



SwyxDECT 700 Installation and Configuration

As of: June 2019

© 2000-2019 Swyx Solutions GmbH. All rights reserved.

Legal Information

This documentation is subject to constant change and may therefore contain inaccurate or erroneous information.

Trademark: Swyx, SwyxIt! and SwyxON are registered trademarks of Swyx Solutions GmbH. This documentation is proprietary intellectual property of Swyx Solutions GmbH. Reproduction, adaptation, or translation of this documentation without the express written consent of Swyx Solutions GmbH is prohibited and will be prosecuted as a violation of intellectual property rights.

Swyx Solutions GmbH

Emil-Figge-Str. 86

D-44227 Dortmund

www.swyx.com

Contents

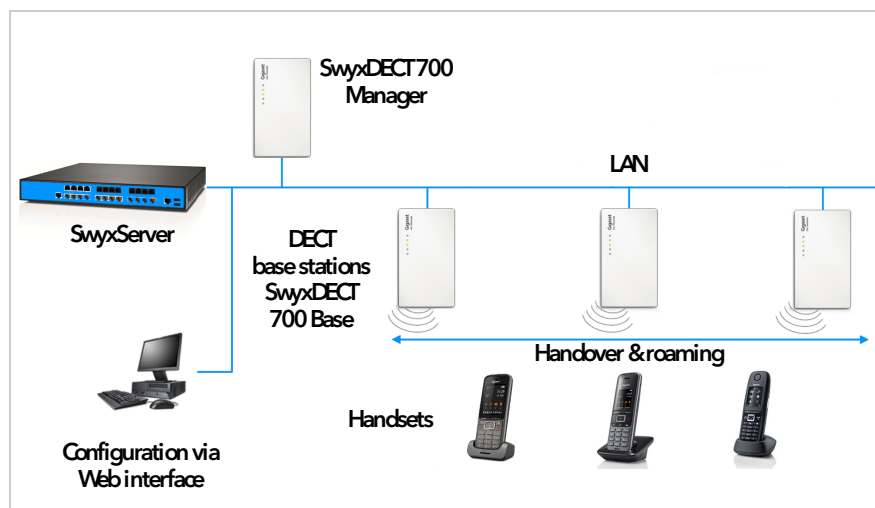
Introduction	3
Safety precautions	5
First steps	6
3.1 Checking the package contents	6
3.2 Installing base stations and DECT Manager – procedure	6
3.3 Connecting base stations and DECT Manager	7
3.3.1 Connecting the power cable	7
3.4 Connecting devices to the local network and to the Internet	8
3.5 Mounting devices on the wall	9
3.6 Preparing to use the telephone system	9
3.6.1 Registering base stations to the DECT Manager	9
3.6.2 Registering handsets and assigning VoIP accounts	10
Operating information	12
4.1 Light emitting diodes (LED)	12
4.2 Resetting the device settings	13
System settings	15
5.1 Date and time	15
Configuring the system on the DECT Manager	16
6.1 Using the Web configurator	16
6.2 Web configurator menu	19
6.3 Connecting the DECT Manager to the local network (LAN/router)	19
6.4 Configuring and synchronising base stations	21
6.4.1 Registering base stations	22
6.4.2 Displaying base stations, changing settings	23
6.4.3 Synchronising base stations	24
6.4.4 Base stations – displaying events	24
6.5 Security settings	24
6.6 Configuring VoIP providers	26
6.6.1 Wizard for selecting provider profiles	26
6.7 Configuring handsets	27
6.7.1 Registering a handset	28
6.7.2 Extended settings for handsets	29
6.8 Additional settings for making a call	32
6.8.1 Activating the area code for local calls using VoIP	32
6.8.2 Additional VoIP settings	33
6.9 Info services	36
6.10 Online directories	36
6.10.1 Public Online Directories	36
6.10.2 Corporate directories	37
6.11 Device management	39
6.11.1 Additional device settings	40
6.11.2 Saving and restoring settings	40
6.11.3 Rebooting the system	41
6.11.4 System Log (SysLog)	42
6.11.5 Updating firmware for the base/downgrading firmware updates	42
6.12 DECT Manager and base station status	43
6.12.1 Status	43
Diagnostics	44
7.1 Systemreport (SysLog)	44
7.2 Displaying of base station events	45
7.3 System dump	45
7.4 DECT network graphics	45
Help and Support	48
8.1 Questions and answers	48
8.2 Information on operating VoIP telephones with routers with Network Address Translation (NAT)	49
8.2.1 Typical problems caused by NAT	49
8.2.2 Possible solution	49

- 8.3 Checking service information 51
- 8.4 Environment 51
 - 8.4.1 Environmental management system 51
 - 8.4.2 Disposal 51
- 8.5 Appendix..... 52
 - 8.5.1 Care 52
 - 8.5.2 Contact with liquid 52
 - 8.5.3 Authorisation SwyxDECT 700 Base 52
 - 8.5.4 Specifications 52
- Glossary..... 54
- Accessories 64

1 Introduction

SwyxDECT 700 is a DECT multicell system for connecting DECT base stations to a VoIP PABX. It combines the options of IP telephony with the use of DECT telephones.

The following illustration shows the components of the SwyxDECT 700 and the way the system is embedded in the IP telephone environment:



DECT Manager: SwyxDECT 700 Manager

Central management station for managing the DECT network. One DECT Manager must be used for each installation. The DECT Manager

- Manages up to 30 DECT base stations
- Manages up to 100 handsets on multicell systems
- Enables division in up to 10 subnets (**Cluster** formation)
- Represents the interface to an IP PABX

The DECT Manager offers a Web user interface for the configuration and administration of the DECT network.

Getting started with the DECT Manager, see 3.2 *Installing base stations and DECT Manager - procedure*, page 6.

Configuring the DECT network using the Web user interface, see 6 *Configuring the system on the DECT Manager*, page 16.

SwyxDECT 700 Base DECT base stations

- These are the cells of the DECT telephone network.
- Each base station can manage up to eight calls simultaneously.

Getting started with the base stations, see 3.2 *Installing base stations and DECT Manager - procedure*, page 6.

Configuring the base stations, see 6.4 *Configuring and synchronising base stations*, page 21.

Handsets

- Up to 100 handsets can be connected and 30 DECT connections can be made simultaneously (calls, email checks, connections to online directories and the Info Centre).
- Subscribers can accept or initiate calls in all DECT cells with their handset (**Roaming**), and can also switch between the DECT cells during a call (**Handover**). A handover is only possible within the same cluster.

Configuring handsets, see 6.7 *Configuring handsets*, page 27.

Forming clusters with the SwyxDECT 700

You can divide DECT base stations that you have installed at your location into several independent groups, i.e., clusters, and manage them using one SwyxDECT 700 Manager DECT Manager (see 6.4.3 *Synchronising base stations*, page 24).

This means DECT domains that are a long way apart can be managed from a central point. The DECT Manager is connected to the base stations and the PABX via the local network and is therefore not dependent on DECT ranges. It guarantees access to the centrally configured IP connections, directories etc. However, a handover of handsets between clusters is not possible.

Planning your DECT wireless network

Careful planning of your DECT wireless network is the prerequisite for successful operation of the SwyxDECT 700 with good call quality and adequate call options for all subscribers in all the buildings and areas belonging to the PABX. When deciding how many base stations are needed, and where these should be positioned, both the requirements

for the capacity of the PABX and its wireless coverage, as well as many ambient conditions, must be taken into consideration.

The "SwyxDECT 700 Site Planning and Measurement Guide" will make it easier for you to plan your multicell DECT network, explain the necessary preparatory work for the installation and describe how to carry out measurements in order to find the best positions for your base stations. Please read these instructions before starting installation.

Swyx also offers the SwyxDECT 700 SPK PRO (Site Planning Kit) to help you measure the wireless coverage and signal quality on your DECT network. Information about setting up and using the measuring equipment can also be found in the "SwyxDECT 700 Site Planning and Measurement Guide".

2 Safety precautions



Read the safety precautions and the user guide before use



The device cannot be used in the event of a power failure. In case of a power failure it is also not possible to make emergency calls.



Do not use the devices in environments with a potential explosion hazard (e.g. paint shops).



The devices are not splashproof. For this reason do not install them in a damp environment such as bathrooms or shower rooms.



Use only the power adapter indicated on the device.

Use only the cable supplied for LAN connection and connect it to the intended ports only.



Use only rechargeable batteries that correspond to the specification (see 8.5.4 **Specifications**, page 52). Never use a conventional (non-rechargeable) battery or other battery types as this could result in significant health risks and personal injury. Rechargeable batteries, which are noticeably damaged, must be replaced.



If you give your device to a third party, make sure you also give them the user guide.



Remove faulty devices from use or have them repaired by our Service team, as these could interfere with other wireless services.



Do not use the device if the display is cracked or broken. Broken glass or plastic can cause injury to hands and face. Send the device to our Service department to be repaired.



Using your telephone may affect nearby medical equipment. Be aware of the technical conditions in your particular environment, e.g. doctor's surgery. If you use a medical device (e.g. a pacemaker), please contact the device manufacturer. They will be able to advise you regarding the susceptibility of the device to external sources of high frequency energy (for the specifications of your product see *Specifications*, page 52).

3 First steps

3.1 Checking the package contents



1. One SwyxDECT 700 Manager DECT Manager or
2. One SwyxDECT 700 Base station



The SwyxDECT 700 devices are powered by Power over Ethernet (PoE). If you do not use an Ethernet switch with PoE functionality and require a power adapter to connect to the mains power supply, you can order this as an accessory.

Firmware updates

Whenever there are new or improved functions for your device, firmware updates are made available for you to download to your DECT Manager and your base station.

3.2 Installing base stations and DECT Manager - procedure



Read the "SwyxDECT 700 Site Planning and Measurement Guide" before you start installing the devices.

- When installing the base stations, please take into account the technical conditions for positioning and the installation guidelines, which are described in the "SwyxDECT 700 Site Planning and Measurement Guide".
- Install the base stations at the positions you determined when planning or measuring your DECT wireless network.
- The SwyxDECT 700 Manager (DECT Manager) can be installed anywhere within the range of the local network. It does not need to be installed in the coverage area of the DECT wireless network.
- The SwyxDECT 700 Base base stations and the SwyxDECT 700 Manager are intended for wall mounting, see *Mounting devices on the wall*, page 9.



The devices are designed for use in dry rooms with a temperature range of +5°C to +45°C.



Never expose the devices to heat sources, direct sunlight or other electrical appliances. Protect your device from moisture, dust, corrosive liquids and fumes.

3.3 Connecting base stations and DECT Manager

To be able to make calls with your SwyxDECT 700 via VoIP, the following conditions must be fulfilled:

- The DECT Manager is installed
- Your DECT Manager and base station are connected to the local network, see *Connecting devices to the local network and to the Internet*, page 8.
- At least one base station is registered, see *Registering base stations to the DECT Manager*, page 9.
- At least one handset is registered to the telephone system, see *Registering handsets and assigning VoIP accounts*, page 10.

Perform the following steps in the specified sequence, first for the DECT Manager and then for all the base stations to be installed:

- 1 Connect the power cable to the device and connect to the mains power supply, if necessary.
- 2 Connect the base to the router/switch to access the local network and configure via the Web configurator.
- 3 Fix the device to the planned position on the wall.

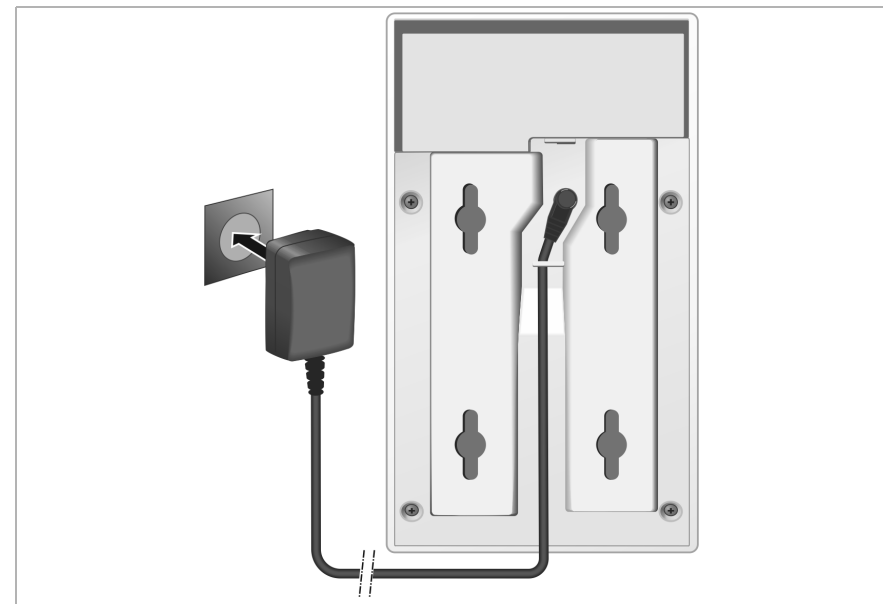


Your SwyxDECT 700 is supplied with sufficient power via PoE (Power over Ethernet) if the device is connected to an Ethernet switch with PoE functionality (PoE class IEEE802.3af). In this case, you do not need to connect the device to the main power supply and step 1 can be omitted.

3.3.1 Connecting the power cable



This connection is only required if the device is not powered via PoE. If you do not use PoE, the power adapter must be plugged in at all times for operation, as the device will not work without a power supply.



- 1 Insert the power cable of the power adapter into the connection socket at the rear of the device.
- 2 Insert the cable into the cable recess provided.
- 3 Insert the power adapter into the mains socket.



Use only the power adapter recommended in the Accessories section, see **Power adapter**, page 64.

3.4 Connecting devices to the local network and to the Internet

When the device is connected to the Internet, it automatically contacts the support server to make it easier for you to configure the devices and to enable communication with Internet services.

For this purpose, the DECT Manager sends the following information when the system is started and then every five hours:

- Serial number/item number
- MAC address
- IP address for the Device on the LAN/its port numbers
- Device name
- Software version

The following data is transmitted once every day:

- Number of registered handsets
- Information for each handset: DECT identifier (IPUI), device type, user name and display name

On the support server, this information is linked to the existing device-specific information:

- System-related/device-specific passwords

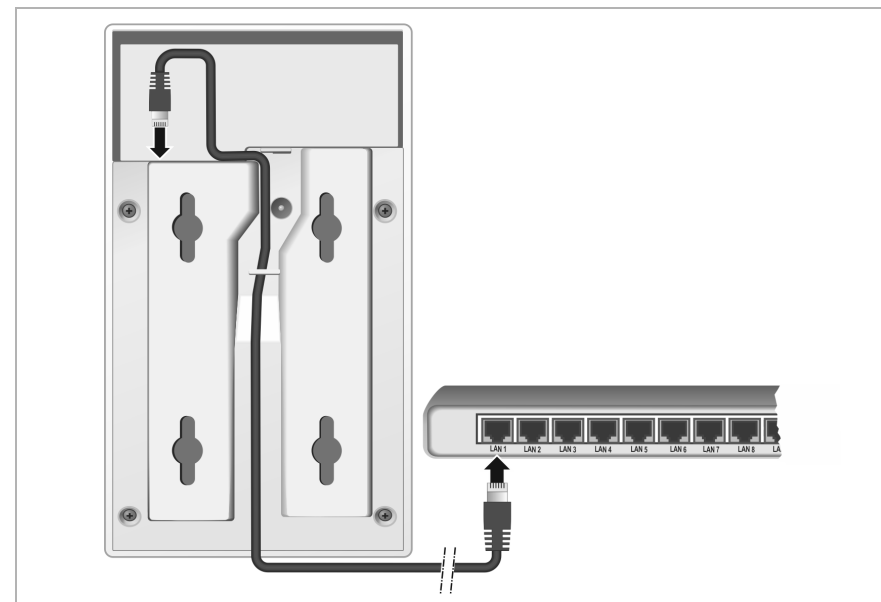
The base stations and DECT Manager have a LAN connection, which you use to connect the device to your local network via a switch/hub or directly with a router. A VoIP PABX is required for Internet telephony. This must be accessible via the local network and must have network access (to the Internet and/or the analogue or ISDN telephone network). Otherwise it will only be possible to make calls within the LAN.

You also need a PC connected to the local network, so that you can configure your telephone system via the Web configurator.



Each base station contains two DECT modules with their own MAC address, which are connected to a LAN port via an integral Ethernet switch.

To prevent security warnings, you will need to allow MAC address cascading on your corporate network.



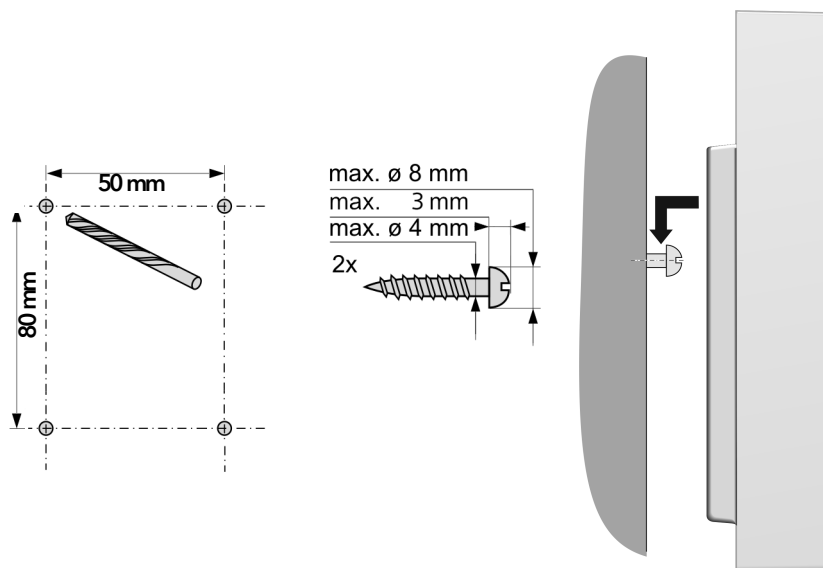
- 1 Insert a plug from the Ethernet cable supplied (Cat 5 with 2 RJ45 modular jacks) into the LAN connection socket at the rear of the device.
- 2 Insert the second Ethernet cable plug into a LAN socket for your local network or on the router.
- 3 Insert the cable into the cable recess provided.

3.5 Mounting devices on the wall

SwyxDECT 700 Base station and SwyxDECT 700 Manager are intended for wall mounting.

You can fix the device to the wall with two or four screws:

- 1 Drill holes with the following spacing:
Horizontal: 50 mm, vertical: 80 mm.
- 2 Affix wall plugs and secure the screws. Let the screws protrude by approx. four mm.
- 3 Hang the device on the screws.



3.6 Preparing to use the telephone system

To start using your SwyxDECT 700, you must now perform the following steps:

- Register base stations to the telephone system and synchronise them
- Register handsets to the telephone system, configure and assign VoIP accounts

3.6.1 Registering base stations to the DECT Manager

Before starting to register the base stations, please ensure that you have the installation plans available, which you created during the planning phase of your DECT network.

You need the MAC address of the installed base stations and the following planning data:

- Name, location
You can select any name for the base station. This should contain its location, to enable the relevant SwyxDECT 700 Base to be found quickly for maintenance purposes.
- Synchronisation level
Base stations that combine to form a DECT wireless network must synchronise with one another to ensure a smooth transition of the handsets from cell to cell (handover).
As a base station in a multicell DECT network often has an inadequate connection to some of the other base stations, you must set up a synchronisation hierarchy.
Detailed information about synchronisation planning can be found in "SwyxDECT 700 Site Planning and Measurement Guide".
- Cluster structure
Groups of base stations that are a long way apart must be assigned to different clusters.



Synchronisation always refers to a cluster. You can set up several clusters that are not synchronised with one another, so there is no possibility of a handover between clusters.

To register the base stations, set up clusters and define the synchronisation hierarchy, please use the Web configurator on the DECT Manager.

This is described in section [Configuring the system on the DECT Manager](#).

Registering base stations

- 1 Open the Web configurator and log in (see [Logging into/off the Web configurator](#), page 16).
- 2 Open the "Settings | Network and Connections | Base Station Registration" page (see 6.4.1 [Registering base stations](#), page 22).
 - ✓ The window shows a list of all DECT base stations connected to the local network which have not yet been registered. The base stations are identified by their MAC address and by the date and time of their initial contact with the system.
- 3 Register all the base stations that are to belong to your telephone system, as described in section [Registering base stations](#).

Synchronising base stations and forming clusters

- 1 Open the "Settings | Network and Connections | Base Station Synchronization" page (see 6.4.3 [Synchronising base stations](#), page 24).
 - ✓ The registered base stations are displayed.
- 2 Assign each base station to a cluster.
If you only want to manage one cluster, assign all the base stations to the same cluster number.
- 3 Assign the planned synchronisation level to each base station.
Be aware that synchronisation level one can only be assigned once.
- 4 Save your settings.
 - ✓ Synchronisation starts automatically. If synchronisation is successful, this is indicated by the DECT 1 / DECT 2 LEDs on the SwyxDECT 700 Base base stations (see 4.1 [Light emitting diodes \(LED\)](#), page 12).

3.6.2 Registering handsets and assigning VoIP accounts

All the handsets to be used for making calls on the SwyxDECT 700 must be registered on the DECT Manager. When registering, the handset is permanently assigned a VoIP connection as the receive and send connection.

Up to 100 handsets can be connected.

Setting up VoIP connections

Before you start registering the handsets, please make sure that there are sufficient accounts available from your local VoIP PABX or from a VoIP provider, and that you have the login data to hand. You can set up accounts from a maximum of ten different providers.

First configure the VoIP connections.

- 1 Log in to the Web configurator (see [Logging into/off the Web configurator](#), page 16).
- 2 Open the "Settings | VoIP Providers" page and create an entry for each provider (see 6.6 [Configuring VoIP providers](#), page 26).

Registering the handset



If auto-provisioning is provided by the manufacturer, operator or supplier of the telephone system, handsets are automatically registered to the DECT multicell system and assigned to a VoIP connection. In this case, you need to carry out only step b) in the steps described below.

Handset registration must be initiated in parallel on the DECT Manager (a) and on the handset (b). To do so, the handset must be located in at least one cell of the DECT network, i.e., close to a base station which is registered on the DECT Manager.

a) On the DECT Manager

- 1 Open the Web configurator and log in (see [Logging into/off the Web configurator](#), page 16).

- 2 Open the "Settings | Handsets" page (see 6.7 **Configuring handsets**, page 27) and press the "Add" button. You can decide whether you want to set up a handset with new data, or transfer the data from a handset that has already been set up.
- 3 Select the VoIP provider from the list and enter the login data for the account the handset is to use to make calls.
- 4 Start registering the handset for this account.
 - ✓ The DECT Manager is now ready for registering. A registration PIN is generated and displayed.

b) On the handset

- 1 Start the registration procedure on the handset in accordance with the handset's user guide.
 - ✓ A message appears on the display stating that the handset is searching for a base that is ready for registration.
 - ✓ If the handset has found a base, you will be asked to enter the registration PIN.
- 2 Enter the four-digit registration PIN, produced on the DECT Manager, on the handset.

c) On the DECT Manager

- 1 Confirm the message "Mobile device registered" by clicking "OK".
 - ✓ Once registration is complete, the handset returns to idle status. The handset name is shown in the display. If not, repeat the procedure.



The handset name is either the Username or Display name for the VoIP account to which the handset is assigned. You can set this in the Web configurator, see 6.7 **Configuring handsets**, page 27.

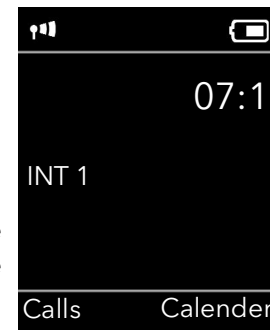
Immediately after registration, the handset is assigned the VoIP connection as the receive and send connection (incoming calls are signalled on the handset and can be answered).

You can now make calls with the handset.

Displays

- Reception between the base station and the handset:
 - Good to poor:
 - No reception: (red)

If several base stations are within range, the connection quality to the base station with the best reception is displayed.
- Battery charge status:
 - Empty to full:
 - Batteries almost empty: (flashes red)
 - Charging:
- Name of the handset

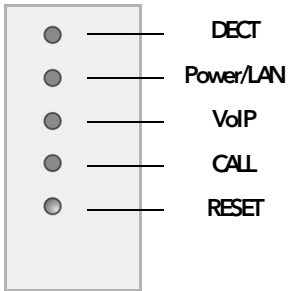


Depending on the device type, you can register your handset on other individual base stations or on a SwyxDECT 700 (up to four).

4 Operating information

4.1 Light emitting diodes (LED)

LEDs on the DECT Manager



From top to bottom

- Connection status to the base stations
- Power supply status If the power supply is OK, the LED indicates the LAN connection status.
- VoIP connections status (activation and registration)
- Active call display
- Reset button (see *Resetting the device to factory settings*, page 13)

DECT	Power/LAN	VoIP	CALL	Description
Off	Off	Off	Off	No power supply / No supply voltage
Off	Flashes (every two seconds)	Off	Off	No LAN connection or waiting for address to be assigned by the DHCP server
Off	On	Off	Off	IP address assigned by DHCP, VoIP service not (yet) available
Off	On	Flashes (every four seconds)	Off	At least one VoIP service activated, waiting for SIP registration
Off	On	On	Off	All activated VoIP services successfully registered

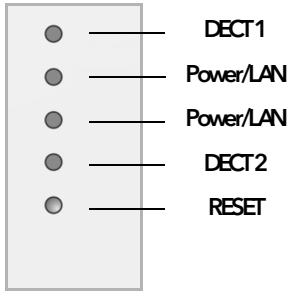
Flashes (every four seconds)	On	On	Off	At least one base station connected
On	On	On	Off	All registered base stations connected
On	On	On	On	At least one active call
Off	Flashes (every two seconds)	Flashes (every two seconds)	Off	Firmware is being updated

Other displays:

- The second LED from the top ("Power/LAN") flickers when you are restoring the factory settings to indicate that the resetting process will begin as soon as you release the reset button (see *Resetting the device to factory settings*, page 13).
- All LEDs light up for one second when the device has been successfully reset to static IP addresses, see *Resetting to static IP addresses*, page 14 or to DHCP, see *Resetting to dynamic addressing (DHCP)*, page 14.

LEDs on the base stations

The SwyxDECT 700 Base base stations contain two DECT modules with separate status displays.



From top to bottom

- Status of DECT module 1
- Power supply status If the power supply is OK, the LED indicates the LAN connection status.
- Status of DECT module 2
- Reset button (see *Resetting the device to factory settings*, page 13)

Power/LAN 1/ 2	DECT 1/2	Description
Off	Off	No power supply / No supply voltage
Flashes (once a second)	Off	The base station is looking for the DECT Manager
On	Off	Connection established to DECT Manager, base station service not yet ready
Flashes (every two seconds)	Off	Firmware is being updated, base station service not active
On	On	Base station DECT module ready, DECT synchronised
On	Flashes (every four seconds)	Base station DECT module ready, DECT not synchronised
Flashes (every four seconds)	On	Base station DECT module overloaded, DECT synchronised
Flashes (every four seconds)	Flashes (every four seconds)	Base station DECT module overloaded, DECT not synchronised

Other displays:

- The second LED from the top ("Power/LAN") flickers when you are restoring the factory settings to indicate that the resetting process will begin as soon as you release the reset button, see *Resetting the device to factory settings*, page 13.



You can deactivate the base station LED displays using the Web configurator on the DECT Manager, see **Deactivating LEDs on the base stations**, page 40.

4.2 Resetting the device settings

The devices have a reset button that you can use to restore the default device settings.

This button is below the LEDs on the front of the device.



Resetting the device to factory settings



This function resets all the settings you have made. The procedure deletes the saved data from the base stations and handsets. The base station's assignment to the DECT Manager is cancelled.

This operation is available on the DECT Manager and on the base stations.

- 1 Disconnect the power supply.
- 2 Press and hold the reset button.
- 3 Reconnect the device to the mains power supply while the reset button is depressed.
- 4 Release the reset button again when the second LED from the top ("Power/LAN") starts flickering.
 - ✓ The device is reset to the factory settings.



If the device is powered via PoE, you must remove the LAN cable to interrupt the power supply.

Resetting the IP configuration and password

The two procedures described below reset the DECT Manager's IP configuration settings and the password for registering on the DECT Manager.

You will need to use this function if you can no longer access the system, e.g., because you have forgotten the password for the Web configurator or you are experiencing problems accessing the LAN.

You can reset the IP configuration either to specific static IP addresses or to dynamic addressing (DHCP). You will then be able to access the DECT Manager again and you can change the password or LAN configuration if required, see **Logging into/off the Web configurator**, page 16.

All the LEDs on the DECT Manager light up for one second to confirm that the two resetting processes have been activated successfully.

Resetting to static IP addresses

- 1 Press the reset button and hold it for four seconds.
- 2 Release the reset button.
- 3 Press the reset button again for four seconds.
- 4 Release it again.
✓ The reset is carried out. The IP configuration is now set as follows:

Parameter	Value for the reset
IP address type	Static
IP address DECT Manager	192.168.143.1
Subnet mask	255.255.0.0
Standard gateway	192.168.1.1
Preferred DNS server Alternate DNS server	192.168.1.1
Password for access to the Web configurator	admin
VLAN Tagging	Off

Resetting to dynamic addressing (DHCP)

This allows you to specify that the DECT Manager will automatically receive an IP address from a DHCP server in the local network.

- 1 Press the reset button and hold it for four seconds.
- 2 Release the reset button.
- 3 Press the reset button for one second.
- 4 Release it again.

- 5 Press the reset button again for four seconds.
- 6 Release it again.
✓ The reset is carried out. The IP configuration is set as follows.

Parameter	Value for the reset
IP address type	Obtained automatically
Password for access to the Web configurator	admin
VLAN Tagging	Off

5 System settings

System settings are made via the Web configurator on the DECT Manager (see 6 **Configuring the system on the DECT Manager**, page 16) and cannot be changed using the handsets.

This applies in particular for:

- Registering and de-registering the handset to the telephone system, handset name.
- All settings for the VoIP account used by a handset for calls.
- Settings for the network mailbox and the email account.
- Configuration of online directories.

Handset-specific settings are preset on your device. You can change these settings.

This applies, for example, for:

- Display settings, such as language, colour, backlight etc.
- Settings relating to ringtones, volume, speaker profiles etc.

Information about this can be found in the user guide for the relevant handset.

5.1 Date and time

Date and time are set in the Web configurator of the DECT Manager, see **Date and time**, page 39 and are synchronised system-wide on all base stations and handsets.

Synchronisation is carried out in the following cases:

- If the date or time has been changed on the DECT Manager.
- If a handset is registered to the telephone system.
- If a handset is switched off and switched back on again, or is outside the wireless range of the telephone system for more than 45 seconds and then comes back into range.
- Automatically every night at 4.00 am.

You can change the date and time on the handset. This setting only applies for that handset and will be overwritten when the next synchronisation takes place.

The date and time are displayed in the format set for that handset.

6 Configuring the system on the DECT Manager

Use the Web configurator to set up your SwyxDECT 700 and configure your DECT network.

- Set up the **DECT** network, register and synchronise the base stations.
- Make basic settings for the VoIP connections and register and configure the handsets you wish to use in the DECT network.
- You can make additional settings, e.g., meet particular prerequisites for connecting the handsets to a corporate network or adjust the voice quality on VoIP connections.
- Use the DECT Manager to save data required to access specific services on the Internet. These services include access to public online directories and to the incoming eMail server for eMail accounts, as well as synchronising the date/time with a time server.
- You can save your DECT Manager's configuration data as files on your PC and reload these onto your DECT Manager in the event of an error. You can arrange firmware updates for the DECT Manager.
- Manage the directories on registered handsets (save to PC, compare them with one another or against a directory on your PC).

6.1 Using the Web configurator

Connecting the PC to the Web configurator on the DECT Manager

Prerequisites:

- A standard Web browser is installed on the PC, e.g., Microsoft Internet Explorer or Mozilla Firefox.
- The DECT Manager and PC are directly connected to one another in a local network. The settings of any existing firewall installed on your PC allow the PC and DECT Manager to communicate with each other.



Depending on your VoIP PABX/VoIP provider, it is possible that you will be unable to change individual settings in the Web configurator.



While you are connected to the Web configurator, it is blocked to other users. Simultaneous access is not possible.

- 1 Launch the Web browser on your PC.
- 2 Enter **www.swyx.com/dect700config** in the address field of the Web browser.
 - ✓ The known devices with this name are displayed.
- 3 If several devices are found, select your DECT Manager using the name or the MAC address.
 - ✓ A connection is established to the Web configurator for the DECT Manager.

If connecting to **www.swyx.com/dect700config** does not produce any results:

- 1 Establish the DECT Manager's current IP address.
- 2 Enter **http://** and the current IP address for the DECT Manager in the address field of the Web browser (for example: **http://192.168.2.10**).



The IP address is assigned dynamically via your local network's DHCP server. You can find the DECT Manager's current IP address on the DHCP server in the list of registered DHCP clients. The computer name for the DECT Manager is SwyxDECT 700. The MAC address can be found on the rear of the device. If necessary, contact the network administrator for your local network.

Once a handset is registered on the system, you can also find the IP address via the Info menu on the handset, see *Service-Info abfragen*, page 55.



Your DECT Manager's IP address may change occasionally depending on the DHCP server settings, see *Connecting the DECT Manager to the local network (LAN/router)*, page 19.

Logging into/off the Web configurator

Once you have successfully established the connection, the login screen is displayed in the Web browser.



SwyxDECT 700

SWH

Welcome

You can use this user interface to administer your DECT manager and the connected phones. For your security, the configuration program is protected with a password.

Choose your language: English

Enter your password:

OK

You can select the language in which you want the menus and Web configurator dialogues to be displayed.

- 1 If necessary, click ▼ to open the list of available languages.
- 2 Select the language.
 - ✓ The Web page is reloaded in the selected language. Reloading may take some time.
- 3 Enter the password in the bottom field of the Web page (default setting: **admin**) to access the Web configurator functions.
- 4 Click **OK**.



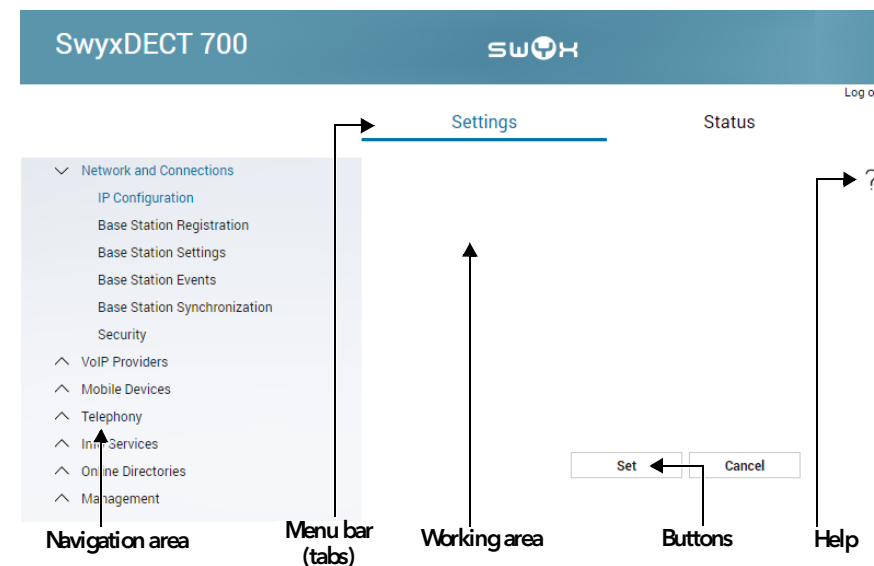
You should change the password for security reasons, see *Security settings*, page 24



If you do not make any entries for a lengthy period (approx. 10 minutes), you are automatically logged off. The next time you try to make an entry or open a Web page, the login screen is displayed again. Enter the password again to log back in. Any entries that you did not save on the DECT Manager before automatic logoff will be lost.

Understanding the structure of the Web configurator pages

The Web configurator pages contain the following UI elements (example):



The Help function includes a link to a website where you can obtain further information.

Menu bar

The Web configurator menus are displayed as tab pages in the menu bar. You will find an overview of the Web configurator menu on *Web configurator menu*, page 19.

The following menus are available:

Settings

The menu allows you to make settings on the DECT Manager.

If you select the settings menu, a list of this menu's functions is displayed in the navigation area.

Status

The menu supplies information about the configuration and status of the DECT Manager and base stations.

Log off

You will find the "Log off" function at the top right of each Web page, above the menu bar.



Always use the „Log off“ function to end the connection to the Web configurator. If, for example, you close the Web browser without logging off beforehand, access to the Web configurator may be blocked for a few minutes.

Navigation area

The functions of the menu (see *Menu bar*, page 17) selected in the menu bar are listed in the navigation area.

If you select a function, the associated page containing information and/or input fields opens in the working area. The selected function is highlighted in orange.

If a function is assigned subfunctions, these are listed below the function as soon as you select the function (in the example **Network and Connections**).

The relevant page for the first subfunction (highlighted in orange) is displayed in the working area.

- Network and Connections
 - IP Configuration
 - Base Station Registration
 - Base Station Settings
 - Base Station Events
 - Base Station Synchronization
 - Security
 - VoIP Providers
 - Mobile Devices
 - Telephony
 - Info Services
 - Online Directories
 - Management

Working area

Depending on the function selected in the navigation area, information or dialogue boxes are displayed in the working area that allow you to make or change your DECT network settings.

Making changes

You can make settings via input fields, lists or options.

- There may be restrictions regarding the possible values for a field e.g., the maximum number of characters, entering special characters or certain value ranges.
- To open a list, click ▾. You can choose between default values.
- There are two kinds of options:
 - Checkboxes: You can activate one or more options from a list. Active options are indicated by ☒, non-active options by ☐. You can activate an option by clicking ☐. The status of the other options in the list does not change. You can deactivate an option by clicking ☒.
 - Alternative options (radio buttons): The active option in the list is indicated by ☒, and the non-active by ☐. You can activate an option by clicking ☐. The previously activated option is deactivated. You can only deactivate an option by activating another option.

Applying changes

As soon as you have made your change on a page, save and activate the new setting on the DECT Manager by selecting **Set**.

If your entry does not comply with the rules for this field, an appropriate error message is displayed. You can then repeat the input.



Changes that have not been saved on the DECT Manager are lost if you move to another Web page or the connection to the Web configurator is lost, e.g., due to exceeding the time limit.

Buttons

Buttons are displayed in the bottom section of the working area. Depending on the current function of a Web page, various buttons are displayed. The functions of these buttons are described in the respective function below.

The most important buttons are:

Cancel

Reject changes made on the Web page and reload the settings that are currently saved in the DECT Manager to the Web page.

Set

Store changes made on a Web page in the DECT Manager.

Opening Web pages

A brief outline of how to navigate to the individual Web configurator functions is given below.

Example:

Defining dialling plans:

Settings | Telephony | Dialing Plans

To open the Web page, proceed as follows after login:

- 1 Select the **Settings** menu in the menu bar.
- 2 Click the **Telephony** function in the navigation area.
 - ✓ The **Telephony** subfunctions are displayed in the navigation tree.
- 3 Select the **Dialing Plans** subfunction.

6.2 Web configurator menu

Settings	— Network and connections	IP Configuration	p. 19
		Base Station Registration	p. 22
		Base Station Settings	p. 23
		Basestation Events	p. 24
		Base Station Synchronisation	p. 24
		Security	p. 24
	VoIP Providers	— List of VoIP Providers	p. 26
	Handsets		p. 27
	Telephony	— Dialling Plans	p. 32
		Advanced VoIP Settings	p. 36
	Info Services		p. 36
	Online Directories		p. 36
	Management	— Date and Time	p. 39
		Local Settings	p. 32
		Miscellaneous	p. 40
		Save and Restore	p. 40

Reboot	p. 41
System Log	p. 42
Firmware Update	p. 42
Status	p. 43

6.3 Connecting the DECT Manager to the local network (LAN/router)

You can find the functions for connecting to the LAN on the Web page:

Settings | Network and Connections | IP configuration

In most cases, special settings are not required to connect the DECT Manager to the local network. Your DECT Manager is preconfigured for dynamic assignment of the IP address by default (IP address). A DHCP server that assigns the IP address dynamically must be activated in the local network in order for the DECT Manager to be "recognised".

If the local network DHCP server cannot or should not be activated, you must assign a fixed/static IP address to the DECT Manager.

Address Assignment for DECT Manager

IP address type	Obtained automatically
IP address	192 . 168 . 100 . 075
Subnet mask	255 . 255 . 252 . 000
Standard gateway	192 . 168 . 100 . 001
Preferred DNS server	192 . 168 . 100 . 216
Alternate DNS server	192 . 168 . 100 . 205
Device name in network	SwyxDECT-700

IP address type

- Select **Obtained automatically** if your device receives the IP address via a DHCP server (default setting).
- Select **Static** if your device receives a fixed IP address.

If the **Obtained automatically** setting is selected, all further settings are automatically configured. They are displayed and cannot be changed.

If you have selected **Static** as the address type, you must create the following settings:

IP address

Enter an **IP address** for your DECT Manager. This IP address allows your DECT Manager to be reached by other subscribers in your local network (e.g., PC).

The IP address comprises four individual groups of numbers with decimal values from 0 to 255 that are separated by a dot, e.g., 192.168.2.1.

Please note:

- The IP address must be included in the address block used by the router/gateway for the local network. The valid address block is defined by the IP address for the router/gateway and the subnet mask (see example).
- The IP address must be unique across the network, which means that it must not be used by another device connected to the router/gateway.
- The fixed IP address must not belong to the address block that is reserved for the DHCP server for the router/gateway.

Check the settings on the router or ask your network administrator.

Example:

Router IP address:	192.168.2.1
Network subnet mask	255.255.255.0
DHCP server address block	192.168.2.101 - 192.168.2.254
Possible IP addresses for the DECT Manager	192.168.2.2 - 192.168.2.100

Subnet mask

The **Subnet mask** specifies how many parts of an IP address the network prefix must comprise.

For example, 255.255.255.0 means that the first three parts of an IP address must be the same for all devices in the network, while the last part is specific to each device. In subnet mask 255.255.0.0, only the first

two parts are reserved for the network prefix. Enter the subnet mask that is used by your network.

Standard gateway

Enter the IP address for the standard gateway through which the local network is connected to the Internet. This is generally the local (private) IP address for your router/gateway (e.g., 192.168.2.1). Your DECT Manager requires this information to be able to access the Internet.

Preferred DNS server

Enter the IP address for the preferred DNS server. **DNS** (Domain Name System) allows you to assign public IP addresses to symbolic names. The DNS server is required to convert the DNS name into the IP address when a connection is being established to a server.

You can specify the IP address for your router/gateway here. This forwards address requests from the DECT Manager to its DNS server.

There is no default setting for a DNS server.

Alternate DNS server

Enter the IP address for the alternate DNS server that should be used in situations where the preferred DNS server cannot be reached.

Devise Name in Network

The product name of the DECT Manager is displayed in this field. You can change this name to identify the device in the network.

Configuring a HTTP proxy

HTTP Proxy

Enable proxy server ☐ Yes ☒ No

Proxy server address

Proxy server port

- 1 Select whether you want to release a separate proxy server in the network for your DECT Manager.
- 2 If **Yes**, enter the IP address for the proxy server in the **Proxy server address** field.

The default setting for the **Proxy server port** is 80. Change this if your server uses another port.

VLAN Tagging

A local network can be divided into logical subnetworks known as VLANs (VLAN = Virtual Local Area Network, Standard IEEE 802.1Q). Multiple VLANs share a physical network and its components, e.g., switches. Data packets from a VLAN are not forwarded to another VLAN. VLANs are often used to separate the data traffic of different services (Internet telephony, Internet TV etc.) and to define different priorities for the data traffic.

You can run your DECT Manager and a PC used to configure the DECT Manager on a separate VLAN. In this case, you enter the VLAN identifiers (VLAN tags) for your VLAN. Your network operator will supply you with this data.



If you operate the PC in a different VLAN from the DECT Manager, you will no longer have direct access to the Web configurator of the DECT Manager from the PC.

VLAN Tagging

You should receive the tagging values of the virtual LAN (VLAN) from your provider. Wrong settings will require hardware reset.

Use VLAN tagging

☐ Yes ☒ No

VLAN identifier

VLAN priority

Set

Cancel

- 1 Select **Yes** if you do not want to use a VLAN (default setting **No**).
- 2 Enter the VLAN identifier for your virtual network in the **VLAN identifier** field.



If you enter an incorrect value for VLAN Tagging and save the settings, you will no longer be able to access the DECT Manager from the PC used for configuration. If you then reset the DECT Manager to a static or dynamic IP address, this will also disable the VLAN tagging. You will then need to reinstate the DECT Manager's access to the local network, see *Connecting the DECT Manager to the local network (LAN/router)*, page 19.

- 3 Select **VLAN Priority** to transfer the PC data.

Prioritising VLANs

Data packets from VLANs can be prioritised. The priority determines whether the data traffic from a VLAN is given preferential treatment by the network components. You can define the priority for voice and data separately. In the case of a local network with a lot of data traffic, you can achieve better quality phone connections by giving a high priority to voice data.

Range of values and assignment of values to service classes (according to IEEE 802.1p):

0	No priority (Best Effort)
1	Background services, e.g., news ticker (Background)
2	Not defined
3	General data services (Excellent Effort)
4	Control services, e.g., routing (Controlled Load)
5	Video
6	Voice data (Voice)
7	Top priority for network control software (Network Control)

Saving settings

- 1 Click on **Set** to save your settings on the **IP Configuration** page.

6.4 Configuring and synchronising base stations

The SwyxDECT 700 automatically recognises the base stations, but they need to be confirmed, activated and synchronised.

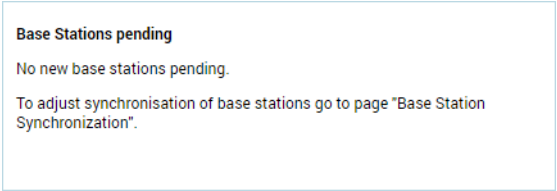
To do this you will need a list of all base stations, each with the MAC address of a DECT module and the location in the building or a unique name for the cell. You will find the MAC addresses for the DECT modules on the sticker attached to each respective SwyxDECT 700 Base base station.

6.4.1 Registering base stations

Settings | Network and Connections | Base Station Registration

The window shows a list of all DECT base stations connected to the network which have not yet been registered. The base stations are identified by their MAC address and by the date and time of their initial contact with the system.

If there are no base stations on the local network that have not yet been registered, a message to this effect will be displayed.



- 1 Select **Confirm** if this base station is to be registered to the system.
✓ The **Own Base Station Data** window opens to configure this base station.

Own Base Station Data

Name / Location

Base station 1

Cluster

1

Synchronization level

1

Status

Active and synced

IP address type

Obtained automatically

DECT Module 1

MAC address

7C:2F:80:C3:EA:25

IP address

192168100076

RFPI = PARI + RPN (hex)

10 2D 94 9C 02

RTP port range

5004 - 5034

Current firmware version

71.103.00.000.00

DECT Module 2

MAC address

7C:2F:80:C3:EA:26

IP address

192168100077

RFPI = PARI + RPN (hex)

10 2D 94 9C 03

RTP port range

5036 - 5066

Current firmware version

71.103.00.000.00

Activate base station

☒ Yes ☐ No

Delete base station

Reboot base station

Set

Cancel

- 2 Enter a unique identifier for the base station in the **Name / Location** field (e.g., Ground Floor West). This name should make it easier to assign the base station within the logical and spatial structure of the DECT network.
- 3 **Cluster** and **Synchronization level** can be specified later on the **Synchronising base stations** page.
✓ The base station status is displayed:
Offline: The base station is not connected to the telephone system

via LAN.
Deactivated
Active
Active and synced

The IP address type is copied from the setting for the DECT Manager on the **IP Configuration** page ([p. 19](#)). You can change the IP address type. The settings for the DECT Manager and the base stations do not have to match. For example, the DECT Manager could receive a fixed IP address so that it will always be able to access the Web configurator with the same address, while the base stations receive their IP addresses dynamically.

If you select the **Obtained automatically** option for the IP address, you will not need to enter any further details.

If you are using static IP addresses on your local network, you will also need to enter an IP address for each base station ([p. 20](#)).

The MAC addresses, the **RFPI** identifier (Radio Fixed Part Identity) and the RTP port range calculated by the system are displayed for both the base station's DECT modules.

4 Select **Activate base station**.

If you do not activate the base station, the data remains stored in the DECT Manager.

- 5 Click **Set** to save the settings.
- ✓ The **Base Station Registration** window now opens again to allow you to register and configure the remaining base stations. When you have registered and configured all the required base stations, the window shows that there are no more unregistered base stations visible in the system.

You must now synchronise the base stations.

6.4.2 **Displaying base stations, changing settings**

Settings | Network and Connections | Base Station Settings

Connected Base Stations

List of connected base stations with Radio Fixed Part Number (RPN), synchronization level and status.

Base station	RPN	Cluster	Sync level	Status	Activate
Base station 1	02	1	1	Active and synced	<input checked="" type="checkbox"/>

Details

Set

Cancel

The **Base Station Settings** page shows a table of all connected base stations with the name, RPN (Radio Part Number, number of the cell on the DECT network), cluster number, synchronisation level and status.

- 1 Click the **Details** button to display the settings for a base station.
 - ✓ This opens the **Own Base Station Data** screen ([p. 22](#)). This shows the base station's current status and IP addresses. You can modify the IP addressing settings if required.
- 2 If you wish to remove the base station from the network, click on **Delete base station**.



If you delete the base station, all data for this base station will be deleted from the DECT Manager.

- 3 Click on **Set** to apply the changes on this page.

6.4.3 Synchronising base stations

Synchronisation and the logical structuring of the base stations in clusters are prerequisites for the functioning of the PABX, the radio connection between base stations and mobile phones and the handover.

To carry out the synchronisation you will need the plan of the clusters with the synchronisation level for each base station.

- 1 View the list of installed base stations and check that all base stations have been registered and configured see *Registering base stations*, page 22. They will then appear in the list in the following window:

Settings | Network and Connections |Base Station Synchronization

Base Station Synchronization

Base station	Cluster	Synchronization level
Base station 1	1	1

Saving the settings will automatically start synchronization.
Connections to the handset will be terminated.

Set

Cancel

- 2 Now assign the cluster number and synchronisation level to each base station as given in the plan.
- 3 Select **Set**.
 - ✓ Synchronisation starts automatically and contact with handsets that have already been registered is interrupted.

6.4.4 Base stations - displaying events

This page displays counters for diagnostic purposes relating to various events that affect the base stations, e.g. active radio connections, handovers, unexpectedly terminated connections to a handset etc.

Settings | Network and Connections | Base Station Events

All displayed values are accumulated since the event list was last deleted.

- 1 Click on **OK** to delete all displayed events.
- For detailed information on the information displayed, see chapter [Diagnostics](#) (p. 44).

6.5 Security settings

The DECT Manager supports the establishment of secure data connections on the Internet with the [TLS](#) security protocol (Transport Layer Security). With TLS, the client (the phone) uses certificates to identify the server. These certificates must be stored on the base.

You can also set the **Remote Management** function on this page.

Settings | Network and Connections | Security

Certificates

When removing or uploading a certificate, connection with mobile devices may be lost.

Server certificates

Remove

Details

CA certificates

Class 3 Public Primary Certification A

Thawte Premium Server CA

Class 3 Public Primary Certification A

Gigaset.net

Equifax Secure Certificate Authority

GTE CyberTrust Global Root

Remove

Details

New certificate

Import local certificate (size < 10 KB)

Browse

Upload

This page contains the **Server certificates** and **CA certificates** lists. These show the certificates stored in the DECT Manager. The certificates have either already been saved by default or you have downloaded them to the DECT Manager via the Upload button.

Invalid certificates

Accept

Reject

Details

The **Invalid certificates** list contains the certificates received from servers that have not passed the certificate check when establishing a connection, and certificates from the **Server certificates/CA certificates** lists that have become invalid (e.g., because they have expired).

You can remove certificates and download new certificates to the DECT Manager and you can also accept or reject invalid certificates.

If the connection to a data server on the Internet is not made because the phone does not accept the certificate received from the server (e.g., when downloading your eMail messages from the POP3 server), you will be prompted to open the **security settings** Web page.

The **Invalid certificates** list contains the certificate used to make the connection. You can display information on the certificate by highlighting it and clicking on the **Details** button. This information includes who issued the certificate (certification authority) and for whom, as well as its validity period.

You must use the information to decide whether to accept or reject the certificate.

If you accept the certificate, depending on its type, it is transferred to one of the **Server certificates/CA certificates** lists (even if it has already expired). If a server responds again with this certificate, this connection is accepted immediately.

If you decline the certificate, it is transferred to the **Server certificates** list with the label **Reject**. If a server responds again with this certificate, this connection is rejected immediately.

Remote Management

If you permit remote management, you can also access the DECT Manager Web configurator from other networks.

Remote Management

Allow access from other networks

Yes

No

Activating this parameter increases the risk of unauthorized access to your device settings.

- 1 Select "Yes" if you wish to **allow access from other networks** or "No" if not.

If you allow **Remote Management**, this increases the risk of unauthorised access to your device settings.

6.6 Configuring VoIP providers

This page allows you to create a list of systems providing VoIP connections and other services for your phones. You can enter the following:

- Your company's VoIP PABX(s)
- Public providers from which you have requested VoIP services

You can configure up to ten different VoIP PABXs or VoIP providers.

Settings | VoIP Provider

List of VoIP Providers		
Name	Domain	
1. IP1	provider01.com	<input type="button" value="Edit"/>
2. IP2	provider02.com	<input type="button" value="Edit"/>
3. IP3	Not configured	<input type="button" value="Edit"/>

- 1 Click on the **Edit** button next to the list entry for the VoIP connection.
 - ✓ A page opens for you to establish a new connection or change the data for an existing connection.
- 2 You enter the details for a PABX manually.

When configuring a VoIP provider, you can use a wizard to select a provider profile.

6.6.1 Wizard for selecting provider profiles

Swyx offers a provider profile that you can use for configuration.



You should apply the provider profile „Swyx“ to ensure full compatibility with SwyxWare.

The SwyxDECT 700 Manager searches for a provisioning file on the network and downloads a provider's configuration data and default settings from this file. You will use this data later to assign VoIP accounts to the handsets ([p. 28](#)).

VoIP Provider 1

Profile Download

Provider

Profile version

- 1 Click on "Select VoIP provider" to load a new VoIP profile.
 - ✓ This launches a wizard to guide you through the process. Select the country first and then the required provider from the list. The data for the selected profile is then loaded and displayed in the window.

If necessary, you can modify the general provider data in the "General Data of your Service Provider" and "Network Data of your Service Provider" sections.

Entering provider data

Enter data manually here for a VoIP PABX or a provider for which there is no existing profile. You can obtain the data from the PABX administrator or your VoIP provider.

- 1 Enter the IP address for the VoIP PABX in the **Proxy server address** field.

General Data of your Service Provider

Domain

Proxy server address

Proxy server port

Registration server

Registration server port

Registration refresh time sec

Network Data of your Service Provider

STUN enabled ☐ Yes ☒ No

STUN server address

STUN server port

STUN refresh time sec

NAT refresh time sec

Outbound proxy mode ☐ Always ☒ Automatic ☐ Never

Outbound server address

Outbound proxy port

Network Protocol

Select protocol ☒ Automatic ☐ UDP only ☐ TCP only

Occasionally you will need to adjust the following settings to correspond to your router settings:

- If you cannot hear the caller on an outgoing call, you may have to switch between outbound proxy server mode and STUN use. The STUN or outbound server replaces the private IP address of your DECT Manager with its public IP address in the sent data packets. If you operate your DECT Manager behind a router with symmetric NAT, STUN cannot be used.
- If you are sometimes unavailable for incoming calls, you may have to adjust the value in **NAT refresh time**:
If you have not activated port forwarding or set up a DMZ on the router for the DECT Manager, an entry in the routing table for the NAT (in the router) is required to make the phone available. The DECT

Manager must confirm this entry in the routing table at certain intervals (**NAT refresh time**) so that the entry stays in the routing table.

For further information on this, please refer to the section *Information on operating VoIP telephones with routers with Network Address Translation (NAT)*, page 49.

6.7 Configuring handsets

You can use the Web configurator to register all handsets on the DECT network and for a VoIP connection. You can edit the settings for handsets that are already registered, deactivate or delete them and make further settings e.g., for using directories and network services.

Settings | Handsets

List of registered Mobile Devices / Subscribers

	Username Display name	SIP connection	Mobile device registered	Email account	Net AM	
3.	123 John	12.34.58.9 ✓	SwyxPhone... 63	—	—	<input type="button" value="Edit"/>

The provider account data should already exist before a mobile device is configured.

New mobile device with own data

New mobile device by copying data from device

Registration PIN ☒ Random ☐ User defined

User defined PIN

Displayed name on idle display ☐ Username ☒ Display name

The DECT Manager starts the check for all mobile devices for which the email check is activated.

Check for new email

Handsets that are already registered are displayed in the list.

- 1 Click on **Edit** to change the settings for this handset.
To start registering and configuring a new handset, click the **Add** button.
Each handset is assigned its own VoIP account. However, you can copy the provider and the "Advanced settings" see also *Extended*

settings for handsets, page 29 from a handset that has already been registered. To do this, select the listed handset from which you want to copy the data and then click on **Add** next to **New mobile device with own data**.

- 2 Specify whether you want to use the **Username** or **Display name** for the VoIP account as the name for the handsets.
The name you choose here will be displayed on the handsets when they are in idle status. Both names are specified when registering the handset see *Registering a handset*, page 28.
- 3 Specify how often the DECT Manager should check for new eMails (for all handsets on which this function is activated).

6.7.1 Registering a handset

Please note:

- Each handset is assigned a VoIP account.
- Registration in the DECT network and for the VoIP connection is started at the same time.
- If you assign a different VoIP account to a handset that is already registered, the connection already configured will be overwritten.

Mobile device 1
No handset registered.

Register mobile device for this SIP connection Start registration

Personal Provider Data
A separate SIP connection must be assigned to each handset.

Authentication name

Authentication password

Username

Display name

Select VoIP provider 1. CloudConnector ▼

Show advanced settings

Set Cancel

- 1 Check that the handset you wish to register is within the wireless range of your DECT network.
- 2 Choose a configured VoIP PABX/provider from the **Select VoIP provider** list.
- 3 Enter the access data for the VoIP account in the relevant fields. These fields may vary depending on the PABX/provider profile.



Use the "Displayed name on idle display" option on the "Handsets" page to specify whether Username or Display name should be used as the handset name on the idle display, see *Specify whether you want to use the Username or Display name for the VoIP account as the name for the handsets.*, page 28.

- 4 Click the Start registration button to start registering the handset.
✓ The PIN is displayed in a window. You must now enter that PIN on the handset to carry out the registration ([p. 11](#)).

6.7.2 Extended settings for handsets

The page offers the following additional setting options for handsets:

- Online directories and network mailboxes
- Settings for audio codecs
- Exporting or importing the local directory
- Configuring the call manager and email reception
- Deregistering and deleting handsets

Open the window via:

Settings | Handsets | Edit

- 1 Click on the **Show advanced settings** button.

Online directories and network mailboxes

Online Directories

You can decide which directory will be opened by directory key and INT key on the handset. An online directory can be selected for automatic name search.

Directory for direct access Local directory

Corporate directory for INT key Deactivate

Automatic look-up Deactivate

LDAP Authentication

To authenticate mobile devices individually, activate this function in online directory settings.

Use personal provider data (SIP) ☐

Username

Password

Network Mailbox Configuration

Call number or SIP name (URI)

Activate network mailbox ☐ Yes ☒ No

Apply changes for all SIP connections OK

The user can call up various directories using the handset control key:

- 1 Choose which directory is called up with the directory key (bottom of the control key). You can select the local directory or one of the online directories from the list.
Depending on this choice, the user can press and hold the directory key to open either the list of online directories or the local directory.
- 2 Choose from the list which corporate directory is opened with the INT key (left on the control key).
- 3 Select an online directory from the list for **Automatic look-up** or deactivate this option. When there is an incoming call, the caller's name is read from this directory and shown in the display (the availability of this function depends on the online directory provider).

Set which online directories are to be made available on the **Online Directories** page, see *Online directories*, page 36.

Network Mailbox Configuration:

- 1 Enter the **Call number or SIP name (URI)** for the network mailbox and activate the network mailbox. (For SwyxWare you should enter „##10“.)
- 2 If these settings are to apply to all configured handsets, click on **OK**.

Setting for Codecs

The voice quality of VoIP calls is determined by the **Codec** used for the transmission. To increase the quality, more data must be transmitted. Depending on the bandwidth of the DSL connection, this can then lead to problems with the volume of data – especially if several VoIP calls are made simultaneously – so that the transmission no longer takes place smoothly.

Settings for Codecs

Selected codecs

- G.722
- G.711 a law
- G.711 μ law
- G.726

Available codecs

< Add

Remove >

Up

Down

Apply codec changes for all mobile devices OK

Both parties involved in a phone connection (caller/sender and recipient) must use the same voice codec. The voice codec is negotiated between the sender and the recipient when establishing a connection. You can select the voice codecs to be used for this VoIP account and specify the order in which the codecs are to be suggested when a VoIP connection is established.

- 1 Select the required codecs and define the sequence in which they should be used.

The following voice codecs are supported:

G.722	Outstanding voice quality. The G.722 wideband voice codec works at the same bit rate as G.711 (64 kbit/s per voice connection) but at a higher sampling rate (16 kHz).
G.711 a law/ G.711 μ law	Excellent voice quality (comparable with ISDN). The required bandwidth is 64 kbit/s per voice connection.
G.726	Good voice quality (inferior to G.711 but better than G.729). Your phone supports G.726 with a transmission rate of 32 kbit/s per voice connection.
G.729A	Average voice quality. The necessary bandwidth is less than or equal to 8 kbit/s per voice connection. You need a licence to use the G.729 codec. You can activate this on the Advanced VoIP Settings page see <i>Additional VoIP settings</i> , page 33.

If these settings are to apply to all configured handsets, click on **OK**.

Export and Import local Directory

Export and import local Directory

Transfer directory from PC to mobile device.

Name of directory file

Browse

Transfer

Save mobile device directory to PC

Save

Delete mobile device directory

Delete

The Web configurator has the following options for editing and coordinating the directories of the registered handsets.

- Save the local directory to a PC. Entries are stored in vCard format in a vcf file on the PC. You can download these files onto every registered handset. You can also copy directory entries to your PC address book.
- Transfer contacts from a PC address book. Export the contacts in vcf files (vCards) and transfer them to the directory on the handset using the Web configurator.
- Delete the local directory from the handset.
If you have edited the directory file (vcf file) on the PC and would like to load this modified directory to the handset, you can delete the current directory on the handset before the transfer.



Back up the current directory on your PC before deleting it. You can then reload it if the modified directory is affected by formatting errors and some, or all, of it cannot be loaded onto the handset.



If you want to copy a directory (vcf file) stored on the PC and containing several entries to the Microsoft Outlook™ address book, please note that Microsoft Outlook™ only ever copies the first (directory) entry from the vcf file to its address book.

Transfer rules

The directory entries from a vcf file that are loaded onto the handset will be added to the directory. If an entry already exists for a name, it will either be supplemented or a new entry for the name will be created. The process will not overwrite or delete any phone numbers.



Depending on your device type, up to three entries with the same name are created in the directory for each vCard - one entry per entered number.

Directory file content (vcf file)

The following data (if available) is written into the vcf file for entry into the directory or transferred from a vcf file into the handset directory:

- Name
- First name
- Number
- Number (office)
- Number (mobile)
- eMail address
- Birthday (YYYY-MM-DD) and time of the reminder call (HH:MM) separated by a "T" (example: 2011-12-24T11:00).

Other information that a vCard may contain is not entered into the handset directory.

Example of an entry in vCard format:

```
BEGIN:VCARD
VERSION:2.1
N:Smith;Anna
TEL;HOME:1234567890
TEL;WORK:0299123456
TEL;CELL:0175987654321
eMail:anna@smith.com
BDAY:2008-12-24T11:00
END:VCARD
```

Call-Manager

Call Manager

Accept calls directly via Call Manager

☐ via headset
☒ via handsfree
☐ No

Select whether calls that are transferred via the PABX call manager are to be accepted directly **via headset**, **via handsfree** or not at all ("No").

Receiving email

Email

Authentication name

Authentication password

POP3 server

POP3 server port

Check for new email
☐ Yes
☒ No

Secure connection (TLS)
☐ Yes
☒ No

Apply email settings for all mobile devices

- 1 If the DECT Manager is to check the receipt of eMails for the handset, enter the data for the eMail account here.
- 2 Activate the option "Yes" for "Check for new email".
- 3 Select whether the notification should be transmitted via a secure connection.
- 4 If these settings are to apply to all configured handsets, click on "OK".

Deregistering and deleting handsets

Mobile device 1

Mobile device registered

Device type
SwyxPhone D750

DECT user identity (IPUI/IPEI)
02 E9 F8 B5 A1

Software version
63

Deregister mobile device for this SIP connection

If the handset for which you are currently editing the settings is registered with the DECT Manager, you can:

Deregister	Deregister the handset for this SIP connection. The connection is interrupted but all data is retained.
Show Advanced Settings Delete	Delete the entire account for the handset on the DECT Manager. This affects all settings on this page, the DECT registration and the VoIP account.

Saving settings

- 1 Click on **Set** to save your settings on the page.



If you have registered or deregistered all handsets, you should back up the DECT Manager settings on the PC. This ensures that the handsets and VoIP accounts will still be assigned consistently if you need to restore the data at a later date.

6.8 Additional settings for making a call

The following settings are available for telephony on all handsets.

- Call barring and access codes (see below, [Dialling plans](#))
- Activating the area code for local calls, see page 32
- Additional VoIP settings, see page 36
 - Audio setting
 - Configuring call transfer
 - R key (hook flash)
 - Setting up local communication ports

Dialling plans

Settings | Telephony | Dialling Plans

Access code

Access Code

The access code is automatically prefixed to numbers before dialling.

Code

Use Never

Depending on your PABX settings, you may need to insert an access code before the phone number for calls outside the area covered by your VoIP PABX (external line prefix, e.g., "0").

- 1 Save an access code and specify when the phone numbers should be automatically prefixed with the digits. You can choose between "Always", "Never"
 - **For net directories** (only when selecting from an online directory),
 - **For call lists** (only when dialling from the call list or an answering machine list),
 - **For net directories and call lists.**
- 2 Enter the maximum number of digits for your internal telephone numbers. This will prevent the access code also being prefixed for internal calls.
- 3 Click on **Set** to save your settings on the page.

6.8.1 Activating the area code for local calls using VoIP

On this page, you provide details about the location of your phone. These are used to determine the international and local area dialling codes as well as country-specific tones (e.g., dialling tone or ring tone).

Settings | Management | Local Settings

Area Codes
 Selection of the country determines the international country code.
 Country Germany

International
 Prefix 00
 Area code 49

Local
 Prefix 0
 Area code
 Use area code for VoIP
☐ For local calls
☐ For local and national calls
☒ No

Tone Selection
 Tone scheme International

Set

Cancel

Area Codes

If you use VoIP to make a call to the fixed line, you may also have to dial the area code for local calls (depending on the provider).

You can set your phone so that the access code is automatically predialled when any VoIP call is made in the same local area, and also for national long-distance calls. This means that the access code is set before all phone numbers that do not start with 0 – even when dialling numbers from the directory and other lists. The exceptions are numbers for which a dialling rule has been defined.

- 1 Select your country. The international and national prefix is then entered in the "Prefix" and "Area code" fields. You can change these settings if required.
- 2 Specify the type of calls (local and national calls) to which the settings are to apply.

Tone selection

Tones (e.g., dialling tone, ring tone, busy tone or call waiting tone) vary from one country or region to another. You can choose from various tone groups for your phone system.

- 1 From the **Tone Selection** list, select the country or region whose ring tones are to be used for your phone.
- 2 Click on **Set** to save your settings on the page.

6.8.2 Additional VoIP settings

On this page you can make settings for sending DTMF signals and for voice quality, set up call transfer and ringback, and configure settings for the ports for establishing VoIP connections.

Settings | Telephony | Advanced VoIP Settings

DTMF in VoIP connections

To send DTMF signals via VoIP, you must first define how key codes should be converted into and sent as DTMF signals: as audible information via the speech channel or as a "SIP Info" message.

Ask your provider which type of DTMF transmission is supported.

DTMF over VoIP Connections
 Automatic negotiation of DTMF transmission ☒ Yes ☐ No

You have the following options:

- If you activate the option "Yes", the phone automatically attempts to set the suitable DTMF signalling type for the current codec for each call.
- If you disable the "No" option, you can use the other options to specify the DTMF signalling type.
 - Enable **Audio** or **RFC 2833** if DTMF signals are to be transmitted acoustically (in voice packets).
 - Enable **SIP info** if DTMF signals are to be transmitted as code.

Enabling the G.722 wideband telephony codec on the DECT network

Both parties involved in a phone connection (caller/sender and recipient) must use the same voice codec. The voice codec is negotiated between the sender and the recipient when establishing a connection.

G.722 Codec
 Enabling or disabling the G.722 codec will restart the system. Connections with mobile devices will be terminated.
 Enable wideband via codec ☐ Yes ☒ No
 G.722
 One base station enables a maximum of 4 wideband calls.

The G.722 codec (wideband connection) enables high voice quality, but only a maximum of four simultaneous connections per base station.

- Enable the G.722 codec to permit wideband transmission for all handsets on the DECT network.

Enabling the G.729 codec

The G.729 codec allows telephony with very low bandwidth requirements and is recommended if minimal network capacity is to be used. You select the codecs for the VoIP connections in the "Advanced settings" for each handset see also **Setting for Codecs**, page 29.

You need a licence to use the G.729 codec. A maximum of ten licences is available; these must be activated. The DECT Manager needs to connect to the Internet for this.

G.729 Codec
 Enable Annex B for codec G.729 ☐ Yes ☒ No

When using G.729 you can also save bandwidth and transmission capacity by suppressing the transmission of voice packets during pauses (default: "No").

- Activate the "Yes" option for "Enable Annex B for codec G.729" to enable the transmission of data packets during pauses. The participants will then hear background noise during pauses, similar to the sound heard during a "traditional" phone call.

Configuring call transfer

Call Transfer
 Use the R-Key to initiate call transfer with SIP Refer method ☒ Yes ☐ No
 Transfer call by on-hook ☒ Yes ☐ No
 You can define the choice of target address in the SIP protocol
 Determine target address automatically ☒ Yes ☐ No
 Hold on transfer target ☒ For attended transfer
☐ For unattended transfer

Participants can transfer a call to another participant as long as the PABX/provider supports this function. The call is transferred using the handset menu (via the display key) or using the R key.

You can expand or change the settings for call transfer as follows:

- **Transfer call by on-hook:** The two participants are connected with one another when you press the end call key. The intermediary's connections with the participants are terminated.
- **Use the R-Key to initiate call transfer with SIP Refer method:** Deactivate call transfer with the R key if you want to assign a different feature to the R key (see below "**Defining R key functions for VoIP (hook flash)**")
- Specify how target addresses are selected in the SIP protocol:
 - **Determine target address automatically**

The participant is automatically determined by the number entered and the SIP information.

- **Derive target address**

You specify how the target address is to be determined:

- From SIP URL
- From SIP contact header



For IP telephony, the call is transferred via the SIP protocol. The unique address is derived from the SIP-URL (SIP-URI). As well as the SIP-URL, the SIP contact header contains additional information for transferring data between the sender and recipient.

- Specify whether the first call is to continue while the second participant is being called, when a call is forwarded. There are two ways of doing this:
 - For attended transfer: This procedure ensures that the call actually takes place.
 - For unattended transfer: The first connection to the participant is ended after the call is transferred.

Defining R key functions for VoIP (hook flash)

Hook Flash (R-key)

Enter the hook flash data you received from your service provider.

Application type

Application signal

Your PABX/VoIP provider may support special performance features. To make use of these features, your phone needs to send a specific signal (datapacket) to the SIP server. You can assign this "signal" as the R function to the R key on the handsets.

- Enter the data received from your provider in the "Application type" and "Application signal" fields.

If the user presses this key during a VoIP call, the signal is sent.



Settings for the R key are only possible if the R key has not been activated for call transfer and SIP Info has been activated.

Defining local communication ports (listen ports) for VoIP

This setting only has to be changed if the port numbers are already being used by other subscribers on the LAN. You can then specify other fixed port numbers for the SIP and RTP port or ranges of numbers for the SIP port.

Listen Ports for VoIP Connections

Use random ports for SIP ☐ Yes ☒ No

SIP port -

RTP port

Maximum value for used RTP ports 6922

The following communication ports are used for VoIP telephony:

• SIP port

The communication port via which the phone receives (SIP) signalling data. The default standard port number is set to 5060 for SIP signalling. You can use values between 5060 and 6000.

If several VoIP phones are operated on the same router with NAT, it makes sense to use randomly selected ports. The phones must then use different ports so that the router's NAT is only able to forward incoming calls and voice data to one (the intended) phone.

Activate "Use random ports for SIP" and specify a number range for **SIP port** from which the ports are to be chosen.

• RTP port

Two consecutive RTP ports (consecutive port numbers) are required for each VoIP connection. Voice data is received via one port and control data via the other. The system uses additional ports for the base station connections (32 ports per DECT module), based on a specified base port. Default setting for the base port: 5004.

The RTP port range calculated for the DECT modules is displayed on the **Own Base Station Data** page ([p. 22](#)).

Saving settings

Click on **Set** to save your settings on the page.

6.9 Info services

You can set up various info services provided via the PABX or a different server. The info services can be opened via the menu on the handsets.

The VoIP account's SIP ID and the handset's DECT ID are transferred when requesting info services. This allows the info service server to offer individual settings for each handset.

Settings | Info Services

Info Services

The handset can display infos received from a server via Info Centre.

Choose info services

- ☐ Customized info service
- ☐ via Gigaset.net
- ☐ via PBX Manager

Settings for the customized RAP Info Service

Server address for online services

Username

Password

Settings for the PBX Manager

Server address for PBX Manager menu

Username

Password

- 1 Select the server for the info services and enter the access data in the relevant fields.
- 2 Click on **Set** to save your settings on the page.



If the PABX provides a RAP server, additional services may be available in the Info Centre and in the Select Services menu on the handsets.

6.10 Online directories

You can make various online directories available so that they can be used and displayed on the handsets:

• Public Online Directories

A number of well-known providers are available here. Each provider can provide a telephone directory and a classified directory. You can also enter an additional provider.

• Corporate directories

You can enter three directories here:

- One directory in LDAP format,
- One general directory in XML format
- One private directory in XML format

Use the handset settings see *Extended settings for handsets*, page 29 to specify which keys are to call up the directories.

6.10.1 Public Online Directories

Settings | Online Directories

Public Online Directories

You can select the online directories of several providers to be displayed on the mobile device.

Provider	Enable directory
KT Phonebook	<input type="checkbox"/>
Telefoongids	<input type="checkbox"/>
Telefonkat.	<input type="checkbox"/>
DGS Navne	<input type="checkbox"/>
[tel.search.ch]	<input type="checkbox"/>

Settings for an additional Provider

You can select the online directories from several providers to be displayed on the handset.

- 1 Tick the required directory providers.
- 2 Click on the **Add** button to set up an additional provider. You can change the entries for a provider by clicking on the **Edit** button.

Settings for an additional Provider

Provider name

Server address

Authentication name

Authentication password

Type	Name
White Pages	<input type="text"/>
Yellow Pages	<input type="text"/>

- 3 Enter the provider's details and a name for the provider and the directories. You can choose between the White and Yellow Pages.
- 4 Click on **Set** to save your settings on the page.
 - ✓ The online directories page is displayed again. The new provider has now been entered in the list.
- 5 Activate this provider.
- 6 Click on **Set** to save your settings on this page.

6.10.2 Corporate directories

If you wish to use a company directory on your telephone, you must activate it on the Web configurator. You may use a directory in LDAP and/or XML format.

Settings | Online Directories

LDAP directory (Lightweight Directory Access Protocol)

The directory is provided via a LDAP server. You need the server address, the server port and the access data for the directory that you wish to use.

Directory via Lightweight Directory Access Protocol (LDAP)

Directory name

Enable directory ☐

Access to the LDAP Data Base

Server address

Server port

LDAP search base (BaseDN)

Mobile device specific authentication ☐ Yes ☒ No

Common username

Common password

- 1 Enter a name in the field "Directory name" (max. 20 characters). This is the name under which the directory will be displayed on the handsets.
- 2 Mark the "Enable directory" option, so that the directory is displayed on the telephones.
- 3 Enter the Server address and the Server port.
- 4 Enter the access data.

Same access data for all handsets:

- Common username (max. 50 characters)
- Common password (max. 50 characters).

Different access data for the handsets:

- Select "Mobile device specific authentication".
- Enter "Username/Password" for each handset.

Settings for LDAP directories

To search in an LDAP company directory, you can set the search criteria and the format of the information for the found entries.

Attributes

A range of attributes are defined in the LDAP database for a directory entry, e.g. surname, first name, telephone number, address, company, etc. The quantity of all attributes which can be saved in one entry is stored in the relevant LDAP server scheme. In order to be able to access

attributes or define search filters, you must know the attributes and their designation in the LDAP server. The majority of attribute designations are standardised, however specific attributes can also be defined.

Examples:

Attributes for a directory entry	Attribute name in the LDAP database
First name	givenName
Surname	sn, cn, displayName
Phone (home)	homePhone, telephoneNumber
Phone (office)	telephoneNumber
Phone (mobile)	mobile
Email	mail
Fax	facsimileTelephoneNumber
Company	company, o, ou
Street	street
City	l, postalAddress
ZIP	postalCode
Country	friendlyCountryName, c
Additional attribute	user-defined

Display format

In this field you can stipulate how the search result is to be displayed on the handset. Here, you can enter combinations of different name and number attributes and special characters. You can select common formats from the list.

For the attribute values to be shown for the required attribute, the attribute name must be preceded by a percent sign (%).

Example

Entry data on the LDAP server:

display-Name	Peter Black	telephoneNumber	0891234567890
givenName	Peter	mobile	012398765432
sn	Black		
...			

Attribute definition in the web UI:

Display format	%sn, %givenName; %telephoneNumber/%mobile
----------------	-------------------------------------------

The entry is shown on the handset as follows:

Black, Peter; 0891234567890/012398765432



The LDAP database is hierarchical in design. With the LDAP-search area (BaseDN) parameter, you can stipulate in which area the search should begin.

Filter

Using the filters, you can define criteria against which specific entries can be searched in the LDAP database. One filter consists of one or more search criteria. A search criterion contains the query for an LDAP attribute, e.g. sn=%. The percent sign (%) is a place holder for the user entry.

Name filter

The name filter decides which attribute is used for the search.

Example: (displayName=%). The percent sign (%) is replaced by the name or part of the name entered by the user.

If a user enters the letter "A", for example, all entries in which the attribute **displayName** begins with "A" are searched for in the LDAP database. If

the user then enters a "b", entries are searched in which the **displayName** begins with "Ab".

Number filter

The number filter stipulates the criteria for the automatic completion of telephone numbers.

Example: `((telephoneNumber=%)(mobile=%))`. The percent sign (%) is then replaced by the part of the telephone number entered by the user.

When dialling, if a user enters the numbers "123", for example, all telephone numbers that begin with "123" are searched for in the LDAP database. The telephone number is completed with the addition of information from the database.

Multiple criteria can be connected using logical AND (&) and/or OR (|) operators. The logical operators "&" and "|" are placed before the search criteria. The search criterion must be placed in brackets and the whole expression must be terminated with a bracket again. AND and OR operations can also be combined.

Examples:

AND operation:	<code>(& (givenName=%) (mail=%%))</code> Searches for entries in which the first name and mail address begin with the characters entered by the user.
OR operation:	<code>((displayName=%) (sn=%%))</code> Searches for entries in which the display name or surname begins with the characters entered by the user.
Combined operation:	<code>((& (displayName=%) (mail=%%))(& (sn=%) (mail=%%)))</code> Searches for entries in which the display name and mail address or the surname and mail address begin with the characters entered by the user.

Directory via XML Protocol

If a corporate directory is provided via an XML server, you will need the access data to set it up.

Directory via XML Protocol

Directory name

Server address

Username

Password

Enable directory

Enable private online directory

Yes No

The private online directory has the same server address as the directory via XML protocol.

- 1 Enter a name in the "Directory name" field. This is the name under which the directory will be displayed on the handsets.
- 2 Enter the XML server details.

Server address	IP address for the directory.
Username	Access ID for the directory.
Password	Password for the access ID to the directory.

Enable private online directory

If a private directory is available on the server in XML format, activate it and enter a name for the directory. The private directory must be provided via the same server as the XML directory.

Saving settings

Click on **Set** to save your settings on the page.

6.11 Device management

Date and time

By default, the DECT Manager is configured so that the date and time are transferred from a time server on the Internet.

Changes to the settings for the time server and activating/deactivating the synchronisation are done via the Web page:

Settings | Management | Date and Time

Time

Automatic adjustment of system time with time server ☒ Yes ☐ No

Last synchronization with time server 08.12.2016 01:35

Time server

Time zone

Automatically adjust clock for daylight saving changes ☒ Yes ☐ No

You can make the following changes:

- Enter another time server
- Deactivate the time server and enter the date and time manually
- Select the time zone for your location
- Activate/deactivate automatic adjustment of the clock to summer time

6.11.1 Additional device settings

This page

Settings | Management | Miscellaneous

allows you to configure additional device settings.

Changing the password for the Web configurator

You should change the password for registering with the WEB configurator for security reasons (up to 20 digits; the default setting is **admin**).



If you have forgotten the password, you will have to reset the device to the factory settings. Further information on this can be found in [Resetting the device settings \(S. 13\)](#).

Deactivating LEDs on the base stations

The LEDs on the base stations can be deactivated. Please note that faults in synchronisation and in the DECT network cannot then be localised immediately.

Starting auto-configuration

The Auto configuration is used to update system settings. It can be started if the manufacturer, operator or supplier of the PABX provides a corresponding file and a code.

Provider and PABX profiles

A profile contains important settings for services and functions on your telephone system. A profile may be made available by a provider or the operator of the PABX. You can specify on this page whether the device should check for an updated profile regularly and load it onto your system.

6.11.2 Saving and restoring settings

You can save and restore the system settings via the Web page:

Settings | Management | Save and Restore

Save Device Settings to PC

Save settings

Restore Device Settings from PC

Settings file

Once you have configured the DECT Manager and after making any changes to the configuration, particularly registering or deregistering handsets, you should save the latest settings in a file on the PC so that the current system can be restored quickly if problems occur. The file is stored with the suffix .cfg.

If you change the settings accidentally or you need to reset the DECT manager due to a fault, you can reload the saved settings from the file on your PC to your phone system. These settings can be restored via the reset button on the device ([p. 13](#)) or by restoring the firmware's default settings, see **Firmware downgrade**, page 43.

The file .cfg contains all system data including the DECT registration data of the handsets, but not the call lists of the handsets.



The secure configuration file can also be loaded onto a new device.
Prerequisites:
-The old device must no longer be in operation.
-The firmware version of the new device must correspond, at least, with the version of the device from which the data is saved, including the set patches

6.11.3 Rebooting the system

Your SwyxDECT 700 can be set to automatically reboot regularly at a convenient time if required as a result of a system check. This does not normally cause the system to become unstable, but if an unforeseeable system error should occur, you can reboot the system manually.

Settings | Management | Reboot



Only perform this function if the following message is displayed:
"Reboot and system synchronization are recommended."
No calls can be made while the phone system is rebooting. Rebooting can take up to a few minutes.

Reboot
 Reboot and system synchronization are not necessary at this time.
 A reboot can take several minutes. During this time calls are not possible.
 Reboot of ☒ DECT Manager only ☐ DECT Manager and base stations

Reboot now

Automated Reboot and System Check
 Reboot and synchronization ☐ Daily ☒ Optional
 The system check determines if a reset is necessary. The check takes place on the selected days at the given time, but at least once a week. If calls are being made, the required reboot is delayed for up to 120 min.
 System check every ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☒ Sunday
 Start time for system check and reboot h min

Set Cancel

Immediate reboot

- Click on "OK" next to "Reboot System".
✓ The reboot begins immediately. All existing connections are terminated.

Regular system check

The system regularly checks whether a reboot is necessary. If it determines that a reboot is required, this operation is performed. If a phone call is in progress, the reboot will be postponed by up to two hours.

The check will be performed at the specified time on the selected days, at least once per week.

- 1 Select a day (or "Daily") and enter a time for the check. The default setting, controlled by a random generator, is between 12.30 a.m. and 3.30 a.m. on a sunday.
- 2 Click on **Set** to save your settings on the page.

6.11.4 System Log (SysLog)

The system report (SysLog) gathers information about selected processes performed by the DECT Manager and base stations during operation and sends this to the configured SysLog server.

Settings | Management | System Log

For detailed information on the information displayed, see chapter [Diagnostics](#) (p. 44)

6.11.5 Updating firmware for the base/downgrading firmware updates

Regular updates to the firmware for the DECT Manager and base stations are provided by the operator or supplier on a configuration server. You can download these updates onto the DECT Manager or base stations as required.

Settings | Management | Firmware Update

Settings for Firmware Update and Downgrade

Current firmware version of DECT Manager 70.103.00.000.00

Firmware status of base stations is shown on status page.

Data server

Configuration file (URL)

Update strategy for base stations ☐ Simultaneous ☒ Sequential

Updating the DECT Manager firmware automatically initiates a base station update.

- 1 Enter the address of the server on which the update is provided in the "Data server" field. You can obtain information on this from the supplier or operator of your system.

- 2 Specify whether the firmware update for the base stations is to be simultaneous or sequential. A sequential update uses fewer network resources.

Start Firmware Update or Downgrade

Available firmware version of DECT Manager Not available

Update time ☒ Immediately ☐ Later

Time h min

Date y m d

On starting the firmware update the device checks if the requirements of a successful firmware download are fulfilled. The firmware is then downloaded without additional feedback. During download and update the handset / base connection is lost. A successful update results in the handset re-establishing the base connection.

You can downgrade the firmware to the previous version.

Previous DECT Manager version **.000.**.*.*.*

You can downgrade the firmware to the delivery version. All your personal settings will be deleted.

You can load new firmware (update) or restore the firmware to an earlier version (downgrade).

- 3 Specify when an update or downgrade should be performed

Immediately	The update/downgrade is performed when you click the "Update firmware" or "Start downgrade" button.
Later	The update/downgrade is performed at the time you indicate in the lines underneath.

When the download is started, the device first checks whether the pre-requisites are in place for successfully downloading the firmware. The handsets lose their connection to the base during the download and updating process. You can tell that the update has been successful when the handsets re-establish the connection to the base.



The DECT Manager firmware update can take up to ten minutes. Updating the individual base stations takes approx. 2–3 minutes. Do not disconnect the devices from the local network (or the power supply) during this time.

Firmware downgrade

You have the following options:

- You can reload the firmware version that was loaded before the last update on the DECT Manager.
- You can reload the firmware version that was loaded by default onto the DECT Manager.

The selected firmware is reloaded and the current firmware is overwritten.



If you reload the default firmware version, you will lose all the settings you have made in the WEB configurator. You should therefore make a point of saving the configuration data first

6.12 DECT Manager and base station status

The **Status** tab displays the following information about the telephone system:

Status | Device

6.12.1 Status

Network identities and Software

- IP and MAC address of the DECT Manager
- Device name in network
- Operating days since the system was started
- Version of the firmware currently loaded for the DECT Manager
- Version of the firmware available for the DECT Manager

- Current date and time, and the time of the last synchronisation with the time server, if time server synchronisation is enabled see **Date and time**, page 39.

Base stations

- List of base stations with names, firmware version currently loaded, time in days and download status, for DECT modules 1 and 2 respectively
- Registered base stations and clusters

Graphics of the relationships between base stations can be displayed here:

Click on the name of a base station or a cluster.

For detailed information on the information displayed, see section [DECT network graphics](#) see *DECT Manager and base station status*, page 43.

7 Diagnostics

The web configurator for the DECT manager see *Configuring the system on the DECT Manager*, page 16 offers different tools for monitoring the operation and diagnosis in the event of problems occurring.

7.1 Systemreport (SysLog)

Settings | Management | System Log

The system report (SysLog) gathers information about selected processes performed by the DECT manager and base stations during operation and sends this to the configured SysLog server. Activate the function if you wish to create an error ticket for Swyx.

System Log

The system log is stored on an external syslog file server.

IP address

Server port

514

Default

Activate syslog

☐

- 1 Enter the **IP address** and **Server port** for storing the system log on a server (default setting for the server port: 514).
- 2 Mark the field by **Activate syslog**.

Setting the filter for the system report

Filter for System Log

New filter settings are valid for future events.

- ☐ System events
- ☐ Errors in DECT operating system
- ☐ Socket layer events
- ☐ SIP events
- ☐ DECT events
- ☐ Email events
- ☐ RAP events
- ☐ Update protection events

Events from Base Stations

- ☐ System events
- ☐ Errors in DECT operating system
- ☐ Socket layer events
- ☐ Media stream events

Set

Cancel

- 1 Select the events you want to log. If you do not know precisely where the cause of the error could be, mark all events.
- 2 Click on **Set** to activate your settings on the screen.
✓ The changes take effect with the next system event.

Try to reproduce the error that occurred. The report will be stored on your SysLog server. Provide this with the error ticket.

7.2 Displaying of base station events

Settings | Network and Connections| Base Station Events

This page displays counters for diagnostic purposes relating to various events that affect the base stations, e.g. active radio connections, handovers, unexpectedly terminated connections, etc. for both DECT module 1 and module 2.

Base Station Events

Cl	Lv	RPN	Sync	Conn	HoIn	HoOut	Loss	Async	Busy	DpcOff	
1	1	02	(FF)	64	0	0	0	0	0	0	Base station 1
		03	(02)	6	0	0	0	0	0	0	

Events since

5-Dec-2016 - 10:01

Delete all event counters

OK

Cl	Cluster number, identifies a group of synchronised DECT modules
Lv	Synchronisation level, synchronisation is permitted with every lower level
RPN	(Radio Fixed Part Number) Hexadecimal identifier of a DECT module
Sync	RPN of the base station, with which the base is synchronised
	(FF) Module not synchronised
	(--) Module not activated
Conn	Number of connections, i.e. calls made
HoIn/ HoOut	Number of incoming/outgoing handovers
Loss	Number of lost connections, i.e. interrupted calls
Async	How often the synchronisation was interrupted

Busy	How often the maximum number of possible connections of the module was achieved
DpcOff	How often the LAN connection to the base station was interrupted

All displayed values are accumulated since the event list was last deleted. Click on **OK** to delete all stored events.



On the Status page, you can check the base stations and clusters as well as the connections and signal strengths using graphics, see *DECT network graphics*, page 45.

7.3 System dump

In case of error, you can create a system dump and transmit to a support server for diagnostic purposes.

- 1 Log in to the Web configurator, see *Logging into/off the Web configurator*, page 16
- 2 Change the URL at: http:<IP-address>/sysdump.html
- 3 The MAC address for the system and the name of the server are displayed.
- 4 Click on **Send**. The information is transmitted to the server.

7.4 DECT network graphics

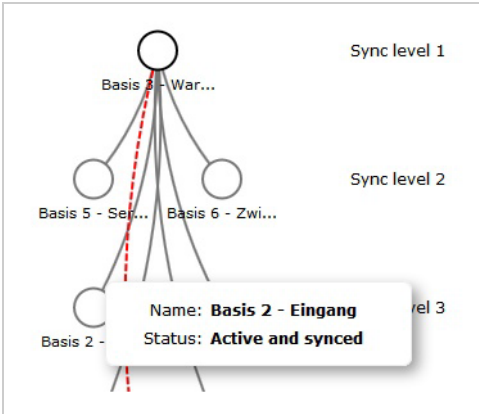
Status|Device

The **Status** tab shows information etc. concerning the connected base stations with names, firmware version currently loaded, time in days and download status, for DECT modules 1 and 2 respectively.

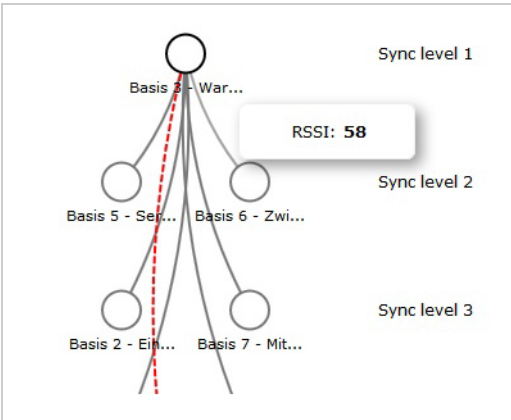
Base station	Module	Current version	Operating days	Download status
Base station 1 - Drucker	1	71.103.00.000.00	14	OK
Base station 2 - Eingang	2	71.103.00.000.00	14	OK

Display graphics of the relationships between the base stations:

- 1 Click on the name of a base station or a cluster.
 - ✓ A graphic shows the base station and its relationship to the surrounding base stations. You will see the synchronisation hierarchy on the right-hand side.
- Information concerning a base station:
- 2 Move the mouse pointer over a base station. The full name and status (e.g. **Active and synced**) is displayed.




- Information concerning a connection:
- 3 Move the mouse pointer over a connection.
 - ✓ The RSSI value for the connection is displayed.
- The RSSI value is an indicator for the connection quality and is given in percent; 100 would be the maximum, 0 the minimum acceptable connection quality



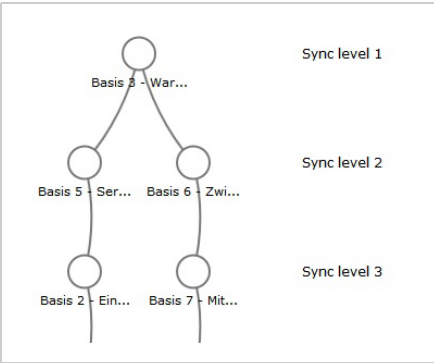
The lines between the base stations show the current connection quality:

Connection	RSSI range (0-100)	Signal strength
Grey line	43 to 100	Very good to good
Red line (dotted)	0 to 43	Weak
No line		No signal

Displaying synchronisation level

- 1 Click on the  icon.

The synchronisation levels are displayed using graphics.



Information concerning a base station:

- 2 Move the mouse pointer over the desired base station. The full name, status and the current RSSI value are displayed.

Information concerning the fluctuation in the RSSI value at specific base stations can be found in the **Base Station Events (S. 45)** tables.



The displayed values are for orientation only. Instructions on how to carry out exact measurements of the connection values can be found in "Swyx DECT 700 - Site Planning and Measurement Guide".

8 Help and Support

Questions? The trade outlet where you bought your PABX will be happy to help with further questions relating to your System.

8.1 Questions and answers

The table below contains a list of common problems and possible solutions.

The display is blank.

Handset is switched off or battery is flat.

- Place the handset in the charger.

You cannot make calls or use other services provided by the phone system (checking eMail, accessing the call list, online directories, info service).

- 1 Handset is not registered on the phone system.
 - Register the handset ([p. 10](#)).
- 2 Handset is outside the range of the wireless network.
 - Reduce the distance from the handset to a base station belonging to the wireless network.
- 3 The firmware is currently being updated.
 - Please wait until the update is complete.
- 4 Base station is without power.
 - Check the power supply to the base stations and the DECT Manager ([p. 7](#)).
 - If the base is powered by PoE, check the switch's power supply.

- 5 No resources available from the nearest base station (all connections are busy).
 - Short-term solution: Move to a different location to check whether connections are available at another base station.
 - Long-term solution: Check the plan of the base stations and set up an additional base station at the location with poor wireless coverage.
- 6 Base stations not synchronised or incorrect synchronisation settings used.
 - Synchronise the base stations.
 - Check that there is a base station assigned synchronisation level 1 in the cluster.
 - Check that each base station can access its superordinate base station wirelessly ([p. 24](#)). If this is not the case, set up additional clusters as required.

Some of the network services do not work as specified.

Features are not activated.

- Query with the PABX administrator or network provider.

The other party cannot hear you.

The handset may be muted.

- Unmute the microphone on the handset.

The number of the caller is not displayed despite CLIP/CLI being activated.

Calling Line Identification is not enabled.

- The **caller** should ask the network provider to enable Calling Line Identification.

The connection to a participant on hold is automatically terminated after a short time.

The session timer on the VoIP PABX is set for an insufficient time.

- Check the timer setting and increase it if necessary.

You hear an error tone (descending tone sequence) when keying an input.

Action has failed/invalid input.

- Repeat the process.

Read the display and refer to the user guide if necessary.

No time is specified for a message in the call list.

Date/time is not synchronised.

- Set the date/time on the DECT Manager or
- Activate synchronisation with a time server on the Internet via the Web configurator.

You cannot establish a connection to the DECT Manager with your PC's Web browser.

- When establishing a connection, check the DECT Manager's local IP address that has been entered. You can check this via the Service menu on a handset (p. 51).
If no handset is registered, establish the DECT Manager's IP address when using a dynamic IP address via the DHCP server. You can find the DECT Manager's MAC address on the rear of the housing. If necessary, contact the network administrator for your local network.
- Check the connections between the PC and the DECT Manager.
Transmit a ping command to your base, e.g., from your PC (ping <DECT Manager's local IP address>).
- You have tried to reach the phone via a secure http (https://...). Try again with http://...



Some displays may contain pixels (picture elements) which remain activated or deactivated. As a pixel is made up of three sub-pixels (red, green, blue); it is possible that pixel colours may vary. This is completely normal and does not indicate a fault.

8.2 Information on operating VoIP telephones with routers with Network Address Translation (NAT)

Generally speaking, no special telephone or router configuration is required when operating a VoIP phone with NAT router. The configuration settings described in this section are only necessary if you encounter one of the following problems.

8.2.1 Typical problems caused by NAT

- No incoming calls are possible via VoIP. Calls to your VoIP phone number are not put through.
- Outgoing calls via VoIP are not connected.
- A connection is established with the other party, but you cannot hear them and/or they cannot hear you.

8.2.2 Possible solution

1. Change the port numbers of the communication ports (SIP and RTP ports) on your phone ("[1. Changing the port numbers for SIP and RTP on your VoIP phone](#)").
2. In some cases, you must also define port forwarding for the phone's communication ports on the router ("[2. Setting port forwarding on the router](#)").

1. Changing the port numbers for SIP and RTP on your VoIP phone

On your VoIP phone system, define different (local) port numbers for the SIP and RTP ports (between 1024 and 49152).

- These numbers must not be used by any other application or host in the LAN and
- Must be considerably higher or lower than the SIP and RTP port numbers that you usually use (and are preset on the phone).

This procedure is particularly useful if additional VoIP phones are connected to the router.

To change the SIP and RTP port numbers on your VoIP phone system, proceed as follows:

- 1 Connect your PC's browser to the Web configurator of the DECT Manager and log in.
- 2 Open the Web page **Settings | Telephony| Advanced VoIP Settings** and change the settings for the SIP and RTP ports ([p. 35](#)). To help you remember the new port numbers (e.g., for router configuration), you can choose port numbers that are very similar to the standard settings, e.g.:

SIP port	49060	instead of	5060
RTP port	49004	instead of	5004

- 3 Save the changes on your phone.
- 4 Wait for the active VoIP connections to be re-registered. To do so, switch to the Web page **Settings | VoIP Providers** to see the Status of your VoIP connections.
- 5 Check to see whether the problem persists. If it does, perform step 2.

2. Setting port forwarding on the router

To ensure that your specified SIP and RTP port numbers are used on the WAN interface with the public IP address, you must define port forwarding rules for the SIP and RTP ports on the router.

To define port forwarding on the router, proceed as follows:

The terms used below may vary from router to router.
To release a port, you must enter the following details (example):

Protocol	Public port	Local port	Local host (IP)	
UDP	49060	49060	192.168.2.10	for SIP
UDP	49004	49004	192.168.2.10	for RTP

Protocol

Enter **UDP** as the protocol to be used.

Public port

Port number/port number range on the WAN interface.

Local port

The SIP and RTP port numbers set on the phone.
You can set an RTP base port for the SwyxDECT 700 base stations, from which the system automatically determines the ports required (32 per DECT module) ([p. 35](#)). You must then also define corresponding port forwarding for this range.

Local host (IP)

Local IP address of your phone in the LAN. The phone's current IP address is displayed on the router.
To enable the router to perform this port forwarding, the DHCP settings of the router must ensure that the phone is always assigned the same local IP address, i.e., the DHCP does not change the IP address assigned to the phone during operation. Alternatively, you can assign a fixed (static) ID address to the phone. However, you must ensure that this IP address is not within the address range reserved for DHCP and is not assigned to any other LAN subscriber.

8.3 Checking service information

If you contact Customer Care, you may need the base's service information.

Prerequisite: You have assigned a line (try to establish a call, make a call).



You may need to wait a few seconds before „Options“ appears on the display

„Options | Service Info“

Confirm selection with „OK“.

You can select the following information/functions with q:

1. Serial number of the DECT Manager (PARI)
2. Serial number of the handset (IPUI)
3. No information stored; only '---' displayed
4. DECT Manager variant (digits 1 and 2)
5. Version of the DECT Manager firmware (digits 3 to 5)
6. Revision of the DECT Manager firmware (digits 6 and 7)
7. No information stored; only '---' displayed
8. DECT Manager's device item number
9. DECT Manager's IP address

RFP-Scan

This function can be used during or after installation and enables you to identify the DECT base stations (SwyxDECT 700 Base) from which a handset receives radio waves at a particular location.

8.4 Environment

8.4.1 Environmental management system



ISO 14001 (Environment): Certified since September 2007 by TÜV SÜD Management Service GmbH.

ISO 9001 (Quality): Certified since 17/02/1994 by TÜV SÜD Management Service GmbH.

8.4.2 Disposal

Batteries should not be disposed of in general household waste. Observe the local waste disposal regulations, details of which can be obtained from your local authority.

All electrical and electronic products should be disposed of separately from the municipal waste stream via designated collection facilities appointed by the government or the local authorities.



This crossed-out wheeled bin symbol on the product means the product is covered by the European Directive 2002/96/EC.

The correct disposal and separate collection of your old appliance will help prevent potential negative consequences for the environment and human health. It is a precondition for reuse and recycling of used electrical and electronic equipment.

For more detailed information about disposal of your old appliance, please contact your local council refuse centre or the original supplier of the product.

8.5 Appendix

8.5.1 Care

Wipe the unit with a **damp** cloth (do not use solvent) or an antistatic cloth. **Never** use a dry cloth. This can cause static.

Impairments in high-gloss finishes can be carefully removed using display polishes for mobile phones.

8.5.2 Contact with liquid ⚠

If the device has come into contact with liquid:

- 1 **Disconnect the power adapter.**
- 2 Allow the liquid to drain from the device.
- 3 Pat all parts dry. Then leave the device in a warm, dry location for **at least 72 hours** (**not** in a microwave, oven or similar).
- 4 **Do not switch on the device again until it is completely dry.**

When it has fully dried out, you will usually be able to use it again.

In rare cases, contact with chemical substances can cause changes to the telephone's exterior. Due to the wide variety of chemical products available on the market, it was not possible to test all substances.

8.5.3 Authorisation SwyxDECT 700 Base

Voice over IP telephony is possible via the LAN interface (IEEE 802.3). Depending on your telecommunication network interface, an additional modem could be necessary. For further information please contact your Internet provider.

This device is intended for use within the European Economic Area and Switzerland. If used in other countries, it must first be approved nationally in the country in question. Country-specific requirements have been taken into consideration.

[Declarations of Conformity](#)

8.5.4 Specifications

Power consumption

SwyxDECT 700 Manager (DECT Manager)		2.3 W
SwyxDECT 700 Base (Base station)	Standby:	3.0 W
	Call:	3.1 W for one DECT connection
		3.3 W for 8 DECT connections (narrow-band)

General specifications

DECT Manager and base stations

Power over Ethernet	SwyxDECT 700 Manager: PoE IEEE 802.3af < 3.8 W (Class 1) SwyxDECT 700 Base: PoE IEEE 802.3af < 6.4 W (Class 2)
LAN interface	RJ45 Ethernet, 10/100 Mbps Protection class IP20
Ambient conditions for operation	+5°C to +45°C; 20% to 75% relative humidity
Protocols	IPv4, SNTP, DHCP, DNS, TCP, UDP, VLAN, HTTP, TLS, SIP, STUN, RTP, MWI, SDP

Base stations

DECT standard	DECT EN 300 175-x
Radio frequency range	1880 - 1900 MHz
No. of channels	120 channels

Number of connections	8 simultaneous connections per base station (G.726, G711, G.729ab codec), 4 connections in wideband operation (G.722)
Range	Up to 300 m outdoors, up to 50 m indoors
Codec	G.711, G.722, G.726, G.729ab (10 licences)
Quality of Service	TOS, DiffServ

9 Glossary

A

ADSL

Asymmetric Digital Subscriber Line
Special form of [DSL](#).

ALG

Application Layer Gateway
NAT control mechanism for a router.

Many routers with integrated NAT use ALG. ALG lets the data packets in a VoIP connection pass and adds the public IP address of the secure private network.

The router's ALG should be deactivated if the VoIP provider offers a STUN server or an outbound proxy.

See also: [Firewall](#), [NAT](#), [Outbound proxy](#), [STUN](#).

Authentication

Restriction of access to a network/service by using an ID and password to log in.

Automatic ringback

See [Ringback when the number is busy](#).

B

Block dialling

Enter the complete phone number, and correct it if necessary. Then pick up the earpiece or press the talk/speaker key to dial the phone number.

Broadband Internet access

See [DSL](#).

C

Call Forwarding

CF

Automatic forwarding of a call to a different telephone number. There are three kinds of call forwarding:

- CFU, Call Forwarding Unconditional
- CFB, Call Forwarding Busy
- CFNR, Call Forwarding No Reply

Call swapping

Call swapping allows you to switch between two callers or between a conference and an individual caller without allowing the waiting caller to listen to the call.

Call waiting

= CW.

Network provider feature. A beep during a call indicates that another caller is waiting. You can accept or reject the second call. You can activate/deactivate the feature.

CF

Call Forwarding

See [Call Forwarding](#).

Client

Application that requests a service from a server.

Cluster

Subdivision of a DECT network into groups (subnets) by a central management station (DECT Manager). All telephones in the network use the central functions of the PABX (VoIP configuration, directories, etc.). However, the base stations only synchronise within a cluster, meaning that a handover of a handset from one cluster to a neighbouring cluster is not possible.

If cells cannot synchronise wirelessly, they must be assigned to different clusters so that synchronisation can take place within these clusters. This is required for problem-free use of the DECT system.

Codec

Coder/decoder

Codec is a procedure that digitises and compresses analogue voice before it is sent via the Internet, and decodes – i.e., translates into analogue voice – digital data when voice packets are received. There are different codecs with differing degrees of compression, for instance.

Both parties involved in the telephone connection (caller/sender and recipient) must use the same codec. This is negotiated between the sender and the recipient when establishing a connection.

The choice of codec is a compromise between voice quality, transmission speed and the necessary bandwidth. A high level of compression, for example, means that the bandwidth required for each voice connection is low. However, it also means that the time needed to compress/decompress the data is greater, which increases execution time for data in the network and thus impairs voice quality. The time required increases the delay between the sender speaking and the recipient hearing what has been said.

COLP/COLR

Connected Line Identification Presentation/Restriction

Feature provided by a VoIP/ISDN connection for outgoing calls.

COLP displays the phone number accepting the call on the calling party's display unit.

The number of the party accepting the call is different to the dialled number, e.g., if the call is diverted or transferred.

The called party can use COLR (Connected Line Identification Restriction) to prevent the number from appearing on the calling party's display.

Consultation call

You are on a call. With a consultation call, you interrupt the conversation briefly to establish a second connection to another participant. If you end the connection to this participant immediately, then this was a consulta-

tion call. If you switch between the first and second participant, it is called [Call swapping](#).

CW

Call Waiting

See [Call waiting](#).

D

DECT

Digital Enhanced Cordless Telecommunications

Global standard for wireless connection of mobile end devices (hand-sets) to telephone base stations.

DHCP

Dynamic Host Configuration Protocol

Internet protocol that handles the automatic assignment of [IP addresses](#) to [Network subscriber](#). The protocol is made available in the network by a server. A DHCP server can, for example, be a router.

The phone contains a DHCP client. A router that contains a DHCP server can assign the IP addresses for the phone automatically from a defined address block. The dynamic assignment means that several [Network subscribers](#) can share one IP address, although they can only use it alternately and not simultaneously.

With some routers you can specify that the IP address for the phone is never changed.

Display name

PABX feature. You can specify any name that is to be shown to the other party during a call instead of your phone number.

DMZ (Demilitarised Zone)

DMZ describes a part of a network that is outside the firewall.

A DMZ is set up, as it were, between a network you want to protect (e.g., a LAN) and a non-secure network (e.g., the Internet). A DMZ permits unrestricted access from the Internet to only one or a few network com-

ponents, while the other network components remain secure behind the firewall.

DNS

Domain Name System

Hierarchical system that permits the assignment of **IP addresses** to **Domain names** that are easier to memorise. This assignment has to be managed by a local DNS server in each (W)LAN. The local DNS server determines the IP address, if necessary by enquiring about superordinate DNS servers and other local DNS servers on the Internet.

You can specify the IP address of the primary/secondary DNS server.

See also: **DynDNS**.

Domain name

Name of one (of several) Web server(s) on the Internet (e.g., swyx.com). The domain name is assigned to the relevant IP address by DNS.

DSCP

Differentiated Service Code Point

See **Quality of Service (QoS)**.

DSL

Digital Subscriber Line

Data transfer technology that allows Internet access with e.g., **1.5 Mbps** over a conventional telephone line. Prerequisites: DSL modem and the appropriate service offered by the Internet provider.

DSLAM

Digital Subscriber Line Access Multiplexer

The DSLAM is a switch cabinet in an exchange where all subscriber connectors converge.

DTMF

Dual Tone Multi-Frequency

Dual tone multi-frequency dialling (DTMF).

Dynamic IP address

A dynamic IP address is assigned to a network component automatically via **DHCP**. The dynamic IP address for a network component can change every time it registers or at certain time intervals.

See also: **Static IP address**.

DynDNS

Dynamic DNS

Domain names and IP addresses are assigned via **DNS**. For **Dynamic IP addresses** this service is enhanced with "Dynamic DNS". This permits the use of a network component with a dynamic IP address as a **Server** on the **Internet**. DynDNS ensures that a service can always be addressed on the Internet under the same **Domain name**, regardless of the current IP address.

E**ECT**

Explicit Call Transfer

Participant A calls participant B. The participant puts the connection on hold and calls participant C. Rather than connect everyone in a three-party conference, A now transfers participant B to C and hangs up.

EEPROM

Electrically Erasable Programmable Read Only Memory

Memory building block in your phone with fixed data (e.g., default and customised settings) and data saved automatically (e.g., call list entries).

Ethernet network

Wired **LAN**.

F**Firewall**

You can use a firewall to protect your network against unauthorised external access. This involves combining various measures and technologies (hardware and/or software) to control the flow of data between a pri-

vate network you wish to protect and an unprotected network (e.g., the Internet).

See also: [NAT](#).

Firmware

Device software in which basic information is saved for the functioning of a device. To correct errors or update the device software, a new version of the firmware can be loaded into the device's memory (firmware update).

Flat rate

Billing system for an [Internet](#) connection. The Internet provider charges a set monthly fee. There are no additional charges for the duration of the connection or number of connections.

Fragmentation

Data packets that are too big are split into smaller packets (fragments) before they are transferred. They are put together again when they reach the recipient (defragmented).

Full duplex

Data transmission mode in which data can be sent and received at the same time.

G

G.711 a law, G.711 μ law

Standard for a [Codec](#).

G.711 delivers very good voice quality that corresponds to that in the ISDN network. As there is little compression, the necessary bandwidth is around 64 kbit/s per voice connection, but the delay caused by coding/decoding is only approx. 0.125 ms.

"a law" describes the European standard and " μ law" describes the North American/Japanese equivalent.

G.722

Standard for a [Codec](#).

G.722 is a **wideband** language codec with a bandwidth of 50 Hz to 7 kHz, a net transmission rate of 64 kbit/s per voice connection and integrated speech pause recognition and comfort noise generation (silence suppression).

G.722 delivers very good voice quality. A higher sampling rate provides clearer and better voice quality than other codecs and enables a speech tone in High Definition Sound Performance (HDSP).

G.726

Standard for a [Codec](#).

G.726 delivers good voice quality. It is inferior to the quality with codec **G.711** but better than with **G.729**.

G.729A/B

Standard for a [Codec](#).

The voice quality is more likely to be lower with G.729A/B. As a result of the high level of compression, the necessary bandwidth is only around 8 kbit/s per voice connection, but the delay is around 15 ms.

Gateway

Connects two different [Networks](#), e.g., a router as an Internet gateway.

For phone calls from [VoIP](#) to the telephone network, a gateway has to be connected to the IP network and the telephone network (gateway/VoIP provider). It forwards calls from VoIP to the telephone network as required.

Gateway provider

See [SIP provider](#).

Global IP address

See [IP address](#).

GSM

Global System for Mobile Communication

Originally a European standard for mobile networks. GSM can now be described as a worldwide standard. However, in the USA and Japan, national standards were previously more frequently supported.

H

Handover

Possibility for a subscriber with a DECT handset to change from one cell to another during a call or a data connection without interrupting this connection.

Headset

Combination of microphone and headphone. A headset enables a comfortable hands free mode. Headsets that can be connected to the base via a cable (wire-bound) or via Bluetooth (wireless) are available.

HTTP Proxy

Server via which the [Network subscribers](#) can process their Internet traffic.

Hub

Uses one [Infrastructure network](#) to connect several [Network subscribers](#). All data sent to the hub by one network subscriber is forwarded to all network subscribers.

See also: [Gateway](#), [Router](#).

I

IEEE

Institute of Electrical and Electronics Engineers

International body that defines standards in electronics and electrical engineering, concerned in particular with the standardisation of LAN technology, transmission protocols, data transfer rate and wiring.

Infrastructure network

Network with central structure: All [Network subscribers](#) communicate via a central [Router](#).

Internet

Global [WAN](#). A series of protocols known as TCP/IP have been defined for exchanging data.

Every [Network subscriber](#) is identifiable via their [IP address](#). [DNS](#) assigns a [Domain name](#) to the [IP address](#).

Important services on the Internet include the World Wide Web (WWW), eMail, file transfer and discussion forums.

Internet Service Provider

Enables access to the Internet for a fee.

IP (Internet Protocol)

TCP/IP protocol on the [Internet](#). IP is responsible for addressing subscribers in a [Network](#) using [IP addresses](#) and routes data from the sender to the recipient. IP determines the paths (routing) along which the data packets travel.

IP address

A unique address for a network component within a network based on the TCP/IP protocols (e.g., LAN, Internet). On the [Internet](#), domain names are usually assigned instead of IP addresses. [DNS](#) assigns the corresponding IP address to the domain name.

The IP address has four parts (decimal numbers between 0 and 255) separated by full stops (e.g., 230.94.233.2).

The IP address is made up of the network number and the number of the [Network subscriber](#) (e.g., phone). Depending on the [Subnet mask](#), the first one, two or three parts make up the network number and the rest of the IP address addresses the network component. The network number of all the components in any one network must be identical.

IP addresses can be assigned automatically with DHCP (dynamic IP addresses) or manually (fixed IP addresses).

See also: [DHCP](#).

IP pool range

Range of IP addresses that the DHCP server can use to assign dynamic IP addresses.

L

LAN

Local Area Network

Network with a restricted physical range. A LAN can be wireless (WLAN) and/or wired.

Local IP address

The local or private IP address is the address for a network component in the local network (LAN). The network operator can assign any address they want. Devices that act as a link from a local network to the Internet (gateway or router) have a public and a private IP address.

See also [IP address](#).

Local SIP port

See [SIP port/Local SIP port](#).

M

MAC address

Media Access Control address

Hardware address by means of which each network device (e.g., network card, switch, phone) can be uniquely identified worldwide. It consists of six parts (hexadecimal numbers) separated by "-" (e.g., 00-90-65-44-00-3A).

The MAC address is assigned by the manufacturer and cannot be changed.

Mbps

Million bits per second

Unit of the transmission speed in a network.

MRU

Maximum Receive Unit

Defines the maximum user data volume within a data packet.

MTU

Maximum Transmission Unit

Defines the maximum length of a data packet that can be carried over the network at a time.

Music on hold

Music on hold

Music that is played while you are on a [Consultation call](#) or during [Call swapping](#). The waiting participant hears music while on hold.

N

NAT

Network Address Translation

Method for converting (private) [IP addresses](#) to one or more (public) IP addresses. NAT enables the IP addresses of [Network subscribers](#) (e.g., VoIP telephones) in a [LAN](#) to be concealed behind a shared IP address for the [Router](#) on the [Internet](#).

VoIP telephones behind a NAT router cannot be reached by VoIP servers (on account of the private IP address). To "get around" NAT, it is possible to use either [ALG](#) in the router, [STUN](#) in the VoIP telephone, or for the VoIP provider to use an [Outbound proxy](#).

If an outbound proxy is made available, you must allow for this in the VoIP settings for your phone.

Network

Group of devices. Devices can be connected in either wired or wireless mode.

Networks can also differ in range and structure:

- Range: local networks ([LAN](#)) or wide-area networks ([WAN](#))
- Structure: [Infrastructure network](#) or ad-hoc network

Network subscriber

Devices and PCs that are connected to each other in a network e.g., servers, PCs and phones.

O

Outbound proxy

Alternative NAT control mechanism to STUN and ALG.

Outbound proxies are implemented by the VoIP provider in firewall/NAT environments as an alternative to [SIP proxy servers](#). They control data traffic through the firewall.

Outbound proxy and STUN servers should not be used simultaneously.

See also: [STUN](#) and [NAT](#).

P

Paging (handset search)

Base function for locating the registered handsets. The base establishes a connection to every registered handset. The handsets start to ring.

PIN

Personal Identification Number

Protects against unauthorised use. When the PIN is activated, a number combination has to be entered to access a protected area.

You can protect your base configuration data with a system PIN (4-digit number combination).

Port

Data is exchanged between two applications in a [Network](#) via a port.

Port forwarding

The Internet gateway (e.g., your router) forwards data packets from the [Internet](#) that are directed to a certain [Port](#) to the port concerned. This allows servers in the [LAN](#) to offer services on the Internet without you needing a public IP address.

Port number

Indicates a specific application of a [Network subscriber](#). Depending on the setting in the [LAN](#), the port number is permanently assigned or it is assigned with each access.

The combination of [IP address/Port](#) number uniquely identifies the recipient or sender of a data packet within a network.

Prepare dialling

See [Block dialling](#).

Private IP address

See [Local IP address](#).

Protocol

Describes the agreements for communicating within a [Network](#). It contains rules for opening, administering and closing a connection, about data formats, time frames and possible error handling.

Proxy/proxy server

Computer program that controls the exchange of data between [Client](#) and [Server](#) in computer networks. If the phone sends a query to the VoIP server, the proxy acts as a server towards the phone and as a client towards the server. A proxy is addressed via [IP address/Domain name](#) and [Port](#).

Public IP address

The public IP address is the address for a network component on the Internet. It is assigned by the Internet service provider. Devices that act as a link from a local network to the Internet (gateway, router) have a public and a local IP address.

See also: [IP address](#), [NAT](#).

Q

Quality of Service (QoS)

Describes the quality of service in communication networks. Differentiations are made between various quality of service classes.

QoS influences the flow of data packets on the Internet e.g., by prioritising data packets, reserving bandwidth and optimising data packets.

In VoIP networks, QoS influences the voice quality. If the whole infrastructure (router, network server etc.) has QoS, the voice quality is better, i.e., fewer delays, less echoing, less crackling.

R

Registrar

The registrar manages the current IP addresses of the **Network subscriber**. When you register with your VoIP provider, your current IP address is saved on the registrar. This means you can also be reached when on the move.

RFP

Radio Fixed Part

Base stations in a multicell DECT network.

RFPI

Radio Fixed Part Identity

ID for a base station in a multicell DECT network. It includes the number (RPN) and an ID for the DECT Manager. A handset uses it to recognise the base stations it is connected to and the DECT network to which it belongs.

Ringback when the call is not answered

= CCNR (Completion of calls on no reply). If a party does not reply when called, a caller can arrange an automatic ringback. As soon as the destination phone has completed a call and is free again, the caller is called back. This feature must be supported by the exchange. The ringback request is automatically cancelled after about two hours (depending on the network provider).

Ringback when the number is busy

= CCBS (Completion of calls to busy subscriber). If a caller hears the busy tone, he or she can activate the ringback function. As soon as the connection is free, the caller is called back. As soon as the caller lifts the earpiece, the connection is made automatically.

Roaming

Possibility for a subscriber with a DECT handset to accept or make calls in all cells of a DECT network.

ROM

Read Only Memory

A type of memory that can only be read.

Router

Routes data packets within a network and between different networks via the quickest route. Can connect **Ethernet networks** and WLAN. Can be a **Gateway** to the Internet.

Routing

Routing is the transfer of data packets to another subscriber in your network. On their way to the recipient, the data packets are sent from one router to the next until they reach their destination.

If data packets were not forwarded in this way, a network like the Internet would not be possible. Routing connects the individual networks to this global system.

A router is a part of this system; it transfers data packets both within a local network and from one network to the next. Data is transferred from one network to another on the basis of a common protocol.

RPN

Radio Fixed Part Number

Number for the base station in a multicell DECT network.

RTP

Real-Time Transport Protocol

Global standard for transferring audio and video data. Often used in conjunction with UDP. In this case, RTP packets are embedded in UDP packets.

RTP port

(Local) **Port** that is used to send and receive voice data packets for VoIP.

S

Server

Provides a service to other [Network subscribers \(Clients\)](#). The term can indicate a computer/PC or an application. A server is addressed via [IP address/Domain name](#) and [Port](#).

SIP (Session Initiation Protocol)

Signalling protocol independent of voice communication. Used for establishing and ending a call. It is also possible to define parameters for voice transmission.

SIP address

See [URI](#).

SIP port/Local SIP port

(Local) [Port](#) that is used to send and receive SIP signalling data for VoIP.

SIP provider

See [VoIP provider](#).

SIP proxy server

IP address of your VoIP provider's gateway server.

Static IP address

A fixed IP address is assigned to a network component manually during network configuration. Unlike the [Dynamic IP address](#), a fixed IP address does not change.

STUN

Simple Transversal of UDP over NAT

NAT control mechanism.

STUN is a data protocol for VoIP telephones. STUN replaces the private IP address in the VoIP telephone data packets with the public address of the secure private network. To control data transfer, a STUN server is also required on the Internet. STUN cannot be implemented with symmetric NATs.

See also: [ALG](#), [Firewall](#), [NAT](#), [Outbound proxy](#).

Subnet

Segment of a [Network](#).

Subnet mask

[IP addresses](#) consist of a fixed line number and a variable subscriber number. The network number is identical for all [Network subscribers](#). The size of the network number part is determined in the subnet mask. In the subnet mask 255.255.255.0, for example, the first three parts of the IP address are the network number and the last part is the subscriber number.

Symmetric NAT

A symmetric NAT assigns different external IP addresses and port numbers to the same internal IP addresses and port numbers – depending on the external target address.

T

TCP

Transmission Control Protocol

[Transport protocol](#). Session-based transmission protocol: it sets up, monitors and terminates a connection between sender and recipient for transporting data.

TLS

Transport Layer Security

Protocol for encrypting data transmissions on the Internet. TLS is a super-ordinate [Transport protocol](#).

Transmission rate

Speed at which data is transmitted in the [WAN](#) or [LAN](#). The transmission rate is measured in data units per unit of time (Mbit/s).

Transport protocol

Controls data transport between two communication partners (applications).

See also: [UDP](#), [TCP](#), [TLS](#).

U

UDP

User Datagram Protocol

Transport protocol. Unlike [TCP](#), [UDP](#) is a non session-based protocol. UDP does not establish a fixed connection. The data packets ("datagrams") are sent as a broadcast. The recipient is solely responsible for making sure the data is received. The sender is not notified about whether it is received or not.

URI

Uniform Resource Identifier

Character string for identifying resources (e.g., eMail recipient, [http://swyx.com](#), files).

On the [Internet](#), URIs are used as a uniform identification for resources. URIs are also described as SIP addresses.

URIs can be entered in the phone as a number. By dialling a URI, you can call an Internet subscriber with VoIP equipment.

URL

Universal Resource Locator

Globally unique address of a domain on the [Internet](#).

A URL is a subtype of the [URI](#). URLs identify a resource by its location on the [Internet](#). For historical reasons, the term is often used as a synonym for URI.

User ID

See [User name](#).

User name

Name/number combination for access, e.g., to your VoIP account or your private address directory on the Internet.

V

Voice codec

See [Codec](#).

VoIP

Voice over Internet Protocol

Telephone calls are no longer placed and transmitted over the telephone network but over the [Internet](#) (or other IP networks).

VoIP provider

A VoIP, SIP or [Gateway provider](#) is an Internet service provider that provides a [Gateway](#) for Internet telephony. As the phone works with the SIP standard, your provider must support the SIP standard.

The provider routes calls from VoIP to the telephone network (analogue, ISDN and mobile) and vice versa.

W

WAN

Wide Area Network

Wide-area network that is unrestricted in terms of area (e.g., [Internet](#)).

10 Accessories

Power adapter

You only need a power adapter if your devices are not powered by PoE (Power over Ethernet).

EU: Item number: C39280-Z4-C706

UK: Item number: C39280-Z4-C745

SwyxDECT 700 SPK PRO (Site Planning Kit)

Equipment for planning and analysing your DECT multicell system. The case contains two calibrated handsets and one base station, plus other useful accessories for measuring the signal quality and wireless coverage on your DECT network.