, 2a4, 2e, 2d#, 2b4, 2a4, 2c, 2d, 2a#4, 2e., e, 1f4, 1a4, 1d#, 2e., d, 2c., b4, 1a4

The three parts are separated with a colon.

- Part 1: name of the ringing tone, some characters presenting the name of the ringing tone.

- Part 2: default values (here: d=4, o=5, b=10), where "d=" is the default length of a note. In this case "4" means that each note without a length description is a quarter of a note. "8" means an eighth of a note and so on. Further on "o=" is the default octave. There are four octaves in the RTTTL-format. "b=" describes the playing speed in hits per minute.

- Part 3: The notes. All notes are separated with commas have the following content: First the optional length description, a normal music note, (c, d, e, f, g, a, b (= international tone description)). Hashes have the function of a cross. B signs aren't existing in the RTTTL format. Then follows the octave description. Missing optional descriptions are replaced with the default parameter.

4.12 Resetting of the Configuration in Case of Emergency

If the administrator password has been changed and was lost and the item ‚reset to factory default is locked', then the configuration can be reset to factory default as follows:

1. Disconnect the device from the power supply.

2. Press the menu key and let it being pressed down.

3. Connect the device with the power supply again.

4. Wait until the LCD display illumination is blinking.

5. Wait until the LCD display illumination is blinking quickly.

6. Stop pressing the menu key.

7. Wait until the LCD display illumination is flashing.

8. Disconnect the device from the power supply.

9. Connect the device with the power supply again.

5 Appendix

5.1 Safety Instructions

The manufacturer assumes no responsibility for any personal injury, damage to property or subsequent damage that can be attributed to improper use of the device. FHF Funke + Huster Fernsig GmbH, hereby declares that the device complies with all basic requirements of the European Directive 1999/5/EG.

5.1.1 Power Supply

The external power supply is designed for operation with Power over LAN or external supply. The power supply to the device can be interrupted by pulling the LAN cable only while using PoE.

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

5.1.2 Installation and Connection

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

5.1.3 Cleaning

Do not use any chemicals or abrasives.

5.1.4 Maintenance

The equipment does not require any maintenance.

5.1.5 Malfunctions

There is no need to open the device if it is operated and serviced as intended.

Do not open or reconnect faulty equipment. In this case, return the equipment to your dealer or service centre. Keep the original packaging in case you need to return the equipment, since it provides ideal protection.

Back up all entries (e.g. on a PC) to avoid losing data.

5.1.6 Disposal

When due for disposal, the device should be disposed of as electronic scrap, in accordance with local regulations.

5.1.7 Environmental Sustainability

There is no contact with hazardous materials if the telephone is used as intended. The plastics used for this device are of glass fibre reinforced partially recycled granulate. The key pad is made of indestructible V4A steel. We do not use any plastic material for our packaging. We only use part recycled cardboard and paper.

5.1.8 Warranty

Your IP telephone is a sophisticated, modern device which has been produced using state-of-the-art production equipment in order to meet high quality requirements. Only high quality components, which ensure a maximum of reliability, are used for their production.

A warranty for a faultless function of the telephone will be promised for the as delivered state only.

5.2 Menu Structure of the VoIP Telephones

```
Menu
| - Call Lists...........
|    | - Calls (combined)....
|    | - Calls (inbound).....
|    | - Calls (outbound)....
|    | - Active Recalls......
| - Directories......
|    | - Directory Input.....
|    |    | - Subscriber:
|    |    | - Number:
|    |    | - Name  :
|    |    | - Setup...............
|    |    |    | - Ringing:          On(Off)
|    |    |    | - Ringing Tone........
|    |    |    |    | - Start...............
|    |    |    |    | - Melody:      Default
|    |    |    |    | - Vol.:            Def
|    |    |    |    | - Speed:           Def
|    |    |    | - Registration........
|    | - Search (local)......
|    | - Search (external)...
|    | - Search (PBX)........
```

```
|    | - Search (combined)...
| - Messages...........
|    | - New Message..........
|    |    | - For:
|    | - Messages(incoming)...
|    | - Messages(outgoing)...
| - User Setup..........
|    | - Call Diversion.......
|    |    | - Unconditional:    Off(On)
|    |    | - Busy:             Off(On)
|    |    | - No reply:         Off(On)
|    | - Presence..........
|    |    | - Activity:............(Away, Busy, Lunch, Meeting,
|    |    |                                          Vacation)
|    |    | - Note
|    | - Do not disturb.......
|    |    | - Do not disturb:   Off(On)
|    |    | - Action:   Ringing off(Busy,Silence,Out of Office)
|    |    | - For:         Any Call(External Calls,
|    |    |                                    Internal Calls)
|    |    | - Out of Office Msg....
|    | - Call waiting: On-def.(On-once,On-mute,Off)
|    | - Number Present.:   On(Off)
| - Phone Setup.........
|    |    | - Headset           Off(On)
|    | - Direct dial.........
|    |    | - Direct dial:      Off(On)
|    |    | - Number:
|    |    | - Delay (seconds):0
|    | - Lock Phone..........
|    |    | - PIN:
|    | - Change PIN..........
|    |    | - Cur PIN:
|    |    | - New PIN:
|    |    | - New PIN:
|    | - LCD Contrast:       7
|    | - LCD Light          On(Off)
|    | - Keypad Light       On(Off)
| - User List...........
|    | - 1 <Name>..<Number> <+*>
|    |    | - Preferences.........
|    |    |    | - Language:      English
|    |    |    | - Time:          Default(24H, AM/PM)
|    |    | - Ring Melody.........
|    |    |    | - Ring Melody (int).....(ext, ret, msg)
|    |    |    | - Start................(Stop)
|    |    |    | - Melody:        Default
|    |    |    | - Vol.:              Def
```

```
|    |    |    | - Speed:             Def
|    |    | - Function Keys
|    |    |    | - 1 ....................
|    |    |    |    | - Type:      Undefined
|    |    |    |    | - Type:Destination No.
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - Number:
|    |    |    |    |    | - Announcement:     Off(On)
|    |    |    |    |    | - Prepare:          Off(On)
|    |    |    |    | - Type:        Partner
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - Number:
|    |    |    |    |    | - Intrude:           No(Conference,
|    |    |    |    |    |                             Monitor)
|    |    |    |    |    | - Display Number.......
|    |    |    |    |    |    | - calling:            On(Off)
|    |    |    |    |    |    | - connected:         Off(On)
|    |    |    |    |    | - Presence:         Off(On)
|    |    |    |    | - Type:           Park
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - Number:
|    |    |    |    |    | - Position:
|    |    |    |    |    | - Display Number.......
|    |    |    |    |    |    | - calling:            On(Off)
|    |    |    |    | - Type:         Pickup
|    |    |    |    |    | - State:                    1(2)
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - LED:                   Off(On,
|    |    |    |    |    |                       Blink,Flicker)
|    |    |    |    |    | - Display Number.......
|    |    |    |    |    |    | - calling:            On(Off)
|    |    |    |    | - Type:            mwi
|    |    |    |    |    | - State:                    1(2)
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - LED:                   Off(On,
|    |    |    |    |    |                       Blink,Flicker)
|    |    |    |    |    | - Number:
|    |    |    |    |    | - Append own Nr.:        Off(On)
|    |    |    |    |    | - Global:                Off(On)
|    |    |    |    | - Type:Call Forwarding
|    |    |    |    |    | - State:                    0(1,2,3,
|    |    |    |    |    |                                   4)
|    |    |    |    |    | - Text:
```

```
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - LED:                    Off(On,
|    |    |    |    |    |                       Blink,Flicker)
|    |    |    |    |    | - Call Diversion
|    |    |    |    |    |    | - Unconditional      Off(On)
|    |    |    |    |    |    | - Busy               Off(On)
|    |    |    |    |    |    | - No Reply           Off(On)
|    |    |    |    | - Type:     Call group
|    |    |    |    |    | - State:                    1(2)
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - LED:                    Off(On,
|    |    |    |    |    |                       Blink,Flicker)
|    |    |    |    |    | - Name:
|    |    |    |    | - Type:      Directory
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - Searching:         Combined
|    |    |    |    |    |      (Local Directory,PBX Directory,
|    |    |    |    |    |                       Ext.Directory)
|    |    |    |    | - Type:       Register
|    |    |    |    |    | - State:                    1(2)
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - LED:                    Off(On,
|    |    |    |    |    |                       Blink,Flicker)
|    |    |    |    |    | - Reg.ID:
|    |    |    |    |    | - Activate Reg.:          Off(On)
|    |    |    |    | - Type:       Activate
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - Reg.ID:
|    |    |    |    |    | - Disable act. Reg:       Off(On)
|    |    |    |    |    | - Act.next Reg.:          Off(On)
|    |    |    |    | - Type:    Ringing off
|    |    |    |    |    | - State:                    1(2)
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - LED:                    Off(On,
|    |    |    |    |    |                       Blink,Flicker)
|    |    |    |    |    | - Do not disturb............
|    |    |    |    |    |    | - Action:        Silence(Busy,
|    |    |    |    |    |    |                    Ringing off)
|    |    |    |    |    |    | - For:          Any Call
|    |    |    |    |    |    |   (External Call,Internal Call)
|    |    |    |    | - Type:   Call waiting
|    |    |    |    |    | - State:                    1(2)
|    |    |    |    |    | - Text:
```

```
|     |     |     |     |     | - Icon:
|     |     |     |     |     | - LED:                    Off(On,
|     |     |     |     |     |                         Blink,Flicker)
|     |     |     |     | - Type:Number Present.
|     |     |     |     |     | - State:                    1(2)
|     |     |     |     |     | - Text:
|     |     |     |     |     | - Icon:
|     |     |     |     |     | - LED:                    Off(On,
|     |     |     |     |     |                         Blink,Flicker)
|     |     |     |     | - Type:       Transfer
|     |     |     |     |     | - Text:
|     |     |     |     |     | - Icon:
|     |     |     |     | - Type:       Redirect
|     |     |     |     |     | - Text:
|     |     |     |     |     | - Icon:
|     |     |     |     |     | - Number:
|     |     |     |     | - Type:     Phone Lock
|     |     |     |     |     | - State:                    1(2)
|     |     |     |     |     | - Text:
|     |     |     |     |     | - Icon:
|     |     |     |     |     | - LED:                    Off(On,
|     |     |     |     |     |                         Blink,Flicker)
|     |     |     |     | - Type:        Headset
|     |     |     |     |     | - State:                    1(2)
|     |     |     |     |     | - Text:
|     |     |     |     |     | - Icon:
|     |     |     |     |     | - LED:                    Off(On,
|     |     |     |     |     |                         Blink,Flicker)
|     |     |     |     | - Type:        Hotdesk
|     |     |     |     |     | - State:                    1(2)
|     |     |     |     |     | - Text:
|     |     |     |     |     | - Icon:
|     |     |     |     |     | - LED:                    Off(On,
|     |     |     |     |     |                         Blink,Flicker)
|     |     |     |     | - Type:    Create Reg.
|     |     |     |     |     | - State:                    1(2)
|     |     |     |     |     | - Text:
|     |     |     |     |     | - Icon:
|     |     |     |     |     | - LED:                    Off(On,
|     |     |     |     |     |                         Blink,Flicker)
|     |     |     |     |     | - Registration...............
|     |     |     |     | - Type:    Delete Reg.
|     |     |     |     |     | - Text:
|     |     |     |     |     | - Icon:
|     |     |     |     | - Type:    Switch User
|     |     |     |     |     | - Text:
|     |     |     |     |     | - Icon:
|     |     |     |     |     | - Registration...............
```

```
|    |    |    |    | - Type:      Recording
|    |    |    |    |    | - State:                    1(2)
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - LED:                    Off(On,
|    |    |    |    |    |                       Blink,Flicker)
|    |    |    |    | - Type:      Bool Obj.
|    |    |    |    |    | - State:                    1(2,3,4)
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - LED:                    Off(On,
|    |    |    |    |    |                       Blink,Flicker)
|    |    |    |    |    | - Number:
|    |    |    |    |    | - Toggle:                 Off(On)
|    |    |    |    | - Type:       Presence
|    |    |    |    |    | - State:                    1(2)
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - LED:                    Off(On,
|    |    |    |    |    |                       Blink,Flicker)
|    |    |    |    | - Type: Prep. override
|    |    |    |    |    | - State:                    1(2)
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - LED:                    Off(On,
|    |    |    |    |    |                       Blink,Flicker)
|    |    |    |    | - Type:         Toggle
|    |    |    |    |    | - State:                    1(2)
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - LED:                    Off(On,
|    |    |    |    |    |                       Blink,Flicker)
|    |    |    |    | - Type:        Message
|    |    |    |    |    | - Text:
|    |    |    |    |    | - Icon:
|    |    |    |    |    | - Message....................
|    |    |    | - 2 ....................
|    |    |    | - 3 ....................
|    |    |    | - 4 ....................
|    |    |    | - 5 ....................
|    |    |    | - 6 ....................
|    |    |    | - 7 ....................
|    |    |    | - 8 ....................
|    |    |    | - 9 ....................
|    |    |    | - 10 ...................
|    |    |    | - 11 ...................
|    |    |    | - 12 ...................
|    |    |    | - 13 ...................
```

```
|     |     |     | - 14 ...................
|     |     |     | - 15 ...................
|     |     |     | - 16 ...................
|     |     |     | - 17 ...................
|     |     |     | - 18 ...................
|     |     |     | - 19 ...................
|     |     |     | - 20 ...................
|     | - 2 <Name>..<Number> <+*>
|     | - 3 <Name>..<Number> <+*>
|     | - 4 <Name>..<Number> <+*>
|     | - 5 <Name>..<Number> <+*>
|     | - 6 <Name>..<Number> <+*>
| - Administration.......
|     | - Information
|     | - IP Settings
|     |     | - DHCP Mode      Client(Server,Off)
|     |     | - IP Addresses..........
|     |     |     | - Interface IP Address
|     |     |     | - IP Address Mask
|     |     |     | - Default IP Gateway
|     |     | - VLAN
|     |     |     | — VLAN Header:      Off(On)
|     |     |     | - VLAN Identifier:
|     |     |     | - Prio. RTP Data :
|     |     |     | - Prio. Signaling:
|     | - Registration
|     |     | - Protocol:        H323(SIP,TSIP,SIPS)
|     |     | - Name:
|     |     | - Number:
|     |     | - Passw.:
|     |     | - VoIP Gatekeeper......(H323)
|     |     |     | - Gatekeeper ID
|     |     |     | - Gatekeeper IP Address
|     |     |     | - Gatekeeper IP Address
|     |     | - VoIP Gatekeeper......(SIP,TSIP,SIPS)
|     |     |     | - Gatekeeper ID
|     |     |     | - Proxy
|     |     |     | - Proxy 2
|     |     | - Options.............
|     |     |     | - Tones:      europe-pbx(europe-public,us,uk,
|     |     |     |             italy-pbx,italy-public,czech-pbx,
|     |     |     |     czech-public,sweden,france,swiss,belgium,
|     |     |     |      nederlands,norway,denmark,germany,spain,
|     |     |     |            finland,austria,ireland,australia,
|     |     |     |            newzealand,malaysia,turkey,russia,
|     |     |     |                          south africa,brazil)
|     | - Reset Configuration..
|     |     | - No..................
```

```
|     |     | - Yes..................
|     | - Tuning
|     |     | - TCP keepalive   :
|     |     | - TCP miss alive  :
|     |     | - TCP time to live:
|     |     | - TCP retry count :
|     |     | - TCP request t.o.:
|     |     | - TCP restart t.o.:
```

5.3 Declarations and Approvals

5.3.1 Declaration of Conformity ResistTel IP2 / IP152, ExResistTel IP2 / IP154

FHF Funke + Huster Fernsig GmbH declares that the telephone ResistTel IP2 / IP152 is in compliance with the requirements of the new EMC-directive 2004/108/EC, the low voltage directive 2006/95/EC and the R&TTE directive 1999/5/EU.

The conformity with the above directives is confirmed with the CE sign.

FHF Funke + Huster Fernsig GmbH
Gewerbeallee 15 - 19
D-45478 Mülheim an der Ruhr
Tel.: +49 208 8268 – 0
Fax: +49 208 8268 – 377
http://www.fhf.de

5.3.2 EC Type Examination Certificate ExResistTel IP2 / IP154

Physikalisch-Technische Bundesanstalt

Braunschweig und Berlin

(1) **EC-TYPE-EXAMINATION CERTIFICATE**

(Translation)

(2) Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres - **Directive 94/9/EC**

(3) EC-type-examination Certificate Number:

PTB 12 ATEX 2025

(4) Equipment: Telephone, type ExResistTel IP2

(5) Manufacturer: FHF Funke + Huster Fernsig GmbH

(6) Address: Gewerbeallee 15-19, 45478 Mülheim a.d. Ruhr, Germany

(7) This equipment and any acceptable variation thereto are specified in the schedule to this certificate and the documents therein referred to.

(8) The Physikalisch-Technische Bundesanstalt, notified body No. 0102 in accordance with Article 9 of the Council Directive 94/9/EC of 23 March 1994, certifies that this equipment has been found to comply with the Essential Health and Safety Requirements relating to the design and construction of equipment and protective systems intended for use in potentially explosive atmospheres, given in Annex II to the Directive.

The examination and test results are recorded in the confidential test report PTB Ex 12-20363.

(9) Compliance with the Essential Health and Safety Requirements has been assured by compliance with:

EN 60079-0:2009 **EN 60079-7:2007** **EN 60079-11:2012**
EN 60079-18:2009 **EN 60079-31:2009**

(10) If the sign "X" is placed after the certificate number, it indicates that the equipment is subject to special conditions for safe use specified in the schedule to this certificate.

(11) This EC-type-examination Certificate relates only to the design, examination and tests of the specified equipment in accordance to the Directive 94/9/EC. Further requirements of the Directive apply to the manufacturing process and supply of this equipment. These are not covered by this certificate.

(12) The marking of the equipment shall include the following:

II 2 G Ex e [ib] mb IIC T4 Gb
II 2 D Ex tb [ib] IIIC T135 °C Db

ZSEx10100e.dotm

Zertifizierungssektor Explosionsschutz
On behalf of PTB:

Braunschweig, January 24, 2013

Dr.-Ing. U. Johannsmeyer
Direktor und Professor

PHYSIKALISCH-TECHNISCHE BUNDESANSTALT 24

sheet 1/3

EC-type-examination Certificates without signature and official stamp shall not be valid. The certificates may be circulated only without alteration. Extracts or alterations are subject to approval by the Physikalisch-Technische Bundesanstalt. In case of dispute, the German text shall prevail.

Physikalisch-Technische Bundesanstalt • Bundesallee 100 • 38116 Braunschweig • GERMANY

Physikalisch-Technische Bundesanstalt

Braunschweig und Berlin

SCHEDULE TO EC-TYPE-EXAMINATION CERTIFICATE PTB 12 ATEX 2025

(13) **S C H E D U L E**

(14) **EC-TYPE-EXAMINATION CERTIFICATE PTB 12 ATEX 2025**

(15) Description of equipment

The telephone, type ExResistTel IP2 is used for voice transmission via Ethernet according to the VoIP mode (IEEE802.3). It is applied as stationary equipment in potentially explosive gas or dust atmospheres. The intended operating position of the telephone is vertically suspended on a wall.

The permissible range of the ambient temperature is -40 °C up to +60 °C.

Electrical data

Supply, DC (terminals 16 & 17)	non-intrinsically safe U_n = 19.2 ... 52.8 VDC safety-related maximum voltage: U_m = 53 VDC
Supply, PoE (terminals 11, 12, 14 &. 15)	non-intrinsically safe U_n = 24 ... 48 VDC safety-related maximum voltage: U_m = 57 VDC
LAN (terminals 8, 9, 10 & 13)	non-intrinsically safe U_n = ± 2,5 V (signal 10 BASE-TX) or U_n = ± 1 V (signal 100 BASE-TX) safety-related maximum voltage: U_m = ± 7 V (signal) U_m = 57 V DC (offset)
LAN cable shield	for terminals refer to operating instructions manual
Relay 1 and 2 (terminals 18 & 19 or 21 & 23)	non-intrinsically safe U_n = up to 250 VAC or up to 230 VDC I_{max} = up to 5 A for permissible maximum values refer to operating instructions manual) safety-related maximum voltage: U_m = 250 V

sheet 2/3

Physikalisch-Technische Bundesanstalt • Bundesallee 100 • 38116 Braunschweig • GERMANY

Physikalisch-Technische Bundesanstalt

Braunschweig und Berlin

SCHEDULE TO EC-TYPE-EXAMINATION CERTIFICATE PTB 12 ATEX 2025

Optional headset (terminals 1, 2, 3 & 4)	type of protection Intrinsic Safety Ex ib IIC, only for connection to passive circuits Maximum values: U_o = 16.4 V I_o = 220 mA P_o = 450 mW the maximum permissible external capacitance C_o is 424 nF, the maximum permissible external L/R-ratio is 78 μH/Ω the circuit is electrically connected to ground

The equipment is infallibly connected to the local equipotential bonding system.

(16) Test report PTB Ex 12-20363

(17) Special conditions for safe use

none

(18) Essential health and safety requirements

met by compliance with the standards mentioned above

Zertifizierungssektor Explosionsschutz
On behalf of PTB:

Dr.-Ing. U. Johannsmeyer
Direktor und Professor

Braunschweig, January 24, 2013

sheet 3/3

5.3.3 IECEx Certificate of Conformity ExResistTel IP2 / IP154

The IECEx certificate of conformity can be seen in the internet at the link:

http://iecex.iec.ch/iecex/iecexweb.nsf/421ce8815c53a3afc1257a1e00576486/a1c67f45a48322ebc1257b18004520b2?OpenDocument

5.3.4 Declaration of Conformity ExResistTel IP2 / IP154

EG-KONFORMITÄTSERKLÄRUNG
EC DECLARATION OF CONFORMITY
DECLARATION CE DE CONFORMITE
DECLARACIÓN DE CONFORMIDAD CE

Bezeichnung des Erzeugnisses: / Designation of Product:
Désignation du produit : / Designación del producto:

- **Telefon**
- **Telephone**
- **Téléphone**
- **Teléfono**

Gerätetyp oder Typenbezeichnung der Einzelkomponenten:
Equipment Type or Type Designation of Individual Component:
Modèle d'appareil ou désignation de modèle des composants :
Tipo de aparato o designación del tipo de los componentes individuales:

- **ExResistTel IP2**

Einschlägige EG-Richtlinie(n): / Relevant EC Directive(s):
Directive(s) CE en vigueur : / Directiva(s) CE pertinente(s):

94/9/EG: Geräte und Schutzsysteme zur bestimmungsgemäßen Verwendung in explosionsgefährdeten Bereichen
94/9/EC: Equipment and protective systems intended for use in potentially explosive atmospheres
94/9/CE: Appareils et systèmes de protection destinés à être utilisés en atmosphères explosibles
94/9/CE: Aparatos y sistemas de protección para uso en atmósferas potencialmente explosivas

Angewandte harmonisierte Normen, insbesondere:
The following harmonised standards have been applied:
Normes harmonisées appliquées, notamment :
Normas armonizadas aplicadas, especialmente:

EN 60079-0:2009
EN 60079-7:2007
EN 60079-11:2012
EN 60079-18:2009
EN 60079-31:2009

EG-Baumusterprüfbescheinigung: / EC-Type Examination Certificate:
Attestation d'examen CE de type : / Certificado de examen CE:

PTB 12 ATEX 2025

Benannte Stelle für die Überwachung:
Notified body of inspection:
Organisme notifié de contrôle:
Organismo encargado del examen:

Kennnummer:
Inspection number: /
Numéro d'identification : /
Número de examen:

0102

- Hiermit erklären wir, dass das Erzeugnis aufgrund seiner Konzipierung und Bauart sowie in der von uns in Verkehr gebrachten Ausführung den einschlägigen grundlegenden Sicherheits- und Gesundheitsanforderungen der(n) genannten EG-Richtlinie(n) entspricht.
  Bei einer nicht mit uns abgestimmten Änderung des Erzeugnisses verliert diese Erklärung ihre Gültigkeit.
- We herewith declare that the product, based on its development and type as well as on the specific design we have brought into circulation, conforms to the relevant basic safety and health requirements of the mentioned EC Directive(s).
  This declaration shall become invalid if any modification we have not authorised is made to the product.
- Nous attestons, par le présent document, que le produit a été conçu et fabriqué, quant au modèle mis en circulation par nos services, conformément aux exigences fondamentales de sécurité et de santé en vigueur de la ou des directives CE citées.
  En cas de modification du produit non convenue avec nos services, la présente déclaration perd sa validité.
- Por la presente declaramos que el producto satisface por su diseño y tipo constructivo así como en la versión comercializada por nosotros los requisitos de seguridad y salud fundamentales y pertinentes de la(s) directiva(s) CE indicada(s).
  En caso de una modificación del producto no acordada con nosotros, la presente declaración pierde su validez.

Diese Erklärung wird verantwortlich für den Hersteller / Importeur · This declaration is made on behalf of the manufacturer / importer · La présente déclaration, dont le fabricant / importateur ci-après assume la responsabilité · Esta declaración es formulada en forma responsable para el fabricante / importador

FHF Funke + Huster Fernsig GmbH
Gewerbeallee 15-19
45478 Mülheim an der Ruhr
Deutschland · Germany · Allemagne · Alemania

abgegeben durch · by the authorised signatory · est déposée par · por

Schwengers, Jörg

Name, Vorname / Surname, forename / nom, prénom / apellido y nombre

Geschäftsführung / Managing Director / Direction / Gerencia

Stellung im Betrieb des Herstellers / Position in manufacturer's company / fonction dans l'entreprise du fabricant / puesto en la empresa del fabricante

Mülheim an der Ruhr

Ort / Place / ville / Lugar

26.02.13

Datum / Date / date / Fecha

Rechtsgültige Unterschrift / Legally binding signature / signature légale / Firma válida

EG-KONFORMITÄTSERKLÄRUNG
EC DECLARATION OF CONFORMITY
DECLARATION CE DE CONFORMITE
DECLARACIÓN DE CONFORMIDAD CE

Bezeichnung des Erzeugnisses: / Designation of Product:
Désignation du produit : / Designación del producto:

- **Telefon**
- **Telephone**
- **Téléphone**
- **Teléfono**

Gerätetyp oder Typenbezeichnung der Einzelkomponenten:
Equipment Type or Type Designation of Individual Component:
Modèle d'appareil ou désignation de modèle des composants :
Tipo de aparato o designación del tipo de los componentes individuales:

- **ExResistTel IP2**

Einschlägige EG-Richtlinie(n): / Relevant EC Directive(s):
Directive(s) CE en vigueur : / Directiva(s) CE pertinente(s):

EMV Richtlinie	**2004/108/EG**	**EMC Directive**	**2004/108/CE**
NSR Richtlinie	**2006/95/EG**	**LV Directive**	**2006/95/EC**
R&TTE Richtlinie	**1999/5/EG**	**R&TTE Directive**	**1999/5/EC**
Directive CEM	**2004/108/CE**	**Directiva CEM**	**2004/108/CE**
Directive BT	**2006/95/CE**	**Directiva de baja tensión**	**2006/95/CE**
Directive R&TTE	**1999/5/CE**	**Directiva R y TTE**	**1999/5/CE**

Angewandte harmonisierte Normen, insbesondere:
The following harmonised standards have been applied:
Normes harmonisées appliquées, notamment :
Normas armonizadas aplicadas, especialmente:

EN 55016-2-3:2006
EN 55022:2010
EN 55024:2010

EN 60529:1991
EN 60950-1:2006/A12:2011
EN 60950-22:2006

EN 61000-6-1:2007
EN 61000-6-2:2005
EN 61000-6-3:2007+A1:2011
EN 61000-6-4:2007+A1:2011

Angewandte nationale Normen und technische Spezifikationen; insbesondere:
The following national standards and technical specifications have been applied:
Normes nationales appliquées et spécifications techniques, notamment :
Normas nacionales y especificaciones técnicas aplicadas, especialmente:

DIN EN 61000-4-2:2009
DIN EN 61000-4-3:2006+A1:2008+A2:2010
DIN EN 61000-4-4:2004+A1:2010
DIN EN 61000-4-5:2006
DIN EN 61000-4-6:2009

ETSI ETS 300019-2-4:2003

ETSI TBR 8 Corr 2001

- Hiermit erklären wir, dass das Erzeugnis aufgrund seiner Konzipierung und Bauart sowie in der von uns in Verkehr gebrachten Ausführung den einschlägigen grundlegenden Sicherheits- und Gesundheitsanforderungen der(n) genannten EG-Richtlinie(n) entspricht.
  Bei einer nicht mit uns abgestimmten Änderung des Erzeugnisses verliert diese Erklärung ihre Gültigkeit.
- We herewith declare that the product, based on its development and type as well as on the specific design we have brought into circulation, conforms to the relevant basic safety and health requirements of the mentioned EC Directive(s).
  This declaration shall become invalid if any modification we have not authorised is made to the product.
- Nous attestons, par le présent document, que le produit a été conçu et fabriqué, quant au modèle mis en circulation par nos services, conformément aux exigences fondamentales de sécurité et de santé en vigueur de la ou des directives CE citées.
  En cas de modification du produit non convenue avec nos services, la présente déclaration perd sa validité.
- Por la presente declaramos que el producto satisface por su diseño y tipo constructivo así como en la versión comercializada por nosotros los requisitos de seguridad y salud fundamentales y pertinentes de la(s) directiva(s) CE indicada(s).
  En caso de una modificación del producto no acordada con nosotros, la presente declaración pierde su validez.

Diese Erklärung wird verantwortlich für den Hersteller / Importeur · This declaration is made on behalf of the manufacturer / importer · La présente déclaration, dont le fabricant / importateur ci-après assume la responsabilité · Esta declaración es formulada en forma responsable para el fabricante / importador

FHF Funke + Huster Fernsig GmbH
Gewerbeallee 15-19
45478 Mülheim an der Ruhr
Deutschland · Germany · Allemagne · Alemania

abgegeben durch · by the authorised signatory · est déposée par · por

Schwengers, Jörg

Name, Vorname / Surname, forename / nom, prénom / apellido y nombre

Geschäftsführung / Managing Director / Direction / Gerencia

Stellung im Betrieb des Herstellers / Position in manufacturer's company / fonction dans l'entreprise du fabricant / puesto en la empresa del fabricante

Mülheim an der Ruhr

Ort / Place / ville / Lugar

26.02.13

Datum / Date / date / Fecha

ppa

Rechtsgültige Unterschrift / Legally binding signature / signature légale / Firma válida

6 Abbreviations

8	
802.1X	Standard for Authorisation in Computer Networks (IEEE)
802.3af	Standard for Power over Ethernet (IEEE)
A	
A	DNS-RR Address Record
AAAA	DNS-RR IPv6 Address Record
AC	Alternate Current
ACM	Avaya Call Manager
A/D	Analogue/Digital
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AOR	Account of Registration
API	Application Program Interface
ARP	Address Resolution Protocol
AS-SIP	Assured Services-Session Initiation Protocol
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
ATEX	Atmosphere Explosive
B	
BER	Basic Encoding Rules (ASN.1)
C	
CA	Certificate Authority
CCP	Compression Control Protocol
CDPN	Called Party Number
CDR	Call Detail Records
CE	Conformite Europeenne
CER	Canonical Encoding Rules (ASN.1)
CEST	Central European Summer Time
CET	Central European Time
CGN	Calling Party Number
CGPN	Calling Party Number
CLIR	Calling Line Identification Restriction
CM	Call Manager, siehe auch CUCM
CME	Call Manager Express
CNAME	DNS-RR Canonical Name Record
CNG	Comfort Noise Generation

CPN	Calling Party Number
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSS	Cascading Style Sheets
CSTA	Computer Supported Telecommunications Applications
CTI	Computer Telephony Integration
CUCM	Cisco Unified Communications Manager (Call Manager)
D	
DC	Direct Current
DECT	Digital Enhanced Cordless Telecommunications
DER	File name extension for a base64 coded certificate
DER	Distinguished Encoding Rules (ASN.1)
DES	Data Encryption Standard
DIN	Deutsches Institut für Normung
DHCP	Dynamic Host Configuration Protocol
DOM	Document Object Model
DN	Directory Number
DNS	Domain Name Server
DNSBL	DNS-based Blackhole List, Block List, or Blacklist
DNS-RR	DNS Resource Record
DRAM	Dynamic Random Access Memory
DSL	Digital Subscriber Line
E	
E.164	Standard for the international public telecommunication numbering plan (ITU-T)
EAP	Extensible Authentication Protocol
EAR	Foundation Elektro-Altgeraete Register
ECN	Encoding Control Notation (ASN.1)
EIA	Electronic Industries Alliance
EMC	Electromagnetic Compatibility
EMV	Elektromagnetische Verträglichkeit
ENUM	Telephone Number Mapping
EUI-64	64-bit Extended Unique Identifier

F	
F/FTP	Foiled / Foiled Twisted Pair Cable
FAT	File Allocation Table. A from Microsoft developed file system.
FAT32	A FAT Variant
FCC	Federal Communications Commission
FQDN	Fully Qualified Domain Name
FQTN	Fully Qualified Telephone Number
FTP	File Transfer Protocol
FTP	Foiled Twisted Pair Cable
G	
GMT	Greenwich Mean Time
GRE	Generic Routing Encapsulation
GSER	Generic String Encoding Rules (ASN.1)
H	
H.323	Higher recommendation of the ITU for protocols
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I	
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IDN	Internationalized Domain Name
IE	Internet Explorer
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.3af	Standard for PoE
IEEE 802.1X	Standard for Authorisation in Computer Networks
IETF	Internet Engineering Task Force
IIS	Internet Information Server
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISA	International Society of Automation
ISC	Internet Systems Consortium
ISDN	Integrated Services Digital Network
ISO	International Standardization Organisation
ISRAM	Internal Static Random Access Memory
ITU	International Telecommunication Union

J	
JAVA	Java is a object orientated programming language
JMS	Java Message Service
K	
Kerberos	Kerberos is a computer network authentication protocol
KPML	Keypad Markup Language
L	
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
M	
MAC	Message Authentication Code
MAC-Address	Media Access Control Address
MD5	Message Digest Algorithm 5
MEST	Middle European Summer Time
MET	Middle European Time
MIB	Management Information Base
MoH	Music on Hold
MPPC	Microsoft Point-To-Point Compression Protocol
MPPE	Microsoft Point-To-Point Encryption Protocol
MS	Microsoft
ms	Millisecond
MTBF	Mean Time between Failures
MTTF	Mean Time to Failure
MTU	Maximum Transmission Unit
MX	DNS-RR Mail Exchange Record
N	
NAPTR	DNS-RR Naming Authority Pointer
NAT	Network Address Translation
NDP	Neighbour Discovery Protocol
NS	DNS-RR Name Server Record
NTP	Network Time Protocol
O	
OBJ	Object Identifier
OUI-24	24-bit Organizationally Unique Identifier
OUI-36	36-bit Organizationally Unique Identifier

P	
P12	PKCS#12 file (see PFX)
PA	Potentialausgleich
PAI	P-Asserted Identity
PBX	Private Branch Exchange
PC	Personal Computer
PCAP	PCAP (Packet Capture) free programming interface (API), to capture network traffic.
PDU	Protocol Data Unit
PEM	File name extension for a base64 coded certificate, enclosed with -----BEGIN CERTIFICATE------ and ------END CERTIFICATE------
PEN	Private Enterprise Number
PER	Packed Encoding Rules (ASN.1)
PFX	Personal Information Exchange File (see P12)
PHP5	Skriptsprache
PIN	Personal Identification Number
PKCS	Private Key Cryptography Standards
PKI	Public Key Infrastructure
PoE	Power over Ethernet
POSIX	Portable Operating System Interface for UniX
PPE	Personal Protective Equipment
PPI	P-Preferred Identity
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunnelling Protocol
Proxy	A hardware server that acts as an intermediary between a work station user and the Internet so that an enterprise can ensure security
PTB	Physikalisch Technische Bundesanstalt
PTR	DNS-RR Pointer Record
Q	
QoS	Quality of Service

R	
R&TTE	Radio and Telecommunications Terminal Equipment
RADIUS	Remote Authentication Dial-In User Service
RAS	Registration Administration Service
RC4	RC4 (Ron's Code 4) ist eine Verschlüsselungsmethode, die 1987 von Ronald L. Rivest entwickelt wurde
RFC	Requests for Comments
RID	The Relative ID of a Windows Domain Group is the last numeric part of the Domain Group SID (Secure ID).
ROHS	Restriction of Hazardous Substances
RPCAP	Remote PCAP
RSA	Asymmetric procedure or algorithm for encryption of discrete data, named after its inventors Ronald L. Rivest, Adi Shamir and Leonard Adleman.
RSTP	Rapid Spanning Tree Protocol
RTCP	Real-Time Control Protocol
RTP	Real-Time Transport Protocol
RTTTL	Ringing Tones Text Transfer Language
S	
S/FTP	Screened / Foiled Twisted Pair Cable
SF/FTP	Screened Foiled / Foiled Twisted Pair Cable
SAX	Simple API for XML
SCCP	Skinny Call Control Protocol
SCP	Secure Copy
SDP	Session Description Protocol
SELV	Safety Extra Low Voltage
SFTP	Secure (SSH) File Transfer Protocol
SHA	Secure Hash Algorithm
SID	Windows Domain Group Secure ID
SIP	Session Initiation Protocol
SIPS	Session Initiation Protocol Secure
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
SOA	Start of Authority Record
SOAP	SOAP (originally defined as Simple Object Access Protocol) is a protocol specification for exchanging structured information in the implementation of web services in computer networks.
SRTCP	Secure Real-Time Control Protocol
SRTP	Secure Real-Time Transport Protocol
SRV	DNS-RR Service Locator
SSH	Secure Shell

SSL	Secure Sockets Layer
STP	Shielded Twisted Pair Cable
STUN	Simple Traversal of UDP over NATs
SYSLOG	SYSLOG is a standard for forwarding log messages in an IP network.
T	
TCP	Transmission Control Protocol
Telnet	Teletype Network Protocol
TFTP	Trivial File Transfer Protocol
TIA	Telecommunication Industry Association
TLS	Transport Layer Security
TNV	Telecommunications Network Voltage
ToS	Type of Service
TSIP	TCP Session Initiation Protocol
U	
U/FTP	Unscreened / Foiled Twisted Pair Cable
U/UTP	Unscreened / Unshielded Twisted Pair Cable
UDP	User Datagram Protocol
UL	Underwriters Laboratories Inc.
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTC	Universal Time Coordinated
UTP	Unshielded Twisted Pair Cable
V	
VAD	Voice Activity Detection
VB	Visual Basic
VIP	Very Important Person
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
W	
WebDAV	Web-based Distributed Authoring and Versioning
WEEE	Waste Electrical and Electronic Equipment
WINS	Windows Internet Name Service
WLAN	Wireless LAN
WSDL	Web Service Description Language

X	
X.509	ITU-T standard for a public-key-infrastructure
X.680ff	ITU-T notation for ASN.1
X.690ff	ITU-T standards for ASN.1
XER	XML Encoding Rules (ASN.1)
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	XSL Transformation, short XSLT, is a programming language for the Transformation of XML-Documents.

7 Overview

7.1 Tables

7.2 Figures

8 Index

9 Technical Data

9.1 Weatherproof Telephones

Connection data	
Power supply	Power over Ethernet refer to IEEE 802.3af or external power supply
Voltage PoE	48V DC (min. 44V, max. 57V)
PoE	Class 0
Voltage external power supply without using the optional voltaic separated inputs	15 V – 57 V DC
Voltage external power supply for using the optional voltaic separated inputs	21.5 V – 57 V DC
Power requirement	12.95 W
Breaking capacity relay (optional)	240 V, 6 A, AC 24 V, 6 A, DC 32 V, 5 A, DC 45 V, 1 A, DC
Connection Ethernet	RJ45 Port (10/100 Mbit/s)
Ringing volume	Max. 98 dB(A) in 1 m distance
Housing (Height x Width x Depth) without cable screw caps	267 x 225 x 132 mm
Weight (default version)	ca. 5.0 kg
Display	• 182 x 64 pixel • Field of view ca. 78 mm x 26 mm
Keypad	• Metal keypad with ice protection • 21 keys with ABC marking
Hook switch	Reed contact without mechanical switch
Operating utilization position	Vertical wall mounting
Handset	
Mouthpiece	Electret-foil microphone
Receiver inset	Dynamic receiver inset with magnetic field generator
Sling holder	Integrated adjustable sling holder
Handset cable	Armed court

Environmental conditions	
Ambient operating temperature	-40°C…+70°C
Transport and storage temperature	-40°C…+80°C
Conformities	
Degree of protection	IP66 acc. to EN/IEC 60529
Degree of protection against external mechanical impacts	IK09 acc. to EN/IEC 62262
Declaration of Conformity	Directive 1999/5/EU (R&TTE) Directive 2004/108/EG (EMC) Directive 2006/95/EG (low voltage)
Restriction of Hazardous Substances (ROHS)	Directive 2011/65/EG
Waste Electrical and Electronic Equipment (WEEE)	Directive 2012/19/EG EAR registration no.: DE 58023377
User interface	
Web-interface (administration)	English
Telephone (user menu)	16 languages adjustable

9.2 Explosion Proof Telephones

Connection data	
Power supply	Power over Ethernet refer to IEEE 802.3af or external power supply
Voltage PoE	48V DC (Min. 44V, Max. 57V). The power has to be transmitted at 10/100 Mbit/s Ethernet connections only with the unused pairs of data lines.
PoE	Class 0
Voltage external power supply	19.2 V – 52.8 V DC
Power requirement	12.95 W
Switching power relays	250 V, 5 A, 100 VA AC 230 V, 0.5 A, 100 W DC 50 V, 1 A, DC 30 V, 5 A, 100 W DC
Connection Ethernet	Terminals (10/100 Mbit/s)
Ringing volume	Max. 95 dB(A) in 1 m distance

Housing	
Material	Glass-fibre reinforced polyester
(Height x Width x Depth) without cable screw caps and without earth bolt	267 x 225 x 132 mm
Weight	ca. 6.0 kg
Display	• 182 x 64 pixel • Field of view ca. 78 mm x 26 mm
Keypad	• Metal keypad with ice protection • 21 keys with ABC marking
Hook switch	Reed contact without mechanical switch
Operation general purpose	Vertical wall mounting. The device must be mounted on a closed rear panel.
Handset	
Mouthpiece	Electret-foil microphone
Receiver inset	Dynamic receiver inset with magnetic field generator
Sling holder	Integrated adjustable sling holder
Handset cable	Armed court
Environment conditions	
Operation environment	-40°C…+60°C
Transport and storage temperature	-40°C…+80°C according to EN/IEC60721
Air humidity	75 %
Conformities	
Degree of protection	IP66 according to EN/IEC 60529
Degree of protection against external mechanical impacts	IK09 according to EN/IEC 62262
Declaration of Conformity	Directive 1999/5/EU (R&TTE) Directive 2004/108/EG (EMC) Directive 2006/95/EG (low voltage) Directive 94/9/EC (ATEX)
Restriction of Hazardous Substances (ROHS)	Directive 2011/65/EG
Waste Electrical and Electronic Equipment (WEEE)	Directive 2012/19/EG EAR registration no.: DE 58023377
EC Type Examination Certificate	PTB 12 ATEX 2025
Marking	II 2 G Ex e [ib] mb IIC T4 Gb II 2 D Ex tb [ib] IIIC T135°C Db
IECEx Certificate of Conformity	IECEx PTB 13.0007
Marking	Ex e [ib] mb IIC T4 Gb Ex tb [ib] IIIC T135°C Db

Employed standards (extracts)	• IEC/EN 60079-0 • IEC/EN 60079-7 • IEC/EN 60079-11 • IEC/EN 60079-14 • IEC/EN 60079-18 • IEC/EN 60079-31 • IEC/EN 60529 • IEC/EN 60721 • IEC/EN 60950-1 • IEC/EN 60950-22 • IEC/EN 61000-6 • IEC/EN 62262
User interface	
Web-interface (administration)	English
Telephone (user menu)	16 languages adjustable

Electric and electronic devices carrying this symbol may contain substances harmful to people and the environment. Therefore, it must not be disposed of together with unsorted municipal waste (household rubbish). In order to protect the environment please use public collecting points for the disposal of electric and electronic devices carrying this symbol.

Subject to alterations
or errors

FHF Funke + Huster Fernsig GmbH

Gewerbeallee 15-19 · D-45478 Mülheim an der Ruhr
Phone +49 / 208 / 82 68-0 · Fax +49 / 208 / 82 68-286
http://www.fhf.de · e-mail: info@fhf.de