Congratulations

Congratulations on your purchase of the Siemens Gigaset SX763 WLAN dsl telephone system! This phone´s DECT6.0 frequency standard and high-speed digital voice encoding provide reception and voice clarity that is superior to other cordless phones. And, its digital spread spectrum technology will provide you with secure, private conversations.

**DO NOT RETURN
THIS PRODUCT TO THE
STORE!**

Please read the following important information.

For Siemens Customer Care, product operation information, or for problem resolution, call toll-free

1-888-777-0211

9 a.m. to 8 p.m. Central Standard Time Monday-Saturday

SIEMENS

www.my-siemens.com

Register now!
It’s fast progress in the world of communication. Register today for the world of Siemens Communications on "my-siemens.com" and stay current with customized information on Siemens latest products and applications.
Please go to: www.icm.siemens.com/register

Contents

Schablone 2005_07_27

The Gigaset SX763 WLAN dsl

The Siemens Gigaset SX763 WLAN dsl is a powerful but simple communications device for connecting your PC or local area network (LAN) to the Internet (via DSL). It contains an integrated ADSL modem (ADSL /ADSL2+) enabling you to access the Internet easily.

You can connect your PC wirelessly to the Gigaset SX763 WLAN dsl and create a wireless local area network (WLAN). The device supports Super G technology making this possible. The transmission rate in the wireless local area network can be increased to 108 Mbps thanks to channel bundling. For network security, wireless transmission can be encrypted using the WPA standard or 64-/128-bit WEP.

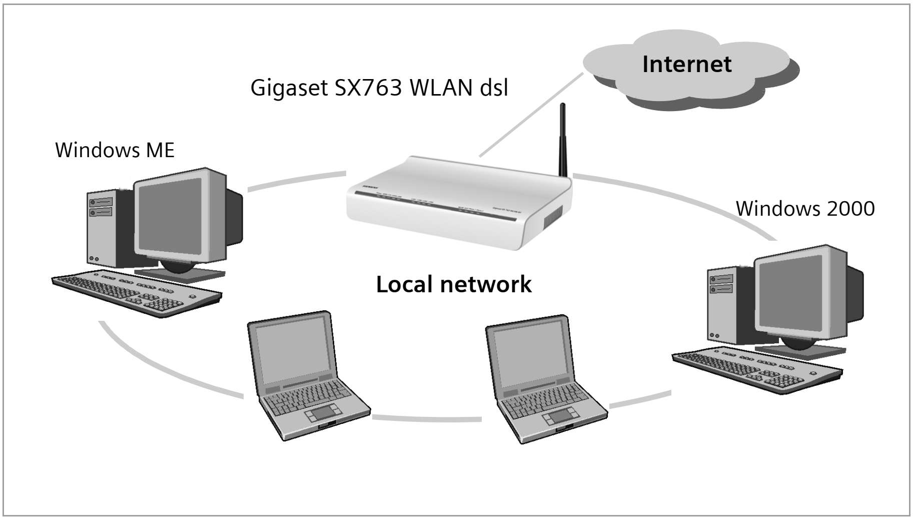
The Gigaset SX763 WLAN dsl also offers the functions of a PABX for Internet telephony (VoIP) and fixed network telephony. You can connect up to two traditional analogue terminals and then use these analogue phones both to make calls via the Internet or also via an existing analogue telephone line. In addition, you can operate SIP clients (wireless SIP telephones and PCs with appropriate software) as PABX extensions and therefore also make calls via the Internet or fixed network.

The Gigaset SX763 WLAN dsl allows several users to access the Internet simultaneously. A single user account can be shared if your Internet service provider permits this. If you want to surf the Internet and make calls using the Internet at the lowest possible cost, the Gigaset SX763 WLAN dsl is a convenient and simple solution.

The Gigaset SX763 WLAN dsl has an extensive range of functions but remains simple to handle. It can be configured and operational within a few minutes.

Local area networks with Gigaset products

You can use the Siemens Gigaset SX763 WLAN dsl to set up a local area network, for example a home network. All PCs in this network can communicate with each other and have access to the Internet.



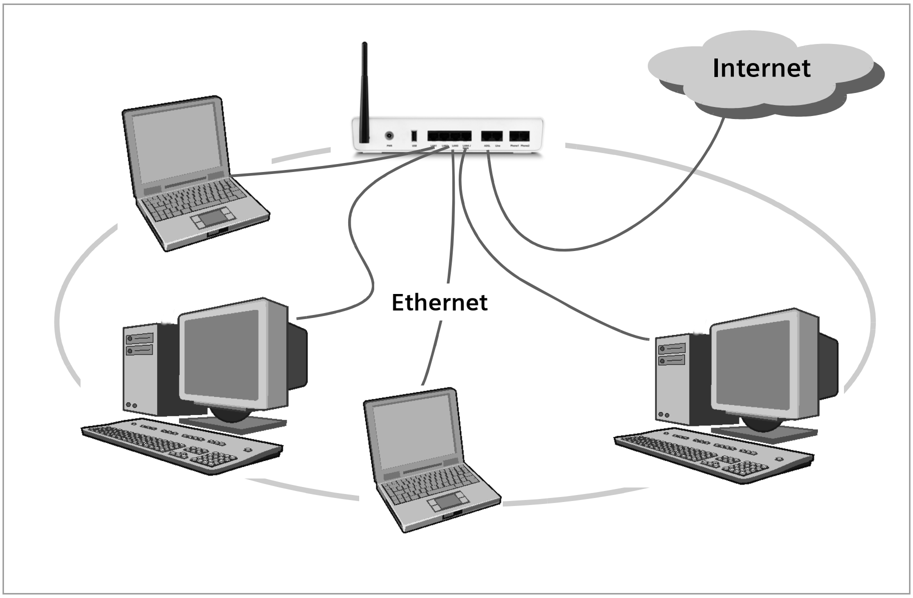
There are various ways in which you can set up the network using a Gigaset SX763 WLAN dsl.

- set up a wired local area network (Ethernet) and allow the connected PCs access to the Internet (page 7).
- set up a wireless local area network (WLAN) and allow the connected PCs access to the Internet (page 8).
- set up a local area network comprising wireless and wired network components (page 10).

Wired local area network (Ethernet)

In a wired local area network, PCs communicate with one another via an Ethernet cable. When the Siemens Gigaset SX763 WLAN dsl is used, it establishes the connection between the PCs. For this it has four Ethernet LAN ports for connecting four PCs. The PCs have to be equipped with a network port (Ethernet). New PCs frequently already have this port. For older PCs you need to install an Ethernet network card. The PC and the Ethernet LAN port on the Gigaset SX763 WLAN dsl are connected using an Ethernet cable (CAT5). There is one supplied. You can obtain additional Ethernet cables from your retailer.

The Gigaset SX763 WLAN dsl allows all PCs to access the Internet simultaneously.



Wireless local area network (WLAN)

In a wireless local area network (WLAN) PCs are linked without wires or cables. The PCs have to be equipped with a wireless local area network adapter (WLAN adapter), for example a Gigaset USB Adapter 108.

We generally differentiate between two types of wireless network:

- infrastructure mode
- ad-hoc mode

infrastructure mode

Infrastructure mode connects wireless and wired networks with one another. In addition to the mobile stations, infrastructure mode needs an access point such as the Gigaset SX763 WLAN dsl. In infrastructure mode, the stations in the network always communicate via this access point. The access point sets up the wireless network on a permanent basis. Each station that wants to be part of the wireless network must first register with the access point before it can exchange data.

The access point establishes the connection between the mobile stations of a wireless network and a wired LAN (Ethernet) or the Internet. In this case this is described as the device's router functionality. The router sends data packets that are not addressed to stations within the network "outside" and forwards data packets originating from "outside" to the appropriate station within the network.

You can use the Gigaset SX763 WLAN dsl to connect

- wirelessly networked PCs to the Internet and
- wirelessly networked PCs to an Ethernet network.

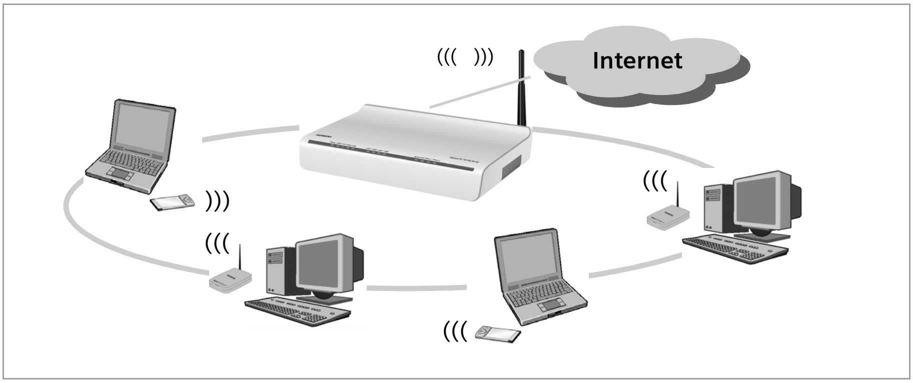
Infrastructure mode is the default configuration for the Gigaset SX763 WLAN dsl.

Ad-hoc mode

An ad-hoc network is a wireless network that has been configured without an access point or a router. The mobile network components that communicate with each other directly and wirelessly form the network on an "ad-hoc" basis, i.e. as and when required. All the stations in the network have the same rights. Ad-hoc networks are used wherever communications networks have to be set up quickly and there is no existing network infrastructure, and where the participants are on the move.

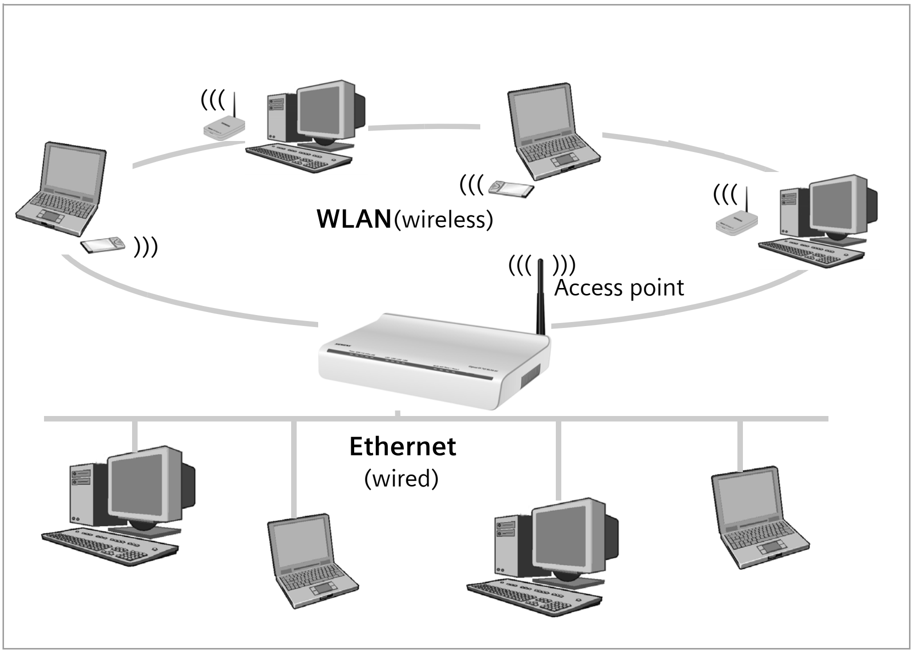
Linking wireless networks with the Internet

The Gigaset SX763 WLAN dsl has an ADSL interface that permits all stations within its local area network to access the Internet simultaneously. To be able to use this functionality you need a DSL connection obtainable from an Internet service provider. Find out whether your service provider supports parallel access by several PCs.



Linking a wireless network to an Ethernet

Wireless local area networks can work easily together with existing Ethernet networks. If you wish to connect mobile stations to an existing wired network, you must group together all mobile stations into a wireless local area network in infrastructure mode.



The Gigaset SX763 WLAN dsl has four Ethernet interfaces (LAN ports). Up to four PCs can be connected directly to these LAN ports.

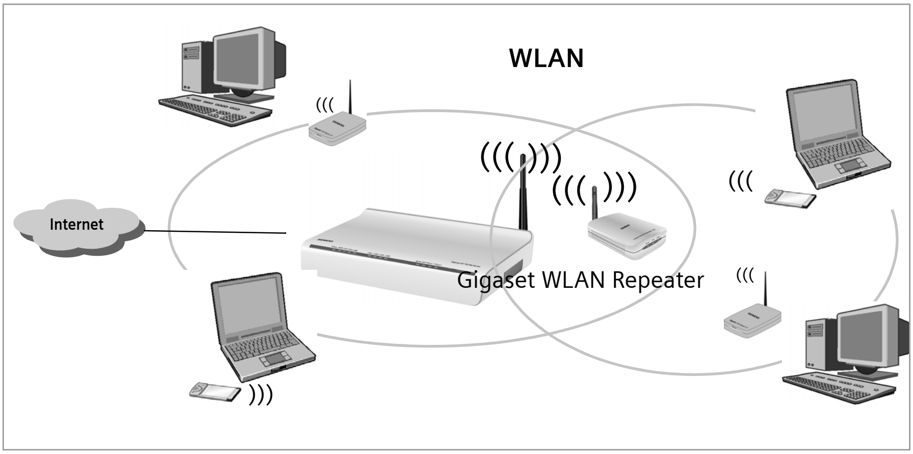
All PCs can access the Internet via the Gigaset SX763 WLAN dsl.

Please remember:

You can also connect an Ethernet router to a LAN port to access a larger Ethernet. If you want to link the Gigaset WLAN network to an existing network, a large number of settings have to be applied. Therefore we cannot provide a general example for this use; the configuration depends greatly on the networks in question. We advise having the configuration of such a network carried out by a specialist.

Extending the wireless network coverage with a repeater

Using the Gigaset WLAN Repeater, you can extend your wireless network's coverage. Set it up within the range of your network. The repeater will now transmit data traffic into its own wireless area. This technology allows you to set up wireless networks that cover a much larger area than is possible with a single Gigaset SX763 WLAN dsl.

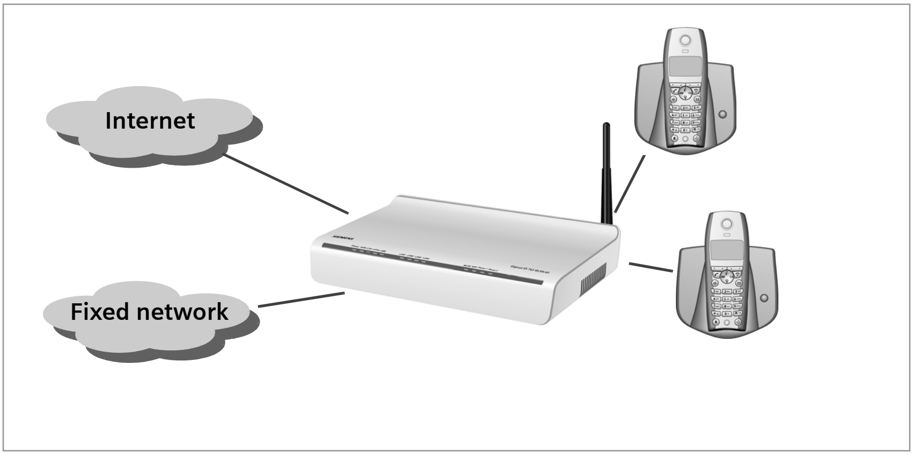


PCs to be connected in a wireless local area network via a repeater must be equipped with a wireless network adapter or a USB adapter.

Internet telephony and connecting analogue phones

The Gigaset SX763 WLAN dsl allows a combination of analogue fixed network telephony and Internet telephony (VoIP) over DSL for two analogue telephones and four other wired or wireless VoIP telephones or SIP clients.

This provides you with the full benefits of both technologies. You can make use of the low-cost call rates of Internet telephony without any additional equipment. In addition, you have the option of using your analogue fixed network connection. The type of calls that are cheaper for you will depend on what calls you make and when you make them, and the rates offered by your service provider. The Gigaset SX763 WLAN dsl gives you the complete freedom of choice at any time.



You can choose whether to connect any two analogue phones, a fax machine or an answering machine to the phone ports. You can configure these ports using the Gigaset SX763 WLAN dsl.

The PABX of the Gigaset SX763 WLAN dsl allows you to connect wireless SIP phones (WLAN handsets) and PCs with SIP clients (software for Internet telephony) as extensions. You can use all functions of your PABX for Internet telephony also.

You will need the relevant access data for your VoIP provider to configure Internet telephony.

Please remember:

You can only be reached via the Internet (VoIP) when an **active Internet connection** is established. You can still be called any time via the fixed network, however.

Features and applications

The Gigaset SX763 WLAN dsl's wide range of features makes it ideal for a large number of applications, such as:

- **Internet access**

  The Gigaset SX763 WLAN dsl allows several users to have Internet access via the integrated ADSL /ADSL2+ modem.

  – Since many DSL providers permit communication with end users via the PPPoE protocol, the Gigaset SX763 WLAN dsl has an integrated Client for this protocol, so you no longer have to install this service on your PC.

  – The Gigaset SX763 WLAN dsl supports shared Internet access for up to 252 users. This means several users in your network can surf the Internet at the same time, all using the same Internet account.

- **Setting up a local area network**

  The Gigaset SX763 WLAN dsl offers the following possibilities:

  – Four devices connected via Ethernet ports with a transmission speed of 10 or 100 Mbps (with automatic recognition).

  – Up to 252 mobile terminals connected via a radio interface with a transmission speed of up to 108 Mbps. It complies with IEEE 802.11g standard and can work with all products that satisfy Standard IEEE 802.11b or 802.11g. The Super G technology allows for high transmission speed.

  – Using a Gigaset SX763 WLAN dsl makes it easy to set up a network at home or in small offices. For example, users can exchange data or share resources in the network, such as a file server or printer. You can connect a USB hard disk or a printer to the USB interface of the Gigaset SX763 WLAN dsl and make them available to all users in your network.

  The Gigaset SX763 WLAN dsl supports DHCP for dynamic IP configuration of the local area network, and DNS for domain name mapping.

- **Connecting phones and Internet telephony**

  The Gigaset SX763 WLAN dsl permits

  – Internet telephony via the DSL port,

  – Fixed network telephony via the analogue port,

  – Connection of two analogue phones for Internet telephony and for fixed network calls as well as connection of wireless SIP phones and PCs with SIP clients for Internet telephony

  – Connection of an answering machine or fax.

  Data transfer for VoIP is handled by the SIP protocol with high connection and voice quality. If the Internet connection has been interrupted or you do not want to make a call via VoIP, you can simply make a call on the fixed network.

- **Security functions**

  The Gigaset SX763 WLAN dsl offers comprehensive security measures:

  – Firewall protection against unauthorised access from the Internet

    All PCs in the local area network use the Public IP address of the Gigaset SX763 WLAN dsl for their Internet connections, which makes them 'invisible' on the Internet. The Gigaset SX763 WLAN dsl only allows access from the Internet if it has been requested from the local area network.

    With the firewall the Gigaset SX763 WLAN dsl also offers comprehensive protection against hacker attacks.

  – Service filtering

    The Gigaset SX763 WLAN dsl can filter Internet access. Here you determine which PCs may access which Internet services.

  – Access control and encryption for the local area network

    You can use various encryption methods and authentication methods (WEP, WPA/WPA2, 802.1x MAC access control) to prevent unauthorised access to your wireless LAN or make data illegible to unauthorised parties.

- **Offering your own services on the Internet**

  – If you want to offer your own services on the Internet, you can set up the Gigaset SX763 WLAN dsl as a virtual server without permitting further access to the local area network.

  – DMZ (Exposed Host)

    This allows you to release a PC in your local area network for unlimited access from the Internet. Note that in this case your local area network will no longer be adequately protected against Internet attacks.

  – You can connect a USB hub to the USB port on your Gigaset SX763 WLAN dsl and thereby at the same time provide a printer and a storage medium for all clients in your local area network.

First steps

Pack contents

The package contains the following components:

- 1 Gigaset SX763 WLAN dsl,
- 1 mains adapter (230 V/12V 1.5A DC),
- 1 LAN cable (CAT5, yellow),
- DSL cable (CAT5, black, connection to splitter)
- 1 telephone cable (green, connection to splitter),
- 1 CD with this user guide,
- 1 supplementary sheet with information about security and disposing of the device.

System requirements

You require the following components to operate your Gigaset SX763 WLAN dsl:

- A PC with
  - an 802.11g or 802.11b compatible wireless Network adapter
    Owing to the superior range and the high data throughput from the Super G technology, we recommend you use the Gigaset PC Card 108 or the Gigaset USB Adapter 108.

  Note:

  An 802.11b-compatible network adapter has a maximum transmission speed of 11 Mbps. An 802.11g-compatible network adapter has a maximum transmission speed of 54 Mbps. A network adapter that supports Super G has a maximum transmission speed of 108 Mbps.

  or

  - an Ethernet port (10Base-T or 100Base-TX)
- A Web browser such as Microsoft Internet Explorer V 6.0 or higher or Mozilla Firefox V 1.0 or higher for configuring your Gigaset SX763 WLAN dsl.

Note:

We recommend you use the Gigaset SX763 WLAN dsl with the Windows XP operating system because only then are all system requirements for using the device fulfilled.

- To access the Internet you require
  - a DSL port (splitter),
  - the access data for your Internet service provider.
- For Internet telephony you also require
  - the access data for your VoIP service provider
  - a phone for connecting to the Gigaset SX763 WLAN dsl or a PC with a SIP client or a VoIP telephone

For experienced users

The default settings for the Gigaset SX763 WLAN dsl are:

- IP address: 192.168.2.1
- Subnet mask: 255.255.255.0
- SSID: ConnectionPoint
- Radio channel: 11

Caution: By default there is no encryption active. Please be sure to make your network secure. You will find information about this in the section entitled "Configuring wireless connections" on page 77.

Trademarks

Microsoft, Windows 98/SE, Windows ME, Windows 2000, Windows XP and Internet Explorer are registered trademarks of the Microsoft Corporation.

Mozilla Firefox is a registered trademark of the Mozilla Organisation.

Super G is a registered trademark of Atheros Communications, Inc.

Overview of the installation steps

1. First install an Ethernet network card or a wireless Network adapter such as the Gigaset PC Card 108 in the PCs you want to connect to the Gigaset SX763 WLAN dsl. The installation is described in the user guides for these products.

   Please remember:

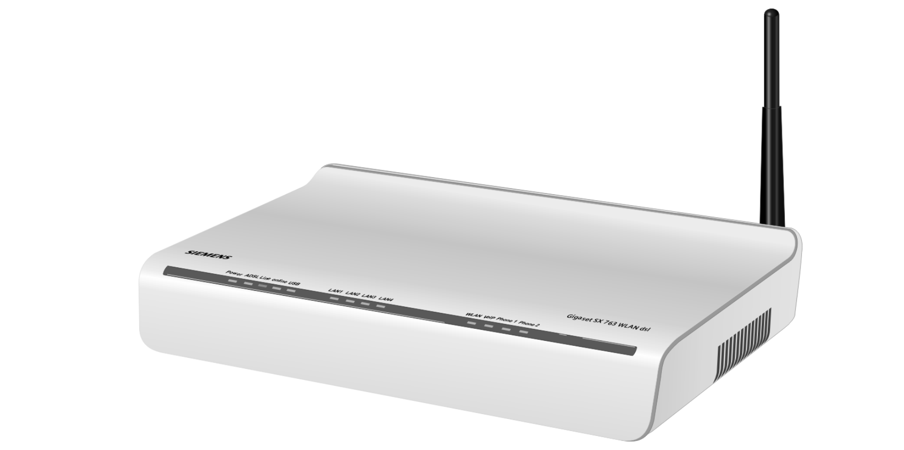
   When installing wireless network adapters, use the default SSID for the Gigaset SX763 WLAN dsl: **ConnectionPoint**.

2. Then make the necessary connections (PCs, phones, splitter) to the Gigaset SX763 WLAN dsl and activate the device (page 19).
3. Before the PCs can communicate with the Gigaset SX763 WLAN dsl and with each other in a local network, you may have to change your network settings (page 28). Configure these network settings on **one** PC first so that it can establish a connection to the Gigaset SX763 WLAN dsl. You can then use this PC to configure the device. To find out how to do this, refer to the section entitled "Das lokale Netzwerk konfigurieren" on page 127.
4. In a wireless connection you establish the link from the PC's wireless network adapter to the Gigaset SX763 WLAN dsl. This is described in the user guide for the network adapter.
5. Then configure the Gigaset SX763 WLAN dsl to activate the device's Internet access (refer to the section entitled "Basic Setup Wizard" on page 35). To do this you will require the access data from your Internet service provider.

- If you want to connect more PCs to the Gigaset SX763 WLAN dsl, configure their network settings so as to set up the local network (refer to the section entitled "Das lokale Netzwerk konfigurieren" on page 127).
- If you want to use the Gigaset SX763 WLAN dsl for Internet telephony, you must configure your VoIP provider's registration data (refer to the section entitled "Setting up Internet telephony (VoIP)" on page 87).
- If you wish to use other functions of the Gigaset SX763 WLAN dsl, for example the comprehensive security features, use the Security Setup (page 42) or the Advanced Setup (page 52).

Setting up the Gigaset SX763 WLAN dsl

Front panel



The Gigaset SX763 WLAN dsl can be set up in any suitable location in the home or office. You do not need any special wiring. However, you should comply with the following guidelines:

- Operate the Gigaset SX763 WLAN dsl only indoors within a temperature range of 0 to +40 °C. Do not position the Gigaset SX763 WLAN dsl near sources of heat. Do not cover the ventilation slots. High temperatures can damage the device.
- A mains socket for 220/230 V~ and a connection socket for the splitter or LAN must be available in the place where you set up the Gigaset SX763 WLAN dsl.
- Do not position the device in the immediate vicinity of stereo equipment, TV sets or microwave ovens. This may cause interference.
- Position the Gigaset SX763 WLAN dsl so that it is as near to the centre of your wireless network as possible. The general rule is: The higher you place the antennae, the better the performance. Make sure that the place where you position the Gigaset SX763 WLAN dsl offers optimum reception throughout the house or office.
- Position the Gigaset SX763 WLAN dsl on a non-slip surface. The router feet do not normally leave any traces on the surface they are on. However, some furniture surfaces may contain substances that attack and soften the router's rubber feet. The feet may well mark the furniture surface in this case.
- Position the Gigaset SX763 WLAN dsl so that it cannot fall down and damage the antennae.
- Do not place the Gigaset SX763 WLAN dsl on any furniture surface that could be affected by the heat from the device.

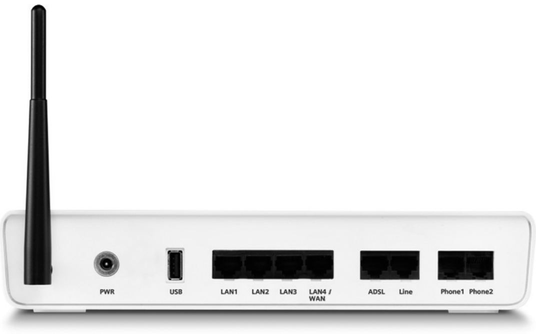
- Lay the cables so that nobody can trip over them. You should not cover the cables with anything.

Please remember:

Network connections (LAN) via cables and telephone lines may only be set up with the Gigaset SX763 WLAN dsl within enclosed rooms.

Connecting and activating the Gigaset SX763 WLAN dsl

Ports on the rear panel



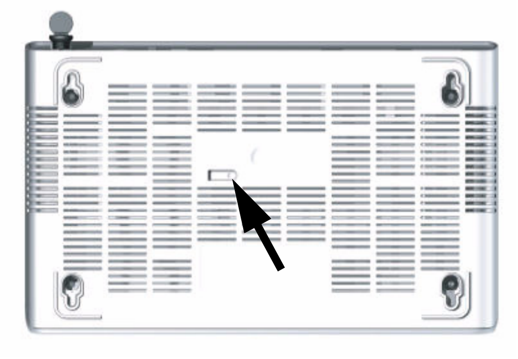
The back panel of the Gigaset SX763 WLAN dsl houses the ports.

Element	Description
PWR	Socket for the mains adapter supplied. **Warning**: Using the wrong power supply unit may damage the Gigaset SX763 WLAN dsl.
USB	USB port for printer or USB memory.
LAN1 – LAN4/WAN	Four 10/100 Mbps switch ports with automatic recognition (RJ-45). You can connect up to four devices with Ethernet ports (such as PCs, a Hub or Switch). You can connect an external VDLS or cable modem to the LAN4 port. The integrated ADLS modem is then deactivated. You will find additional information on the configuration settings in the relevant section.
ADSL	DSL socket for connecting the integrated modem to the DSL port of the splitter

Element	Description
Line	Socket for connecting the phone line to the telephone port on the splitter
Phone1/2	Sockets for connecting two phones, fax or answering machine

Reset button

The underside of the Gigaset SX763 WLAN dsl houses the reset button.



Reboot function: Press and hold the right end of the button for more than 1 second but less than 5 seconds to reboot the device. This does not affect the configuration settings.

Reset function: Press and hold the right end of the button for at least 5 seconds to return all settings to factory settings.
Warning: This will clear all the configuration settings you have made since the initial startup.
Updated firmware will not be affected.

Connecting to the splitter data port

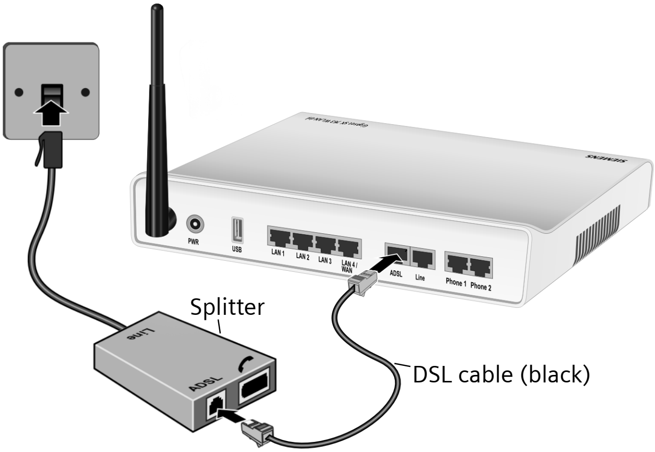
You can operate the Gigaset SX763 WLAN dsl in two different operating modes in order to set up an Internet connection:

- with an integrated ADSL modem

- with an external modem, such as a VDSL or cable modem

Using the integrated ADSL modem

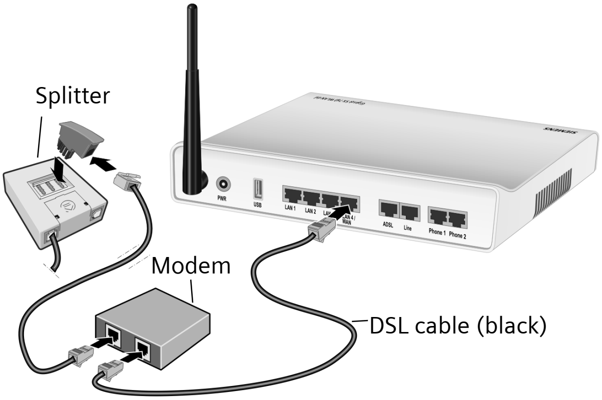
→ Connect the **ADSL** port on the Gigaset SX763 WLAN dsl with the ADSL socket on the splitter. To do this, use one of the phone cords supplied (**black**).



Using an external modem

→ Connect the **LAN4** port on the Gigaset SX763 WLAN dsl with an external modem. To do this, use one of the phone cords supplied (**black**).

→ Then connect this modem with the ADSL socket on the splitter.



Connecting to the phone port

To make conventional calls via the fixed network, you must connect your Gigaset SX763 WLAN dsl with the phone port of the splitter.

Analogue phone port

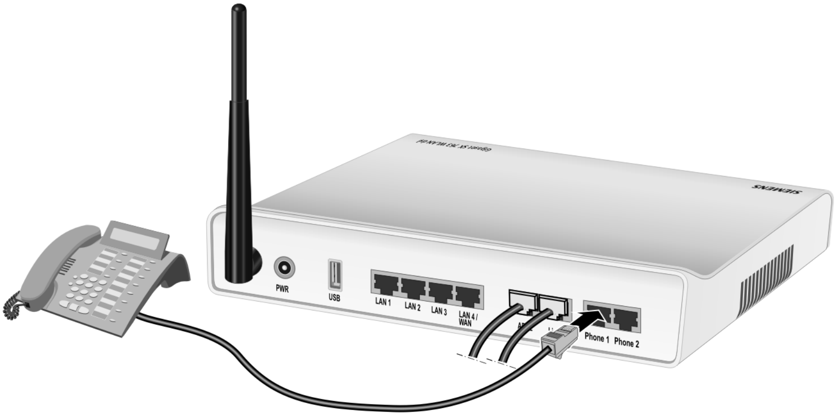
→ Connect the Gigaset SX763 WLAN dsl with the splitter as follows:

- Insert one plug of the phone cord supplied (**green**) into the **Line** port on the Gigaset SX763 WLAN dsl.
- Plug the other connector on the telephone cable into the phone socket on the splitter.

Connecting to the phone

➞ Connect the Gigaset SX763 WLAN dsl with the analogue phone as follows:

– Insert the plug of the telephone into the **Phone 1** or **Phone 2** port on the Gigaset SX763 WLAN dsl.



Note:

You cannot make calls in the event of a power failure. Emergency numbers are also not accessible in this case.

Connecting to the PC

You can connect wired or wireless PCs to your Gigaset SX763 WLAN dsl to create a local area network (LAN).

First connect just **one** PC to the Gigaset SX763 WLAN dsl. You can then carry out the general configuration. (If you wish to connect more PCs, please turn to page 29.)

Wireless

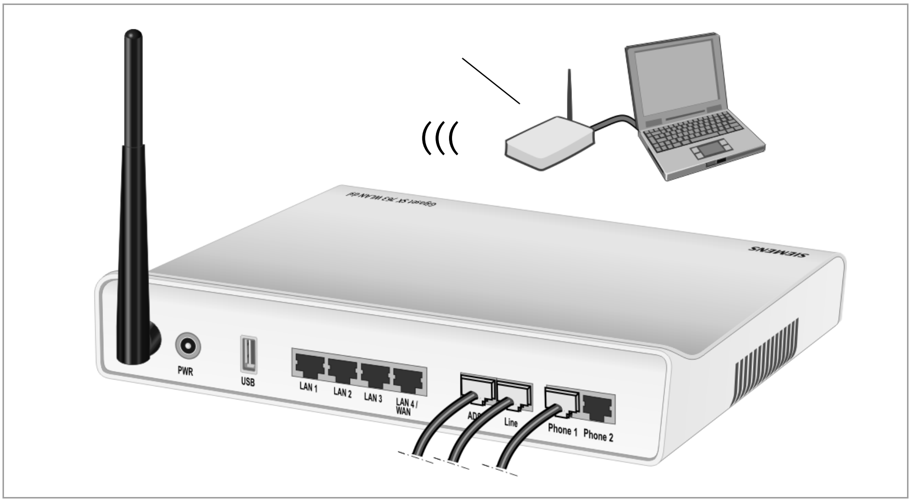
A wireless connection is made using a wireless network adapter that must be installed in your PC. This can be an 802.11g or 802.11b-compatible wireless network adapter. Owing to the superior range and the high data throughput, we recommend that you use the Gigaset PC Card 108 or the Gigaset USB Adapter 108.

A wireless network is defined by assigning an identical SSID to all the devices.

→ You should therefore enter the SSID for the Gigaset SX763 WLAN dsl in your network adapter configuration. The default SSID for the Gigaset SX763 WLAN dsl is **ConnectionPoint**.

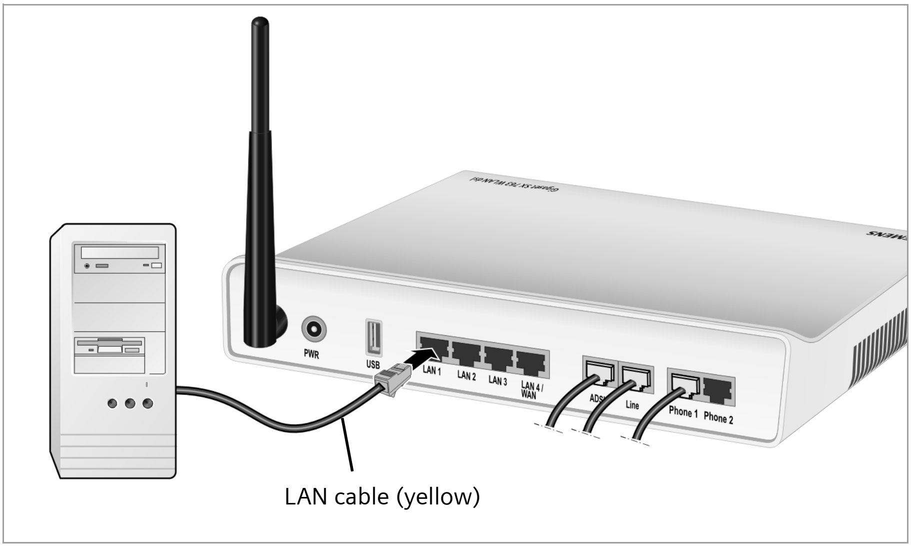
If you use a wireless network adapter from the Gigaset range, enter the SSID using the Gigaset WLAN Adapter Monitor.

If the correct SSID has been entered in your PC's wireless network adapter, the wireless link will be established automatically as soon as you connect your Gigaset SX763 WLAN dsl to the mains (page 26).



Wired

→ Connect one of the LAN ports (**LAN1** – **LAN4**) on the Gigaset SX763 WLAN dsl to the Ethernet network card in your PC. To do this, use the other LAN cable supplied (CAT5, **yellow**).



Connecting to the mains power supply

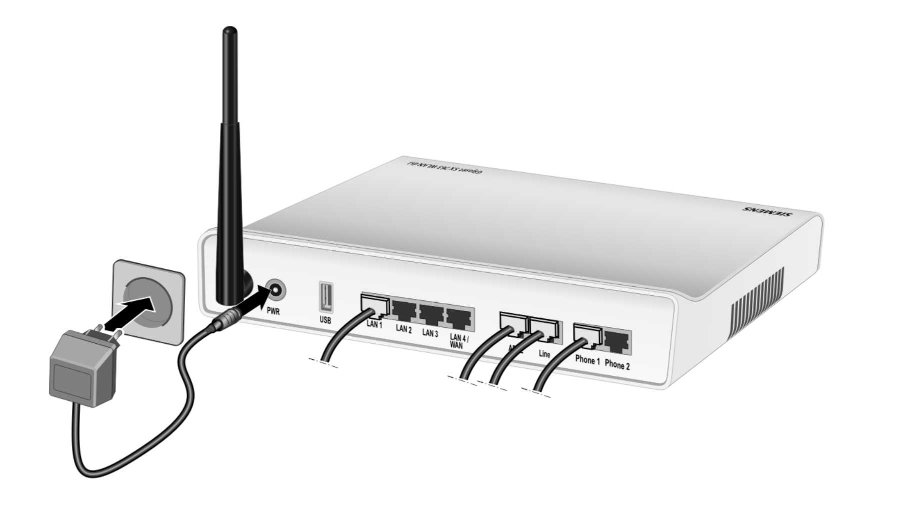
Please remember:

Only use the mains adapter supplied with the device (12V 1.5A DC).

→ Connect the mains adapter cable to the **PWR** socket on the Gigaset SX763 WLAN dsl.

→ Plug the mains adapter into a mains socket.

The Gigaset SX763 WLAN dsl is now switched on and ready for operation.



Checking the operating state

Your Gigaset SX763 WLAN dsl is now ready for use. The LED displays on the top panel of the Gigaset SX763 WLAN dsl provide information about the operating state:

The LEDs (from right to left) have the following functions:

LED	State	Status
Power	On (green)	The Gigaset SX763 WLAN dsl is connected to the mains.
	Off	The Gigaset SX763 WLAN dsl is disconnected from the mains.

LED	State	Status
Phone 1/ Phone 2	On	The relevant port is configured. The receiver of the phone connected to the port has been lifted for a call.
	Flashing	The phone is ringing and a call is being received or a call is being conducted.
	Off	The receiver is down. No call or phone conversation at present.
	On (red)	The port is not configured, no connection is possible. The receiver of the connected telephone is down.
	Flashing (red)	The port is not configured, no connection is possible. The receiver of the connected telephone is lifted.
USB	On (green)	A device is connected to the Gigaset SX763 WLAN dsl via the USB port.
	Flashing (green)	The connected device is active.
	Flashing quickly	The device connected on the USB port is using too much power (see page 134).
	Off	There is no device connected.
ADSL	On	The DSL line is connected and the DSL port is ready for use.
	Flashing	The DSL line is being synchronised. The synchronisation phases are shown as slow flashing (registering) and fast flashing (training).
	Off	The DSL line is not connected.
LAN1 – LAN4	On	A device is connected to the relevant LAN port.
	Flashing	The relevant LAN port is sending or receiving data (traffic).
	Off	There is no device connected.
WLAN	On	The radio interface is active.
	Flashing	The Gigaset SX763 WLAN dsl is sending or receiving data on the radio interface.
	Off	The radio interface has been deactivated or no radio signal is being received.
Line	On	One of the connected phones' receivers has been lifted for a call (fixed network telephony).
	Flashing	The phone is ringing and a fixed network call is being received or someone is waiting on the line.
	Off	There is currently no fixed network connection.
VoIP	On	At least one port is configured for VoIP and VoiP access is registered with the provider.
	Flashing	A call is currently being made via the Internet.
	Off	There is currently no connection for Internet telephony.
Online	On	Connection to the Internet has been established.
	Off	There is no Internet connection.

When the device is ready for use, the LEDs light up as follows:

- The **Power** LED on the front lights up.
- The **ADSL** LED flashes to indicate that the DSL connection is being synchronised. Once this process is complete, the ADSL LED lights up permanently.
- The **WLAN** LED lights up to indicate that the Gigaset SX763 WLAN dsl is ready to establish wireless connections.

  The radio link to a PC that is connected by means of a wireless network adapter is opened automatically provided the network adapter has been configured with the same SSID as the Gigaset SX763 WLAN dsl. It can take a few seconds for the wireless connection to be established. The **WLAN** LED flashes when data is sent or received via this connection.
- The **LAN** LEDs light up if a device is connected to the corresponding LAN port.

If this is not the case, refer to the section entitled Troubleshooting on (page 134).

Network configuration of the PCs

In order to communicate via the Gigaset SX763 WLAN dsl, **network configuration** must be performed on the connected PCs.

With

- **Windows XP** or
- **Windows 2000**

operating systems, this usually takes place automatically provided you have not made any changes to the standard settings for the network configuration.

With **Windows 98/SE** you have to carry out the network configuration.

The description of the network configuration can be found on the CD-ROM.

Making the basic settings

You can now make the basic settings for Internet access using the user interface of the Gigaset SX763 WLAN dsl (page 30).

If you want to connect additional PCs to the Gigaset SX763 WLAN dsl, please read the next section.

Connecting and configuring additional PCs (optional)

Once you have configured one PC as described above you can connect additional PCs to the Gigaset SX763 WLAN dsl. You will need an additional cable for each PC you want to connect via cable. For the wireless connection of additional PCs, you will need a wireless network adapter.

Wireless

→ Install wireless network adapters in each other PC as described in the corresponding user guide, making sure that the SSID of all wireless network components (Gigaset SX763 WLAN dsl and network adapters) is **identical**. If you have not changed the SSID in the Basic Setup Wizard wizard, the default setting will be **ConnectionPoint**.

→ If necessary, set up the network for each newly connected PC (page 28).

Wired

→ Connect the network cards of each additional PC to a free LAN port (**LAN1** – **LAN4**) on the Gigaset SX763 WLAN dsl using an Ethernet cable.

→ Make sure that the corresponding LAN LED on the front of your Gigaset SX763 WLAN dsl flashes.

→ If necessary, set up the network for each newly connected PC (page 28).

→ Reboot the additional PCs.

The user interface

You have connected a PC to the Gigaset SX763 WLAN dsl and possibly made the settings in the local area network. You can now configure the Gigaset SX763 WLAN dsl using this PC from the user interface of the Gigaset SX763 WLAN dsl. We recommend for initial configuration that you connect the PC in wired mode. As Internet browser we recommend Microsoft Internet Explorer V 6.0 or higher, or Mozilla Firefox V 1.0 or higher.

Note:

To start the configuration environment, you may need to deactivate the HTTP proxy for your browser (see page 134 for Windows XP and page 142 for Windows 2000).

If you use Windows XP Service Pack 2 you need to configure the popup blocker (see page 134).

If you use a firewall it must allow connection to the Gigaset SX763 WLAN dsl. For details, refer to the user guide for your firewall. If necessary, deactivate the firewall while you configure your Gigaset SX763 WLAN dsl.

Starting the user interface

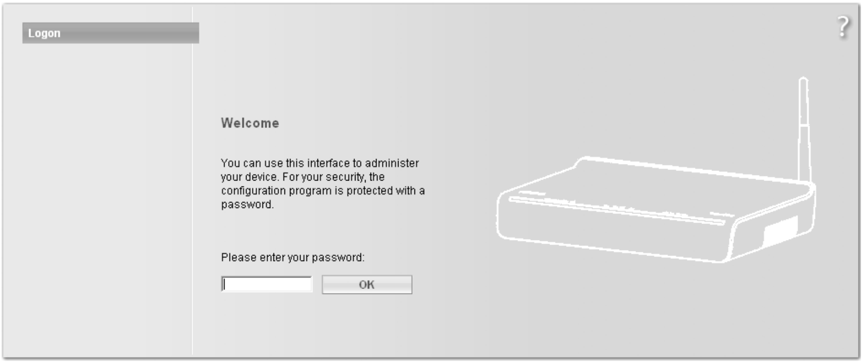
To access the user interface of the Gigaset SX763 WLAN dsl:

➙ Start your Internet browser.

➙ Enter the IP address of the Gigaset SX763 WLAN dsl in the browser's address field:

`http://sx763` or **`http://192.168.2.1`**

The login screen appears:



Welcome

You can use this interface to administer your device. For your security, the configuration program is protected with a password.

Please enter your password:

For your security, the configuration program is protected with a password. The default password is ***admin***.

➙ Enter the password.

➙ Click ***OK***.

Note:

For security reasons you should change this password at a later stage (page 43).

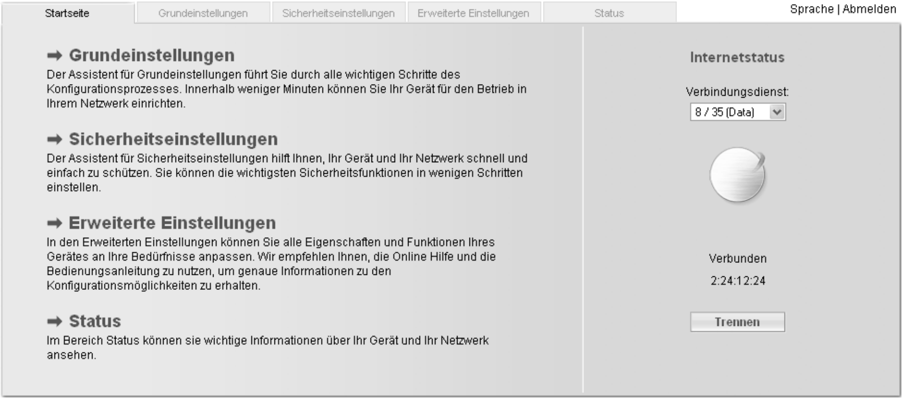
A screen appears with security information; you can skip this for the initial configuration. If you carry out all the general and security settings using the wizard as described below, your device and network will be fully protected. If not, the next time you log on you will be informed of security gaps in the configuration program.

→ Click ***OK***.

You will now see the start screen.

The start screen

The start screen is the starting point for all configuration and administration procedures.



➡ **Grundeinstellungen**

Der Assistent für Grundeinstellungen führt Sie durch alle wichtigen Schritte des Konfigurationsprozesses. Innerhalb weniger Minuten können Sie Ihr Gerät für den Betrieb in Ihrem Netzwerk einrichten.

➡ **Sicherheitseinstellungen**

Der Assistent für Sicherheitseinstellungen hilft Ihnen, Ihr Gerät und Ihr Netzwerk schnell und einfach zu schützen. Sie können die wichtigsten Sicherheitsfunktionen in wenigen Schritten einstellen.

➡ **Erweiterte Einstellungen**

In den Erweiterten Einstellungen können Sie alle Eigenschaften und Funktionen Ihres Gerätes an Ihre Bedürfnisse anpassen. Wir empfehlen Ihnen, die Online Hilfe und die Bedienungsanleitung zu nutzen, um genaue Informationen zu den Konfigurationsmöglichkeiten zu erhalten.

➡ **Status**

Im Bereich Status können sie wichtige Informationen über Ihr Gerät und Ihr Netzwerk ansehen.

Verbunden

2:24:12:24

Start screen functions

On the start screen you can make the following settings:

- Select the language for the user interface (page 33),
- View the selected connection service and the status of the Internet connection, choose a different connection service and set up or close an Internet connection (page 33). Depending on the connection mode selected, the start screen shows the status and also the button ***Connect*** or ***Disconnect***,
- open the Status menu to obtain status information about the Gigaset SX763 WLAN dsl (page 111),
- call up the wizard for the basic configuration (Basic Setup Wizard see page 35),
- call up the Security Setup Wizard (page 42),
- open the Advanced Settings menu for additional configuration options (page 52).

You can call up the wizards, the Advanced Settings menu and status information at any time and on any user interface screen using the tabs at the upper margin of the user interface.

The configuration program comprises the following functions:

Basic Setup Wizard
Use this wizard to make the settings required for connecting to the Internet. You can set up data for your region, make settings for your wireless and wired local network and configure Internet telephony. This is described from page 35.

Security Setup Wizard
This wizard allows you to take security precautions against unauthorised access to the Gigaset SX763 WLAN dsl and the local network. You can assign a password and set up encryption for wireless traffic. This is described from page 42. To protect your network, we strongly recommend that you carry out this setup.

Advanced Settings
Additional functions are offered in the Advanced Settings menu. You can configure your PABX for fixed network/Internet telephony, back up and restore the configuration data, set up the Gigaset SX763 WLAN dsl as a virtual server for the network, configure an HTTP or FTP server for access from the Internet and much more. These configuration steps are optional and can be carried out at a later stage. This is described from page 52.

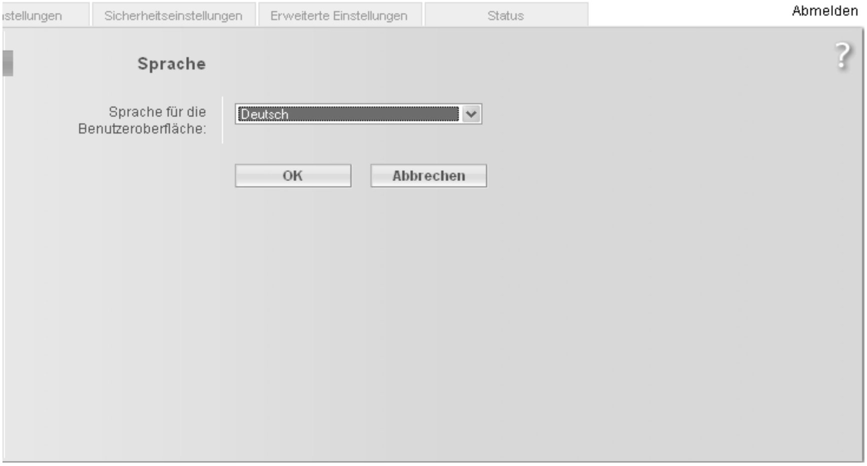
Status
You can view information about the configuration and status of the Gigaset SX763 WLAN dsl in the Status menu. This is described from page 111.

Language
You also have the opportunity to specify the language for the user interface (see page 33).

Selecting a language

The user interface can be presented in various languages.

Click ***Language*** at the top right of the start screen.



Sprache

Sprache für die Benutzeroberfläche: Deutsch

OK Abbrechen

→ If you wish to change the preset language, select the new language you require from the list.

→ Click ***OK*** to apply the setting.

Once the procedure has been concluded, the start screen will be displayed again.

Connecting to the Internet manually

Once you have configured your Internet access (see page 37 and page 56) you can establish a manual connection to the Internet on the start screen if you have selected ***Connect on demand*** or ***Connect manually*** as the Connection mode.

If, for example, you deactivated the ADSL /ADSL2+ function when configuring your Internet access, then Internet applications (such as the browser or the e-mail application) will not automatically establish a connection after they are launched. In this case you will have to establish a connection manually when required, and also close it again when you no longer need it.

To establish or end an Internet connection manually:

→ Open the start screen of the Gigaset SX763 WLAN dsl as described on page 30.

If you have already started the user interface, click the start screen tab at the top left of the window.

If you have not yet started the user interface, do so now and log on.

→ Click ***Connect*** to establish a connection to the Internet.

→ Click ***Disconnect*** if you no longer need the connection.

Note:

The ***Connect*** and ***Disconnect*** buttons will only appear on the start screen if you have **not** selected ***Always on*** as the Connection mode.

Elements on the user interface

The user interface screens contain the following elements:

Button *Log Off*

The ***Log Off*** button is always displayed on the right of the user interface. If you click ***Log Off***, the session is ended and the login screen appears again.

Help

? Click the question mark to display explanations about the current user interface screen.

Buttons and icons used by the wizards

The wizards use graphic icons to show which steps you have already carried out.

As soon as you have changed the configuration on a screen you can activate the new setting by clicking ***Next >***. The ***< Back*** button returns you to the previous configuration step, and ***Cancel*** returns you to the start screen.

Buttons in the Advanced Settings menu

OK Transfers the settings you have made to the Gigaset SX763 WLAN dsl configuration.

Cancel Deletes all the entries on a screen since the last time you clicked ***OK***. This button is not available for the initial configuration of the device.

Other buttons may be displayed depending on the function in question. These are explained in the relevant sections.

Basic Setup Wizard

The Basic Setup Wizard wizard guides you step by step through the general configuration of the Gigaset SX763 WLAN dsl. This includes settings for your region and your Internet access.

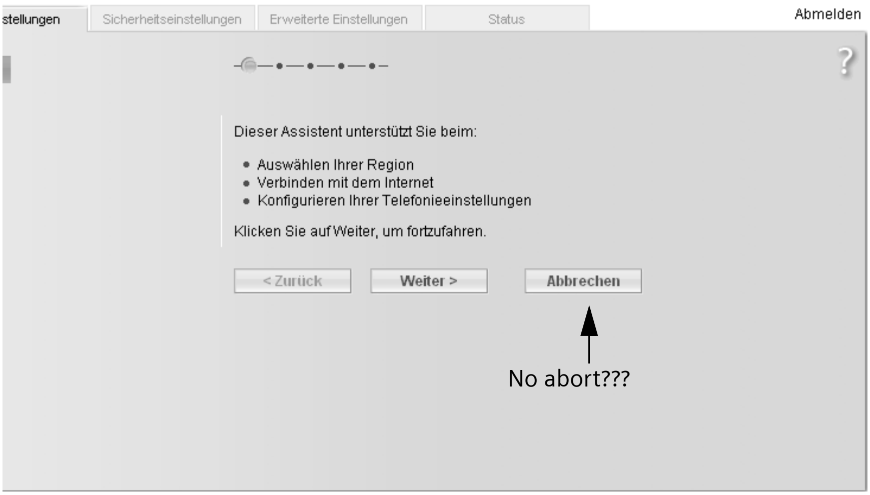
Connection to the Internet is established via the Gigaset SX763 WLAN dsl for all PCs connected to it. You need your Internet service provider's access data for the configuration. Please have this data to hand.

Note:

The Basic Setup Wizard will reconfigure your Internet settings if you have already set these. This does not affect the WLAN and LAN settings.

The access data is saved in the Gigaset SX763 WLAN dsl during configuration. Before passing the device on to somebody else or having your dealer replace it, you should always first restore the factory settings (page 108). Otherwise, unauthorised persons may use your Internet access data at your expense.

→ Select the ***Basic Setup Wizard*** option on the start screen to start the configuration.



Dieser Assistent unterstützt Sie beim:

- Auswählen Ihrer Region
- Verbinden mit dem Internet
- Konfigurieren Ihrer Telefonieeinstellungen

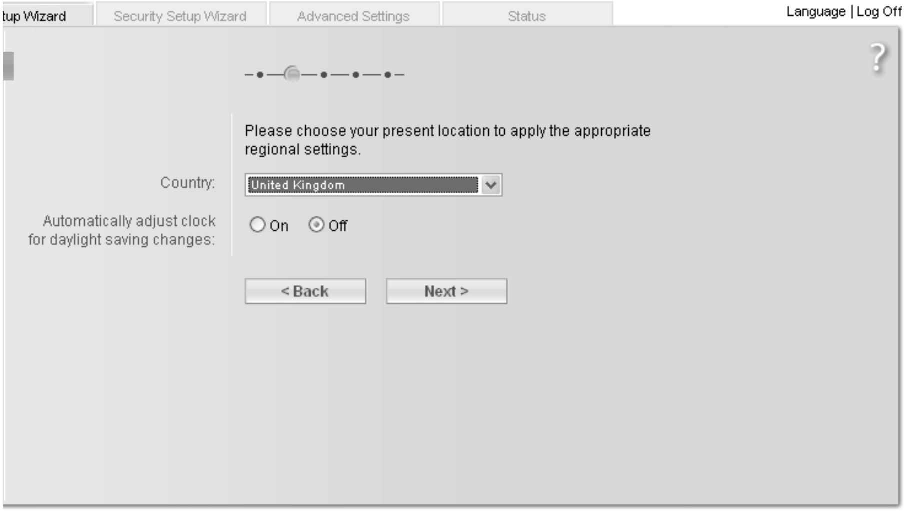
Klicken Sie auf Weiter, um fortzufahren.

No abort???

→ Click ***Next >***.

Regional Options

You can select your present location for the regional settings on this screen.



Please choose your present location to apply the appropriate regional settings.

Country: United Kingdom

Automatically adjust clock for daylight saving changes: ○ On ● Off

➙ Select the country in which you are currently located from the list. You can set the time so that it automatically switches to summer time and/or another time zone of your choice.

➙ Select the required option and/or the time zone for your location.

➙ Click ***Next >***.

Note:

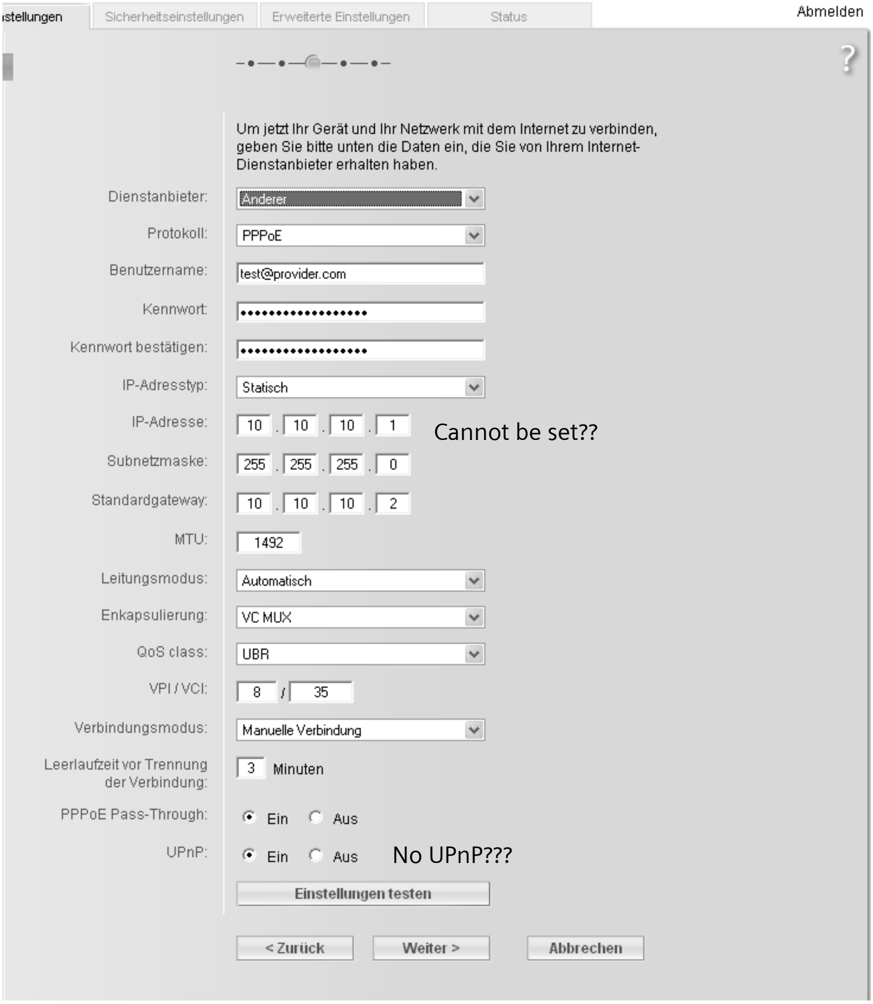
The ADSL parameters and the selection of Internet service providers will be set automatically on the following screens according to the country you choose.

Configuring Internet connections

You will find the access data you require for configuring the Internet connection in the documentation you received from your Internet service provider (ISP).

You can perform the initial configuration of your Internet connection on this screen. If you want to change the data later on, you can do this in the ***Advanced Settings*** (page 53) menu.

If you have connected an external modem, you also have to perform the initial configuration of your Internet connection in the ***Advanced Settings*** (page 53) menu.



Um jetzt Ihr Gerät und Ihr Netzwerk mit dem Internet zu verbinden, geben Sie bitte unten die Daten ein, die Sie von Ihrem Internet-Dienstanbieter erhalten haben.

Dienstanbieter:	Anderer
Protokoll:	PPPoE
Benutzername:	test@provider.com
Kennwort:	••••••••••••••••••
Kennwort bestätigen:	••••••••••••••••••
IP-Adresstyp:	Statisch
IP-Adresse:	10 . 10 . 10 . 1
Subnetzmaske:	255 . 255 . 255 . 0
Standardgateway:	10 . 10 . 10 . 2
MTU:	1492
Leitungsmodus:	Automatisch
Enkapsulierung:	VC MUX
QoS class:	UBR
VPI / VCI:	8 / 35
Verbindungsmodus:	Manuelle Verbindung
Leerlaufzeit vor Trennung der Verbindung:	3 Minuten
PPPoE Pass-Through:	● Ein ○ Aus
UPnP:	● Ein ○ Aus

Cannot be set??

No UPnP???

➥ Select your ***Service provider***. The selection menu will contain various possible providers depending on which country you have chosen. If your provider is not listed, please use the ***Other*** option.

➥ Enter the data you have been given by your service provider: ***Protocol***, ***User name*** and ***Password***.

➥ The ***IP address type*** is set automatically.

Leave the default settings for the parameters ***MTU***, ***Line mode***, ***Encapsulation***, ***QoS class*** and ***VPI / VCI***, unless your service provider has provided you with other data.

Note:

Connection to the Internet is only possible if you have entered all the data for your Internet provider correctly.

➥ Specify how Internet sessions are to be established via ***Connection mode***:

– Select ***Always on*** if the connection is to exist at all times when the Gigaset SX763 WLAN dsl is turned on.

Notes:

◆ This option can result in high connection charges if you are on a time-based tariff.

◆ You must set up the ***Always on*** option if you wish to use Internet telephony.

– Select ***Connect on demand*** if applications such as an Internet browser or an e-mail program are to connect to the Internet automatically.

– In the ***Idle time before disconnect*** field, enter a period after which the Internet connection is to end automatically if no data is transmitted (the default setting is 3 minutes).

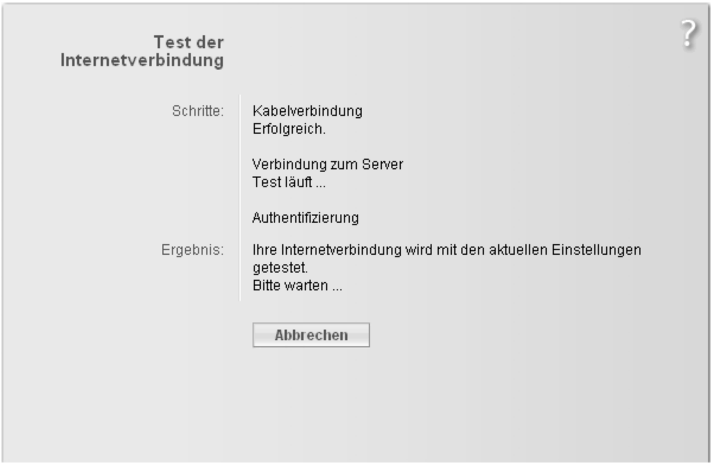
You can deactivate this function by entering "0". This means that the connection will continue to exist even if no data is transmitted. If you are on a time-based tariff, this can result in high charges. In this case you should enter a value other than "0".

This time setting only applies to the ***Connect on request*** option.

– Select ***Connect manually*** if you always want to establish and end the Internet connection manually. If you are on a time-based tariff this will save you high connection charges.

→ Click ***Test Settings*** to check the Internet connection.

> **Note:**
> If you select ***Connect on demand*** or ***Connect manually*** you can establish or end the Internet connection manually on the start screen for the configuration program (page 33).



Test der Internetverbindung

Schritte: Kabelverbindung
Erfolgreich.

Verbindung zum Server
Test läuft ...

Authentifizierung

Ergebnis: Ihre Internetverbindung wird mit den aktuellen Einstellungen getestet.
Bitte warten ...

An attempt is made to set up an Internet connection. The result is shown in a separate window. If the connection could be set up successfully, the ***Close*** button appears.

→ Click the ***Close*** button to return to the ***Basic Setup Wizard***.

PPPoE pass-through

PPPoE pass-through allows you to use an additional Internet connection (through another service provider) on one PC. Further information about this can be found on page 58.

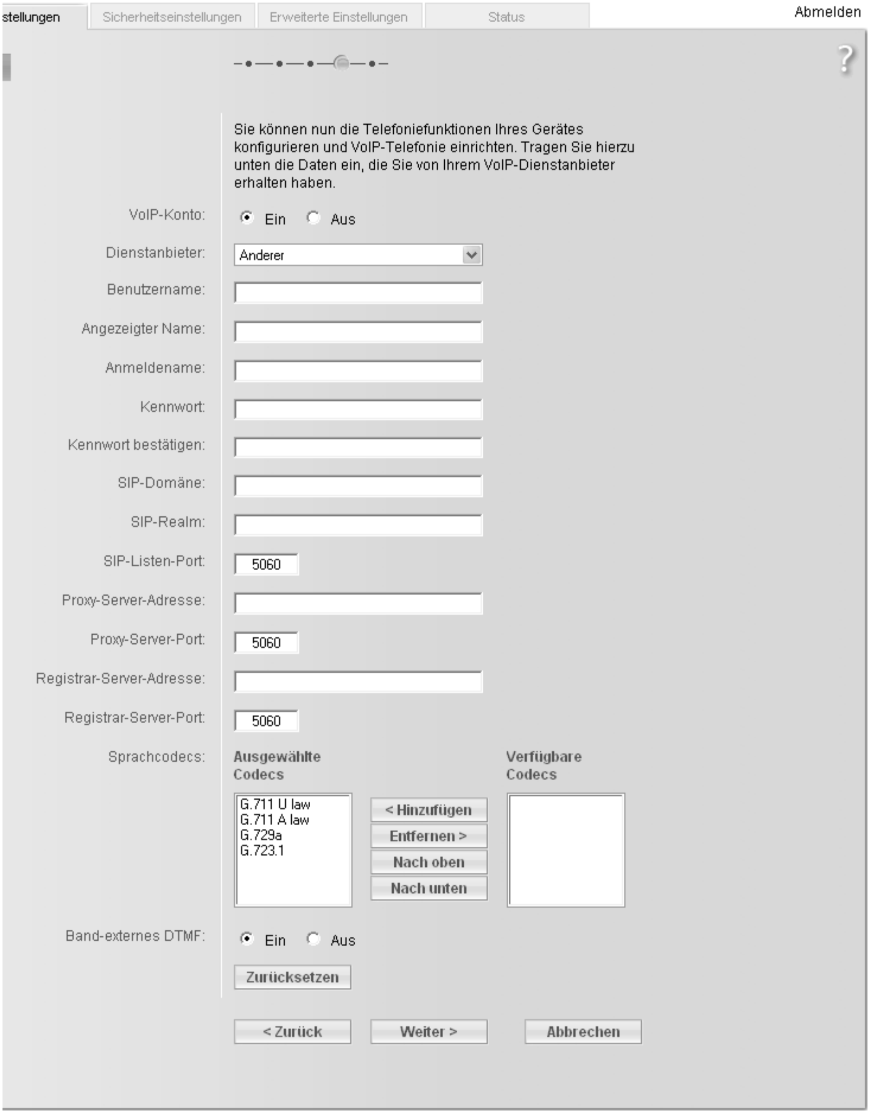
→ Deactivate ***PPPoE pass-through*** if you do not wish to use this function.

→ After entering the data click ***Next >***.

→ To go to the next step, click ***Next >***.

Telephony

You will find the access data you require for configuring Internet telephony (VoIP) in the documentation you received from your service provider.



Sie können nun die Telefoniefunktionen Ihres Gerätes konfigurieren und VoIP-Telefonie einrichten. Tragen Sie hierzu unten die Daten ein, die Sie von Ihrem VoIP-Dienstanbieter erhalten haben.

VoIP-Konto: ● Ein ○ Aus

Dienstanbieter: Anderer

Benutzername:

Angezeigter Name:

Anmeldename:

Kennwort:

Kennwort bestätigen:

SIP-Domäne:

SIP-Realm:

SIP-Listen-Port: 5060

Proxy-Server-Adresse:

Proxy-Server-Port: 5060

Registrar-Server-Adresse:

Registrar-Server-Port: 5060

Sprachcodecs: Ausgewählte Codecs: G.711 U law, G.711 A law, G.729a, G.723.1 — Verfügbare Codecs:

Band-externes DTMF: ● Ein ○ Aus

→ Select ***On*** for ***VoIP account*** if you wish to use Internet telephony (default setting).

→ Select ***Other*** from the ***Service provider*** selection menu (default setting) or, if required, use one of the suggested providers from the list. Enter the data you have received from your service provider:

User name, ***Displayed name***, ***Authorization user name***, ***Password***, ***SIP domain***, ***SIP realm***, ***Proxy server address and Registrar server address***.

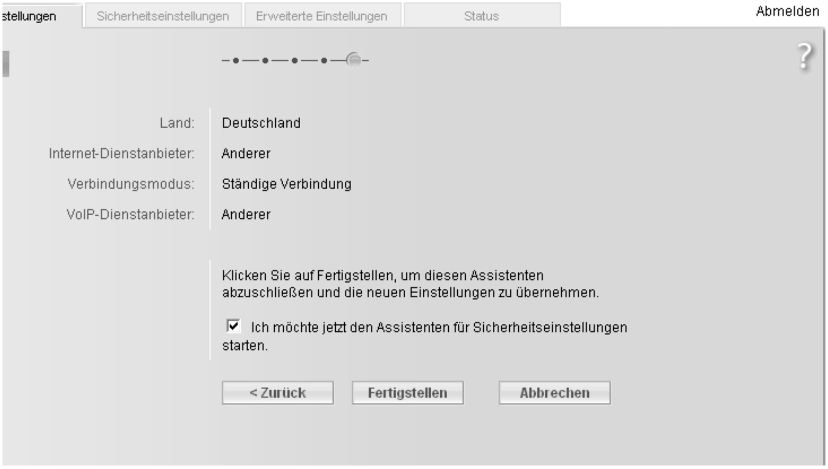
→ Leave the default settings for the parameters ***SIP listen port***, ***Proxy server port***, ***Registrar server port***, ***Voice codecs*** und ***Out-of-band DTMF***, unless your service provider has provided you with other data.

→ If you wish to delete the entered data, click the ***Clear*** button.

→ Confirm your selection with ***Next >***.

Summary

The basic settings you have made through the wizard are shown in the next step for you to check.



Land: Deutschland

Internet-Dienstanbieter: Anderer

Verbindungsmodus: Ständige Verbindung

VoIP-Dienstanbieter: Anderer

Klicken Sie auf Fertigstellen, um diesen Assistenten abzuschließen und die neuen Einstellungen zu übernehmen.

☑ Ich möchte jetzt den Assistenten für Sicherheitseinstellungen starten.

→ If you want to change the settings, click ***< Back***.

→ If you want to confirm the settings, click ***Finish*** to close the Basic Setup Wizard.

The Gigaset SX763 WLAN dsl is now configured and ready to connect to the Internet. The ***Security Setup Wizard*** then opens automatically. We strongly recommend using the Security Setup Wizard to protect your Gigaset SX763 WLAN dsl against attacks. If you want to carry this out at a later stage, deactivate ***I would like to run the Security Setup Wizard now.***

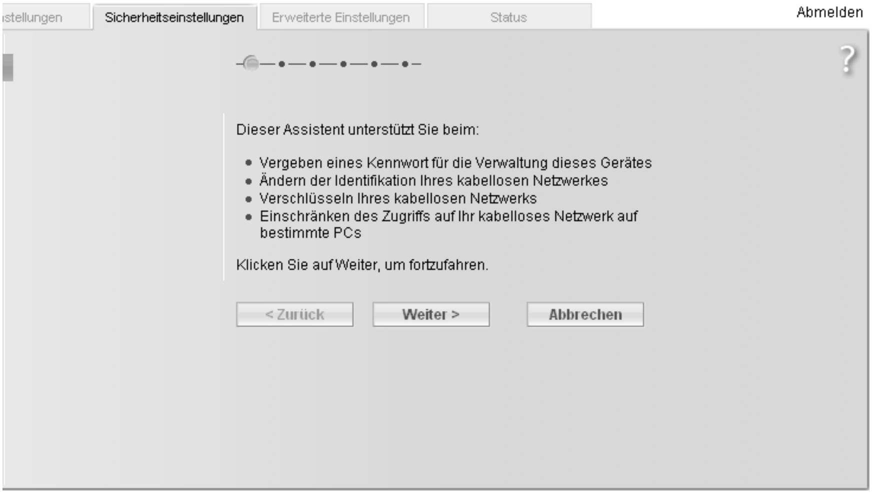
Security Setup Wizard

The ***Security Setup Wizard*** offers you additional settings for improving your network security. You can:

- assign a password for configuring the Gigaset SX763 WLAN dsl (page 43),
- change the SSID for your wireless network (page 44),
- set up the Encryption for the wireless network (page 44),
- limit access to the wireless network to certain PCs (page 49).

The user interface of the Gigaset SX763 WLAN dsl guides you step by step through the security configuration. Once you have completed a screen, click ***Next >***. If you want to make any changes or check your entries, click ***< Back***.

→ Select the ***Security Setup Wizard*** option on the start screen or on the tab to start the security configuration if you did not make the security settings immediately after setting up the basic settings.



Dieser Assistent unterstützt Sie beim:

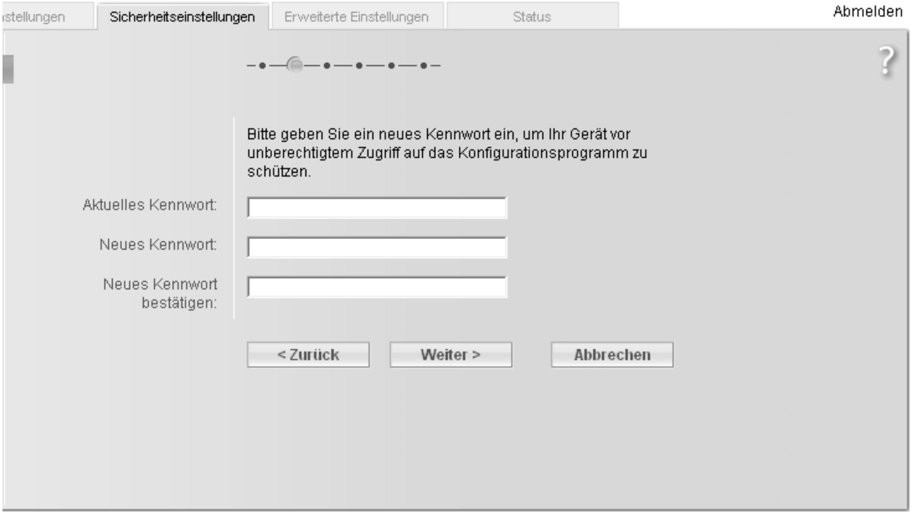
- Vergeben eines Kennwort für die Verwaltung dieses Gerätes
- Ändern der Identifikation Ihres kabellosen Netzwerkes
- Verschlüsseln Ihres kabellosen Netzwerks
- Einschränken des Zugriffs auf Ihr kabelloses Netzwerk auf bestimmte PCs

Klicken Sie auf Weiter, um fortzufahren.

→ Click ***Next >***.

Assigning a password

In the first step of the configuration you can change the password for the user interface. When the device is supplied, the configuration of your Gigaset SX763 WLAN dsl is protected with the ***admin*** password. To prevent unauthorised changes to the configuration, you should change the password at regular intervals.



Bitte geben Sie ein neues Kennwort ein, um Ihr Gerät vor unberechtigtem Zugriff auf das Konfigurationsprogramm zu schützen.

Aktuelles Kennwort:

Neues Kennwort:

Neues Kennwort bestätigen:

➞ Enter the old password in the ***Current password*** field.

➞ Enter the new password in the ***New password*** field and repeat the entry in the ***Confirm new password*** field.

The password can be up to 20 alphanumeric characters long. Avoid using proper names and obvious terms. Combine letters and numbers.

Note:

If you ever forget your password you will have to return the Gigaset SX763 WLAN dsl to its factory settings (page 108). Please bear in mind that this will restore **all** settings to the factory configuration. The password will again be ***admin***.

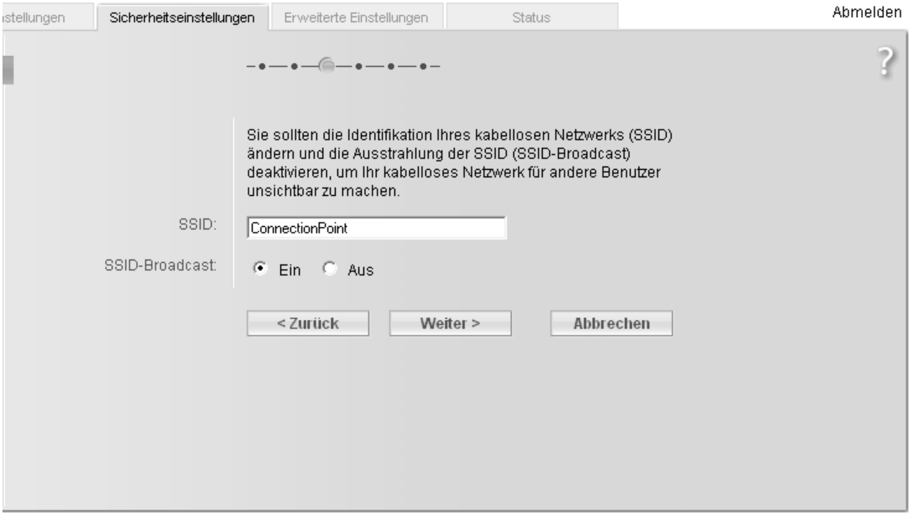
◆ To go to the next step, click ***Next >***.

SSID

For the wireless network components to be able to communicate with one another, you must use the same SSID (Service Set Identifier).

The default SSID for the Gigaset SX763 WLAN dsl is **ConnectionPoint**. For security reasons you should change this SSID and deactivate SSID broadcast.

If this option is enabled, the Gigaset SX763 WLAN dsl will send the SSID in all data transfers and the SSID of the Gigaset SX763 WLAN dsl will be displayed on PCs that have a wireless network adapter. In this case, unauthorised persons could use the SSID to gain access to your network.



Sie sollten die Identifikation Ihres kabellosen Netzwerks (SSID) ändern und die Ausstrahlung der SSID (SSID-Broadcast) deaktivieren, um Ihr kabelloses Netzwerk für andere Benutzer unsichtbar zu machen.

SSID: ConnectionPoint

SSID-Broadcast: ● Ein ○ Aus

➙ Enter a character string of your choice in the ***SSID*** field. The SSID is case sensitive. It can contain up to 32 alphanumeric characters.

> **Note:**
> The connection to the wireless network adapters will be interrupted until the new SSID has also been entered.

➙ Deactivate ***SSID broadcast*** and make a note of the SSID. You will need this to connect your PC with the Gigaset SX763 WLAN dsl at a later time.

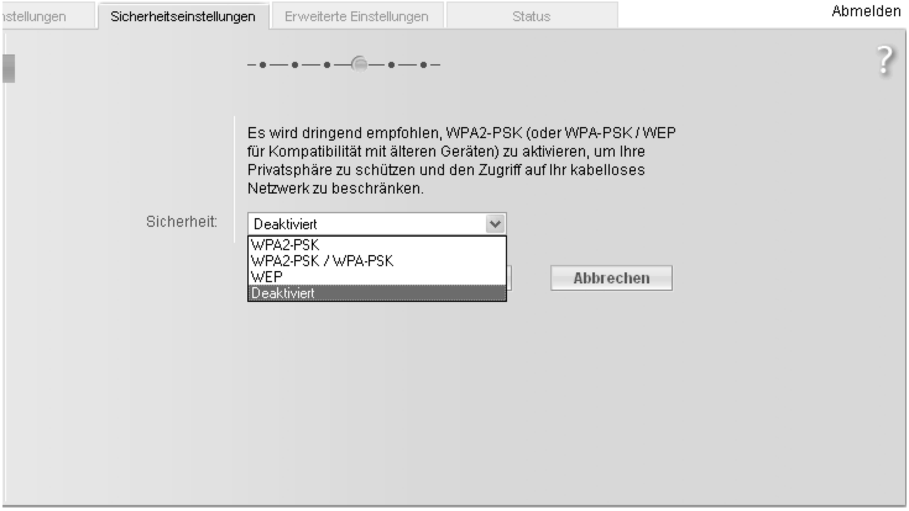
➙ Click ***Next >***.

Setting up security functions for the wireless network

In the next step you can set up the encryption and authentication methods for your wireless network.

Wireless networks are even more susceptible to eavesdropping than wired networks. With conventional network adapters, an intruder only needs a device with a WLAN adapter (e.g. a notebook or a PDA [Personal Digital Assistant]) with an appropriately configured network card in order to eavesdrop on every communication made via a nearby wireless LAN.

The Gigaset SX763 WLAN dsl makes use of effective encryption methods to prevent unauthorised eavesdropping as far as possible.



Es wird dringend empfohlen, WPA2-PSK (oder WPA-PSK / WEP für Kompatibilität mit älteren Geräten) zu aktivieren, um Ihre Privatsphäre zu schützen und den Zugriff auf Ihr kabelloses Netzwerk zu beschränken.

Sicherheit: Deaktiviert

WPA2-PSK
WPA2-PSK / WPA-PSK
WEP
Deaktiviert

You can use the following security mechanisms:

- WPA2-PSK or WPA2-PSK/WPA-PSK (page 46)
- WEP encryption (Wired Equivalent Privacy, see page 47)

We recommend that you use WPA2-PSK if it is supported by all components in your wireless network.

You will find further options for setting up data encryption and authentication in the Advanced Settings menu (page 80).

WPA2/WPA with pre-shared key (PSK)

WPA is a more advanced procedure than WEP for protecting wireless networks. Dynamic keys, based on TKIP (Temporal Key Integration Protocol) offer increased security. The new standard WPA2 uses AES (Advanced Encryption Standard) for encryption.

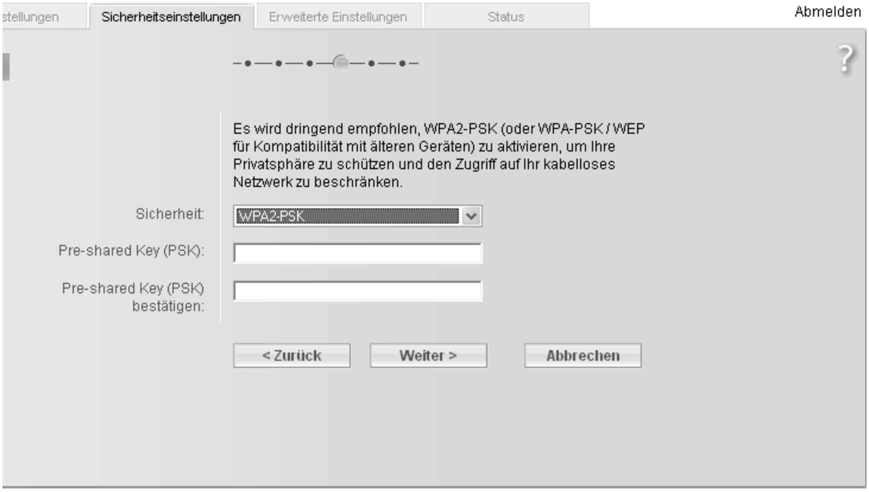
WPA-PSK is a special WPA mode for private users and users in small companies without their own authentication server. After a certain period of time (Rekey interval), encryption keys are automatically generated with the Pre-shared key, automatically changed ("rekeying") and authenticated between the devices.

Note:
Every PC (network adapter) that requires access to a WPA-protected wireless network must also support WPA. To find out whether and how you can use WPA on your PC, read your network adapter's user guide.

→ Select ***WPA2-PSK*** if it is supported by all components in your wireless network.

Or:

→ Select ***WPA2-PSK / WPA-PSK*** if some or all components in your wireless network support WPA with the TKIP protocol.



Es wird dringend empfohlen, WPA2-PSK (oder WPA-PSK / WEP für Kompatibilität mit älteren Geräten) zu aktivieren, um Ihre Privatsphäre zu schützen und den Zugriff auf Ihr kabelloses Netzwerk zu beschränken.

Sicherheit: WPA2-PSK

Pre-shared Key (PSK):

Pre-shared Key (PSK) bestätigen:

→ Enter a key of your choice in the ***Pre-shared key*** field (min. 8 to max. 63 characters) and confirm it by repeating the entry. You must set up the same pre-shared key for all wirelessly connected PCs.

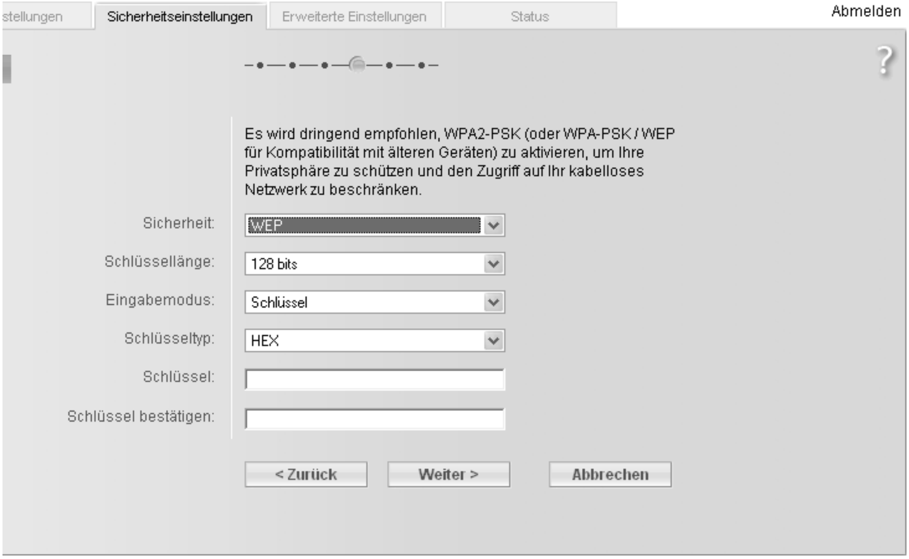
→ To go to the next step, click ***Next >***.

WEP encryption

WEP (Wired Equivalent Privacy) is an encryption for radio signals in wireless networks and meets the IEEE 802.11 standard.

If you transmit data wirelessly and not all components in your wireless network support the higher security standard WPA (page 46), we recommend that you activate WEP encryption.

You can choose either the standard 64-bit default key or the more robust 128-bit key. The keys are generated in hexadecimal or in ASCII format. You must use the same keys for encryption and decryption for the Gigaset SX763 WLAN dsl and all your wireless network adapters.



Es wird dringend empfohlen, WPA2-PSK (oder WPA-PSK / WEP für Kompatibilität mit älteren Geräten) zu aktivieren, um Ihre Privatsphäre zu schützen und den Zugriff auf Ihr kabelloses Netzwerk zu beschränken.

Sicherheit:	WEP
Schlüssellänge:	128 bits
Eingabemodus:	Schlüssel
Schlüsseltyp:	HEX
Schlüssel:	
Schlüssel bestätigen:	

→ Select the ***Key length***: 64 bits or 128 bits.

→ Select the ***Input type***, i.e. whether the key is to be entered manually or generated automatically by means of a ***Passphrase***.

Manual key entry

→ Select the ***Key type***, ***Hex*** or ***ASCII***.

If you select ***Hex*** as the key type you can use the characters **0** to **9** and **A** to **F**.

– With a 64-bit encryption depth, the key is 10 characters long.

– With a 128-bit encryption depth, the key is 26 characters long.

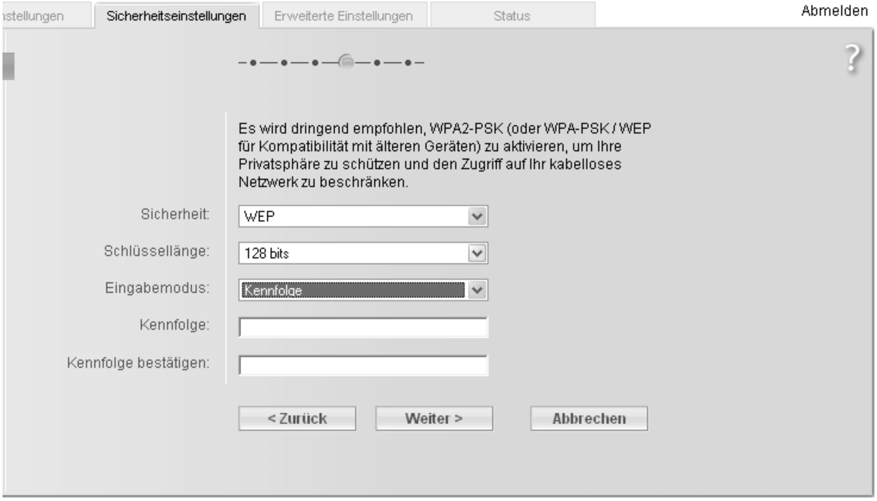
If you select ***ASCII*** as the key type, you can use the characters **0** to **9**, **A** to **Z**, and **a** to **z** plus the special characters in the ASCII character set.

– With a 64-bit encryption depth, the key is 5 characters long.

– With a 128-bit encryption depth, the key is 13 characters long.

→ Confirm the key by entering it again in the ***Confirm key*** field.

Generating a key by means of a Passphrase



Es wird dringend empfohlen, WPA2-PSK (oder WPA-PSK / WEP für Kompatibilität mit älteren Geräten) zu aktivieren, um Ihre Privatsphäre zu schützen und den Zugriff auf Ihr kabelloses Netzwerk zu beschränken.

Sicherheit: WEP

Schlüssellänge: 128 bits

Eingabemodus: Kennfolge

Kennfolge:

Kennfolge bestätigen:

→ Enter a ***Passphrase*** (up to 32 characters) and confirm it by entering it again. The key is generated automatically.

Note:

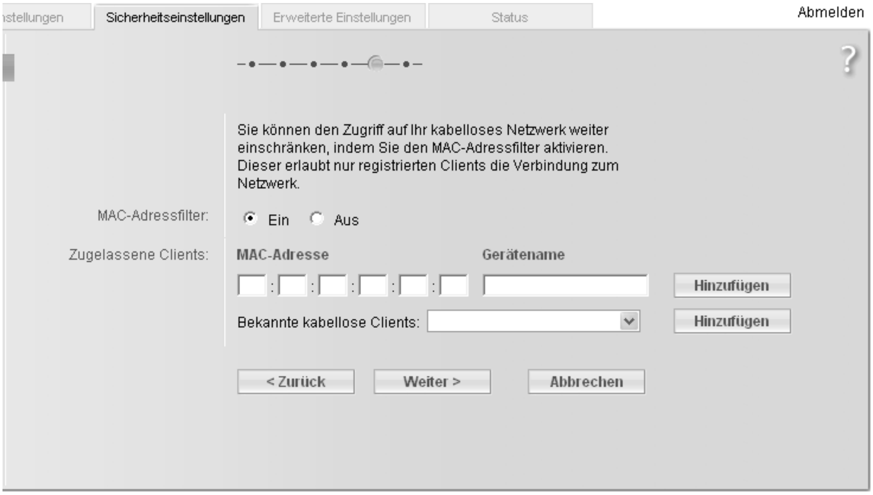
◆ It is very **important** that you make a note of the key or passphrase. You will need this information to configure the wireless network adapters properly.

◆ When you have concluded the Security Setup Wizard, you must change the WEP encryption in the wireless network adapters for the connected PCs in the same way, otherwise they will not be given access to the Gigaset SX763 WLAN dsl wireless network.

→ To go to the next step in the Security Setup Wizard, click ***Next >***.

Access control within the wireless network

In this step you can specify which PCs will have wireless access to the Gigaset SX763 WLAN dsl and hence to the LAN. The access control is based on the MAC address of the PC network adapters. You can enter the MAC addresses for the PCs manually or select these from the list of PCs that are currently logged in.



Sie können den Zugriff auf Ihr kabelloses Netzwerk weiter einschränken, indem Sie den MAC-Adressfilter aktivieren. Dieser erlaubt nur registrierten Clients die Verbindung zum Netzwerk.

MAC-Adressfilter: ● Ein ○ Aus

Zugelassene Clients: MAC-Adresse Gerätename

Bekannte kabellose Clients:

Access control is disabled by default. This means that all PCs that use the correct SSID can be logged in.

➙ Next to the ***MAC address filter*** select ***On*** to activate the MAC filter.

Entering MAC addresses manually

➡ Enter the MAC address of the network adapter. You will find this address on the underside of the device.

➡ Enter the name of the PC.

➡ Click the ***Add*** button to add the entry to the list.

Selecting from the list of logged-in PCs

➡ Select the required PC from the ***Known wireless clients*** list. All PCs that were already entered manually on the router with the MAC address are displayed.

➡ Click the ***Add*** button to add the selected PC to the list.

Note:

If you activate MAC access control, you must at least add the PC, on which you are configuring the Gigaset SX763 WLAN dsl, to the list. Otherwise, you will have no access to the user interface and will receive a corresponding error message.

If you have inadvertently denied all PCs access to the Gigaset SX763 WLAN dsl, you have two options:

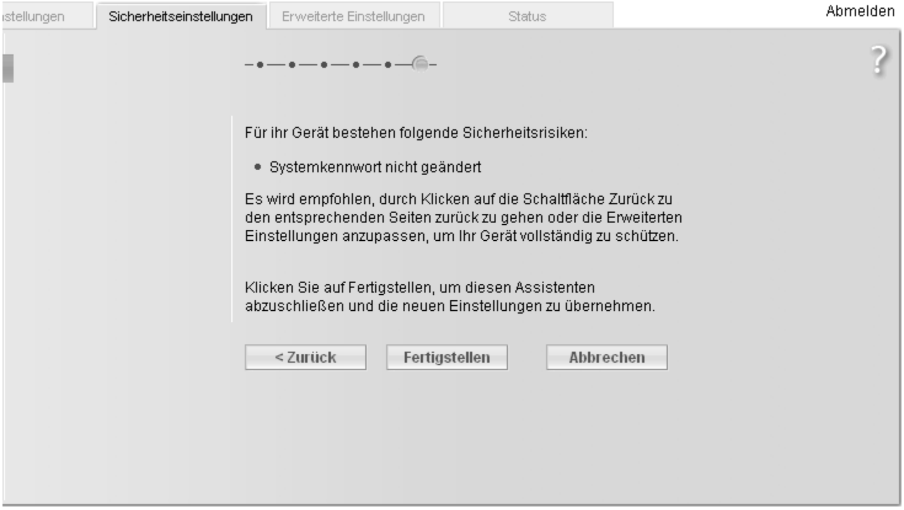
◆ You can completely reset the Gigaset SX763 WLAN dsl (page 20).

◆ You can connect a PC to the Gigaset SX763 WLAN dsl using one of the LAN connections (by cable). As MAC access control only affects PCs that are connected wirelessly, you can use this PC to change the configuration.

➡ To go to the next step, click ***Next >***.

Saving settings

On the next screen you end the wizard and save the settings. You will be informed of any security risks that still exist.



Für ihr Gerät bestehen folgende Sicherheitsrisiken:

- Systemkennwort nicht geändert

Es wird empfohlen, durch Klicken auf die Schaltfläche Zurück zu den entsprechenden Seiten zurück zu gehen oder die Erweiterten Einstellungen anzupassen, um Ihr Gerät vollständig zu schützen.

Klicken Sie auf Fertigstellen, um diesen Assistenten abzuschließen und die neuen Einstellungen zu übernehmen.

→ Click ***Finish*** to end the wizard.

The settings will now be activated on the Gigaset SX763 WLAN dsl.

Note:

You must now configure the WEP or WPA key for the wireless network adapter of the PC that has been configured with other values. After this you can again wirelessly log on to the Gigaset SX763 WLAN dsl.

Configuring Advanced Settings

In the ***Advanced Settings*** menu, you can configure all the options for the Gigaset SX763 WLAN dsl. If required, you can also change the settings you made using the wizard. The following table contains the options available in this menu.

Menu	Description
Internet	This menu comprises all the setting options relating to the Internet. In particular, you can do the following: ◆ Check and change the configuration for Internet access (page 56) or specify a preferred DNS server (page 60), ◆ Configure the firewall, i.e. a number of security and special functions, for example access control from local PCs to the Internet (page 62), ◆ Make the NAT settings required to provide your own services on the Internet (page 66), ◆ Set up dynamic DNS for a static Internet address on the device (page 72), ◆ Set up routing for your Internet connection services (page 71), ◆ Configure the Quality of Service (QoS) (page 73).
Local Network	You can change the Private IP address of the Gigaset SX763 WLAN dsl here and make settings on the DHCP server (page 75).
Wireless Network	You can configure the options for wireless communication (SSID and encryption) here and restrict access to the Gigaset SX763 WLAN dsl (page 77).
Telephony	Here you can make the settings for Internet telephony (VoIP) and configure your extensions ((page 87)).
USB	You can make the settings here for operating an external data carrier, a file server or a print server on the USB port (page 95).
Administration	You can make or change various system settings here, for example assign a password (page 105)or set the time (page 104). In addition, you can also back up the data on the Gigaset SX763 WLAN dsl or load new firmware (page 107).

Internet

If you have configured the Gigaset SX763 WLAN dsl using the two wizards, you have also configured the WAN connection (Internet access). You can check or change these settings in the ***Internet*** menu.

This menu also offers you a wide range of possibilities for setting up security settings and limiting access to the Internet as well as for providing your own services on the Internet.

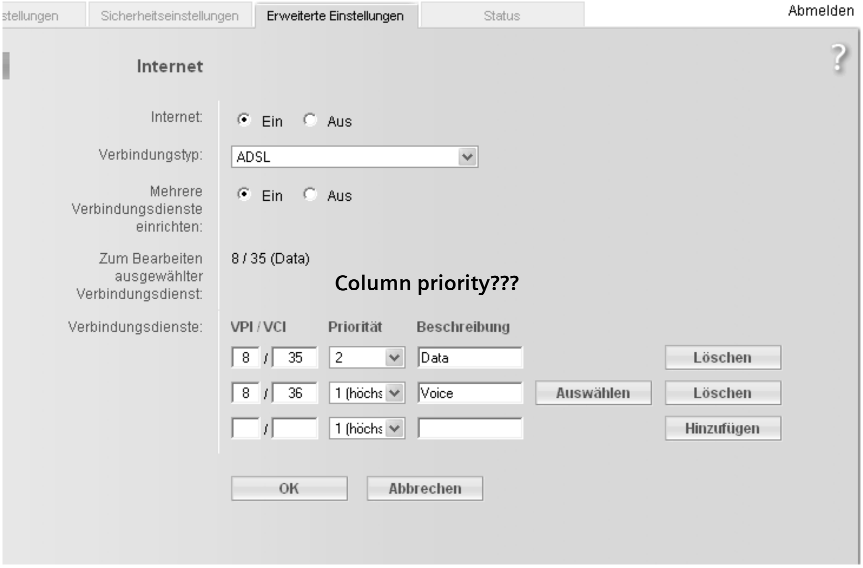
You can carry out the following via the ***Internet*** menu:

- Activate/deactivate the Internet connection and edit the virtual connection parameters (for further information see below),
- check and edit the Internet connection of the Gigaset SX763 WLAN dsl (for further information see below),
- enter the PC's registered MAC address for Internet access (WAN interface, see page 61),
- Make DNS server settings (page 60),
- protect the network against unauthorised external access (firewall),
- provide your own services on the Internet (NAT, see page 66),
- Set up dynamic DNS (page 72),
- set up routing for your Internet connection services (page 71),
- define QoS properties (properties for data transfer, see page 73).

Internet selection

You can activate or deactivate the Internet connection for the Gigaset SX763 WLAN dsl on this screen. You can choose the connection type and set up and edit a number of connection services.

→ Select ***Internet*** from the ***Advanced Settings*** menu.



Internet

Internet: ● Ein ○ Aus

Verbindungstyp: ADSL

Mehrere Verbindungsdienste einrichten: ● Ein ○ Aus

Zum Bearbeiten ausgewählter Verbindungsdienst: 8 / 35 (Data)

Column priority???

Verbindungsdienste:

VPI / VCI	Priorität	Beschreibung		
8 / 35	2	Data		Löschen
8 / 36	1 (höchs	Voice	Auswählen	Löschen
/	1 (höchs			Hinzufügen

→ Select the appropriate option to activate or deactivate the Internet function of the Gigaset SX763 WLAN dsl.

→ Choose the desired ***Connection type*** for your Internet connection:

– Choose the ***ADSL*** if you are using the integrated ADSL modem of the Gigaset SX763 WLAN dsl.

– Choose ***Ethernet*** is you are setting up the connection to the Internet via an Ethernet network connection (e.g. if you are using an external modem with an Ethernet connection).

Configure multiple connection services

Your Internet service provider can permit you to set up a number of ***Connection services***. You can set up these services here. You can configure rules for using these services under the ***Routing*** option (page 71).

→ Select the appropriate option to activate or deactivate ***Configure multiple connection services***.

If you have already configured an Internet connection (e.g. in the Basic Setup Wizard), this is shown as ***Connection service selected to edit***. This is then also displayed on other pages of the ***Internet*** menu.

➥ Enter the values for ***VPI / VCI*** for each connection service that you have received from your Internet service provider. This input option is only available if you are using the integrated ADSL modem for the connection to the Internet.

➥ Choose the desired ***Priority*** for each connection service in comparison with the other connection services.

You can choose between 1 and 6 for the ***Priority***, whereby 1 is the highest priority.

➥ Enter a description to identify the respective connection service.

➥ Click ***Select*** to select an existing connection service to edit. You can then make all other settings in the Internet area for this connection service.

➥ Click ***Add*** to create a new entry.

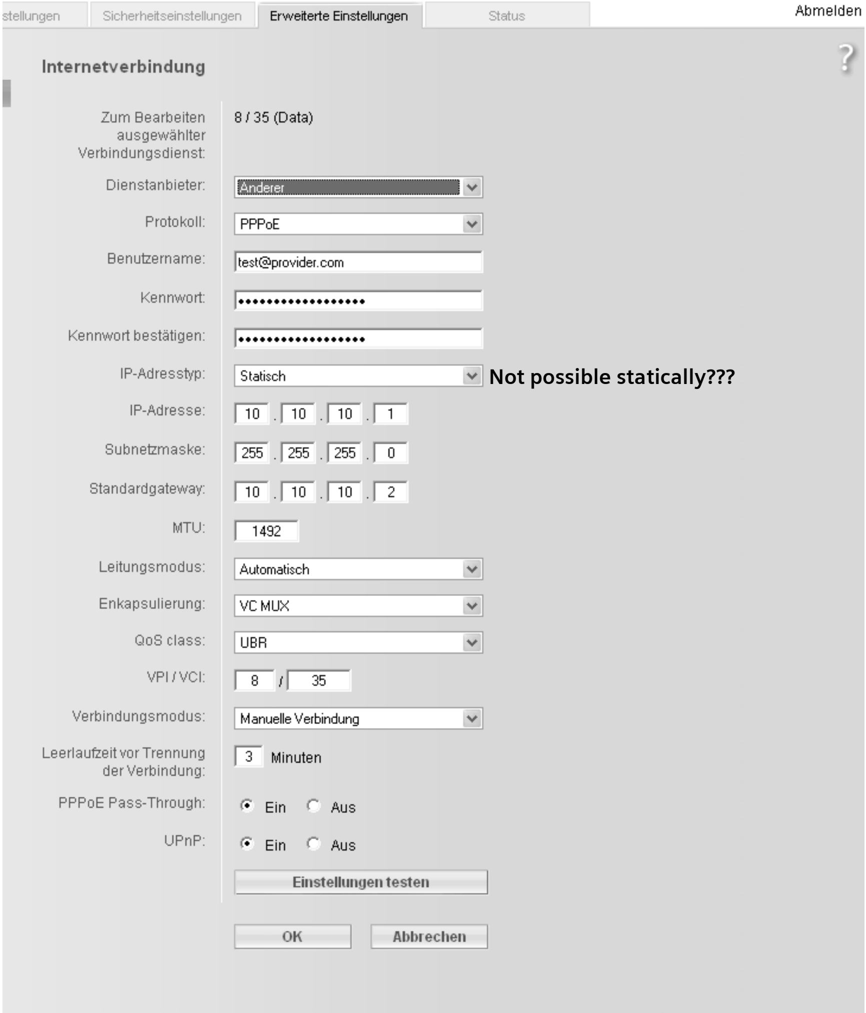
➥ Click ***Delete*** to delete an entry.

➥ Click ***OK*** to save and apply the changes.

Internet Connection

You can set up or change the configuration of your Internet connection on this screen. All the settings you make here must coincide with the features your Internet provider makes available to you. False information can lead to problems with your Internet connection.

→ If you want to set up or change the settings for the Internet connection, select ***Internet Connection*** from the ***Advanced Settings*** – ***Internet*** menu.



Internetverbindung

Zum Bearbeiten ausgewählter Verbindungsdienst:	8 / 35 (Data)
Dienstanbieter:	Anderer
Protokoll:	PPPoE
Benutzername:	test@provider.com
Kennwort:	••••••••••••••••••
Kennwort bestätigen:	••••••••••••••••••
IP-Adresstyp:	Statisch
IP-Adresse:	10 . 10 . 10 . 1
Subnetzmaske:	255 . 255 . 255 . 0
Standardgateway:	10 . 10 . 10 . 2
MTU:	1492
Leitungsmodus:	Automatisch
Enkapsulierung:	VC MUX
QoS class:	UBR
VPI / VCI:	8 / 35
Verbindungsmodus:	Manuelle Verbindung
Leerlaufzeit vor Trennung der Verbindung:	3 Minuten
PPPoE Pass-Through:	● Ein ○ Aus
UPnP:	● Ein ○ Aus

Not possible statically???

All settings apply for the displayed connection service that you selected for editing on the ***Advanced Settings*** – ***Internet*** (page 54) screen.

→ Select your ***Service provider***. Depending on the country you selected when making the basic settings (page 36), the selection menu contains various possible providers. If your provider is not listed, please use the ***Other*** option.

→ Enter the data you have been given by your service provider: ***Protocol***, ***User name*** and ***Password***.

Apply the default settings for the parameters ***IP address type***, ***IP address***, ***Subnet mask***, default gateway, ***MTU***, ***Line mode***, ***Encapsulation***, ***QoS class*** and ***VPI / VCI***, unless your service provider has provided you with other data. The default settings also depend on your choice of country.

Note:

To configure the Internet connection successfully, you must enter the details given by your provider in all fields.

→ If you have connected an external modem and chosen the connection type ***Ethernet***, enter the values for VLAN tag for each connection type that you have received from your Internet service provider.

The fields line mode, encapsulation, QoS class and VPI/VCI are then deactivated.

→ Specify how Internet sessions are to be established via ***Connection mode***:

– Select ***Always on*** if the connection is to exist at all times when the Gigaset SX763 WLAN dsl is turned on.

Notes:

◆ You must set up the ***Always on*** option if you wish to use Internet telephony. Otherwise you can only use fixed network telephony via the Gigaset SX763 WLAN dsl.

◆ If you are on a time-based tariff, this option can result in high connection charges.

– Select ***Connect on demand*** if applications such as an Internet browser or an e-mail program are to connect to the Internet automatically.

– In the ***Idle time before disconnect*** field, enter a period after which the Internet connection is to end automatically if no data is transmitted (the default setting is 3 minutes).

  This time setting only applies to the ***Connect on demand*** option.

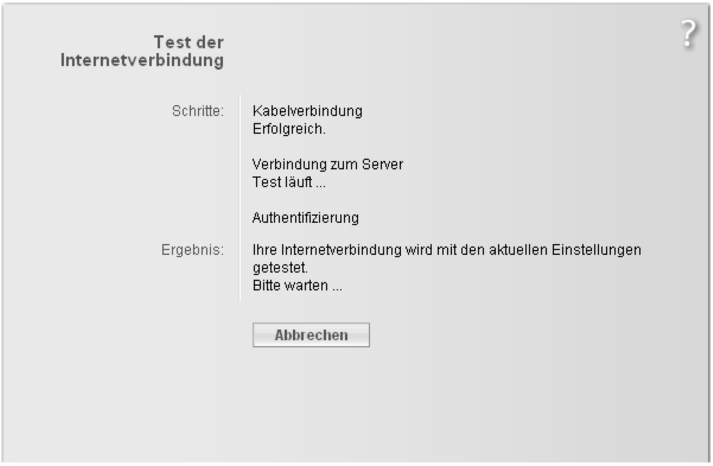
– Select ***Connect manually*** if you always want to establish and end the Internet connection manually. If you are on a time-based tariff this will save you high connection charges.

Note:

If you select ***Connect on demand*** or ***Connect manually*** you can establish or end the Internet connection manually on the start screen for the configuration program (page 33).

→ Click ***Test Settings*** to check the settings.

An attempt is made to set up an Internet connection. The result is shown in a separate window.



Test der Internetverbindung

Schritte: Kabelverbindung
Erfolgreich.

Verbindung zum Server
Test läuft ...

Authentifizierung

Ergebnis: Ihre Internetverbindung wird mit den aktuellen Einstellungen getestet.
Bitte warten ...

→ Click the ***Close*** button, which is shown if the test was successful.

→ Click ***OK*** to apply the settings.

PPPoE pass-through

If you activate the ***PPPoE pass-through*** function, a PC in the network can connect to the Internet via its own connection ID. The router puts this connection through.

→ In the ***Advanced Settings – Internet*** menu, select ***Internet Connection***.

→ Select ***On*** to activate ***PPPoE pass-through***.

→ Click ***OK*** to apply the settings.

Using UPnP (Universal Plug and Play)

PCs with UPnP (Universal Plug & Play) can offer their own network services and automatically use services offered in the network.

Note:

The PC must have Windows ME or Windows XP as its operating system. Check whether the UPnP function has been installed in the PC's operating system. It may be necessary to retrospectively install the UPnP components, even on systems with Windows XP or Windows ME. Please consult your PC's user guide.

As soon as you have installed UPnP in the operating system of a PC and activated it on the router, applications on this PC (e.g. Microsoft Messenger) can communicate via the Internet without you needing to expressly authorise it. In this case, the router automatically implements port forwarding (Port forwarding, see page 68), thereby facilitating communication via the Internet.

The task bar on the PC on which UPnP is installed contains an icon for the Gigaset SX763 WLAN dsl. In systems with Windows XP, the icon is also shown under network connections. Click this icon to open the user interface of the Gigaset SX763 WLAN dsl.

➙ In the ***Advanced Settings*** – ***Internet*** menu, select ***Internet Connection***.

➙ Click ***UPnP***.

> **Note:**
> When the UPnP function is active, system applications can assign and use Ports on a PC. This poses a security risk.

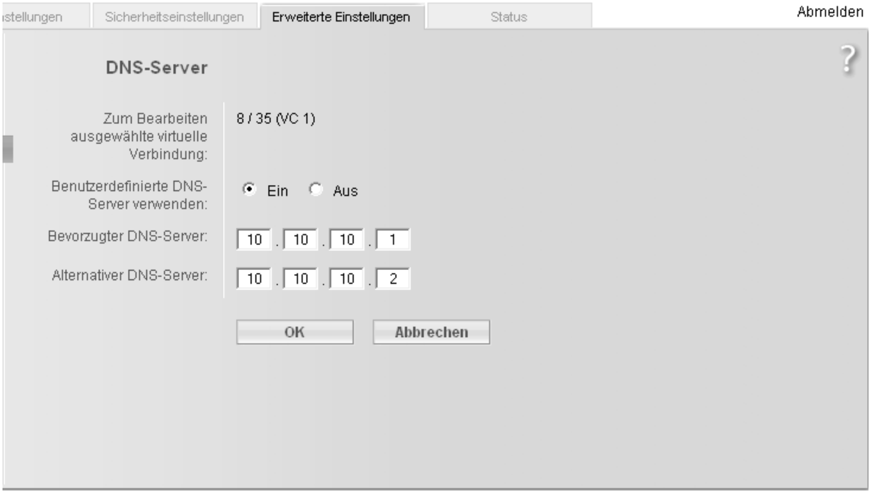
➙ Click ***OK*** to apply the settings.

DNS server

DNS is a decentralised service that assigns PC names or Internet addresses (Domain names) and IP addresses to one another. A DNS server has to administer this information for each server or each LAN with an Internet connection.

Your Internet provider will usually provide you with a DNS server that makes this assignment when an Internet connection is set up. If necessary, you can define the DNS server such that it is used manually for the Internet connections.

→ In the ***Advanced Settings*** – ***Internet*** – ***Internet Connection*** menu, select ***DNS Servers***.



DNS-Server

Zum Bearbeiten ausgewählte virtuelle Verbindung: 8 / 35 (VC 1)

Benutzerdefinierte DNS-Server verwenden: ● Ein ○ Aus

Bevorzugter DNS-Server: 10 . 10 . 10 . 1

Alternativer DNS-Server: 10 . 10 . 10 . 2

All settings apply for the displayed connection service that you selected for editing on the ***Advanced Settings*** – ***Internet*** (page 54) screen.

→ Activate the ***Use custom DNS servers*** function by selecting ***On***.

→ Enter the IP addresses for your preferred DNS servers (***Preferred DNS server*** and ***Alternate DNS server***).

→ Click ***OK*** to apply the settings.

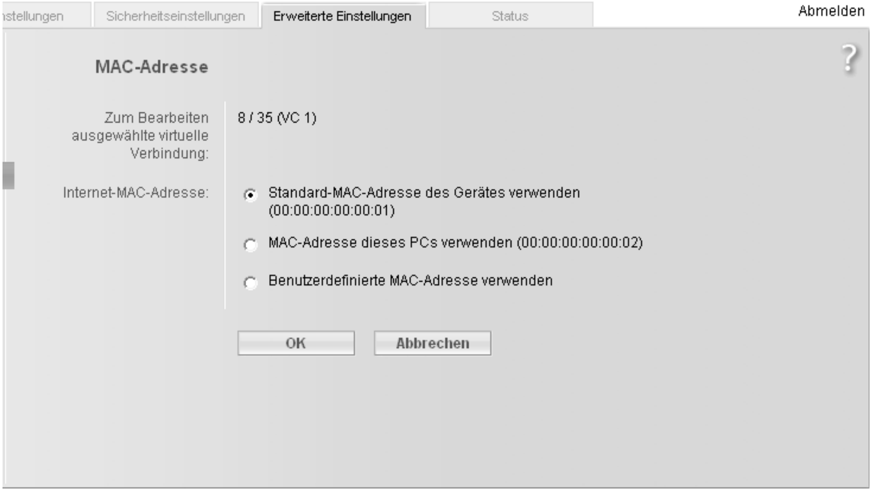
MAC Address

If you already had Internet access through the same Internet provider before connecting the Gigaset SX763 WLAN dsl, it is possible that the MAC address of one of your PCs was used for registration when the connection was being set up. In this case, you must either replace the current MAC address with the MAC address registered with the Internet provider or ask your Internet provider to register a MAC address for you.

Carry out the following steps:

➡ Connect a PC to the Gigaset SX763 WLAN dsl and open the configuration environment.

➡ In the ***Advanced Settings*** – ***Internet*** – ***Internet Connection*** menu, select ***MAC Address***.



MAC-Adresse

Zum Bearbeiten ausgewählte virtuelle Verbindung: 8 / 35 (VC 1)

Internet-MAC-Adresse:
- ● Standard-MAC-Adresse des Gerätes verwenden (00:00:00:00:00:01)
- ○ MAC-Adresse dieses PCs verwenden (00:00:00:00:00:02)
- ○ Benutzerdefinierte MAC-Adresse verwenden

All settings apply for the displayed connection service that you selected for editing on the ***Advanced Settings*** – ***Internet*** (page 54) screen.

➡ Specify which MAC address is to be used for the Internet connection:

– ***Use default device MAC address***: You can leave this default setting if the MAC address of the Gigaset SX763 WLAN dsl is used for connecting to the Internet.

– ***Use MAC address of this PC***: Select this option if the MAC address of the currently connected PC has previously been registered for connecting to the Internet or if you have re-registered the MAC address of the PC on which you are currently working.

– ***Use custom MAC address***: Select this option if you have asked your Internet provider to register a new MAC address and this is not the MAC address of the PC on which you are currently carrying out the configuration.

➡ Click ***OK*** to apply the settings.

Firewall

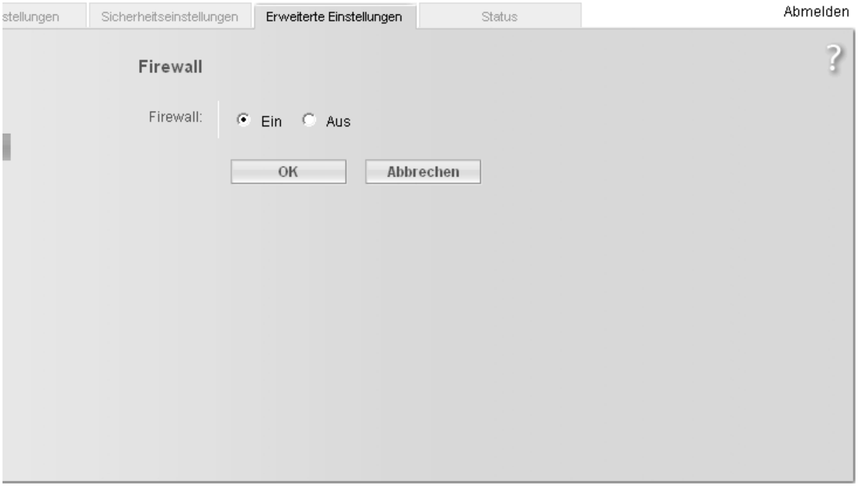
The firewall functions of the Gigaset SX763 WLAN dsl include various security functions for the local network.

You can carry out the following:

- Protect the network against hacker attacks (for information see below),
- Block access by individual PCs to selected services (page 64).

The firewall functions for the Gigaset SX763 WLAN dsl are activated and configured in the factory. If you want to deactivate the firewall, carry out the following steps:

→ In the ***Advanced Settings*** – ***Internet*** menu, select ***Firewall***.



Firewall

Firewall: ● Ein ○ Aus

→ Click the required option.

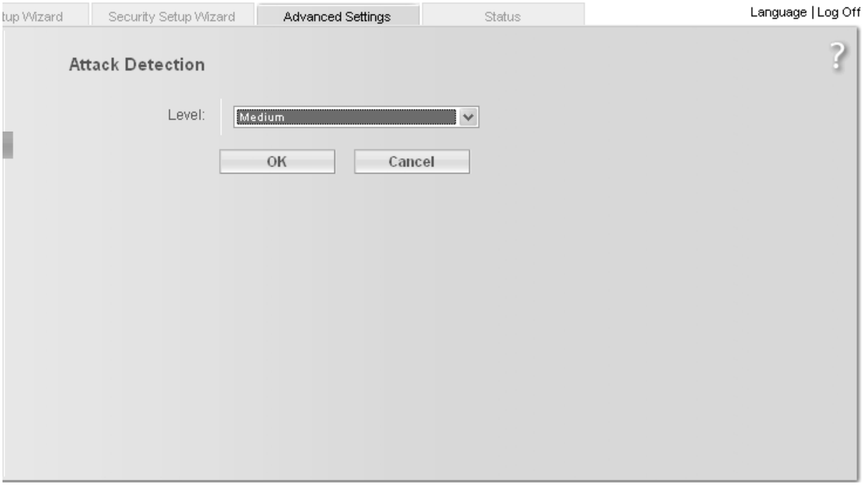
→ Click ***OK*** to apply the settings.

Attack Detection

If the firewall functions of the Gigaset SX763 WLAN dsl are activated, the device monitors and limits access to incoming data traffic via the DSL connection with a function called "Stateful Packet Inspection" (SPI). This allows the Gigaset SX763 WLAN dsl to detect and prevent certain types of attack from the Internet, such as Denial-of-Service (DoS). DoS attacks are aimed at devices and networks with Internet connections. The aim is not so much to steal data as to paralyse the computer or network to such an extent that the network resources are no longer available. A typical hacker attack involves, for example, a remote computer acting in place of the paralysed device and receiving the data intended for the device.

You can use the Attack Detection function to modify default settings of the firewall.

➡ In the ***Advanced Settings*** – ***Internet*** – ***Firewall*** menu, select ***Attack Detection***.



Attack Detection

Level: Medium

➙ Select the security level for the firewall:

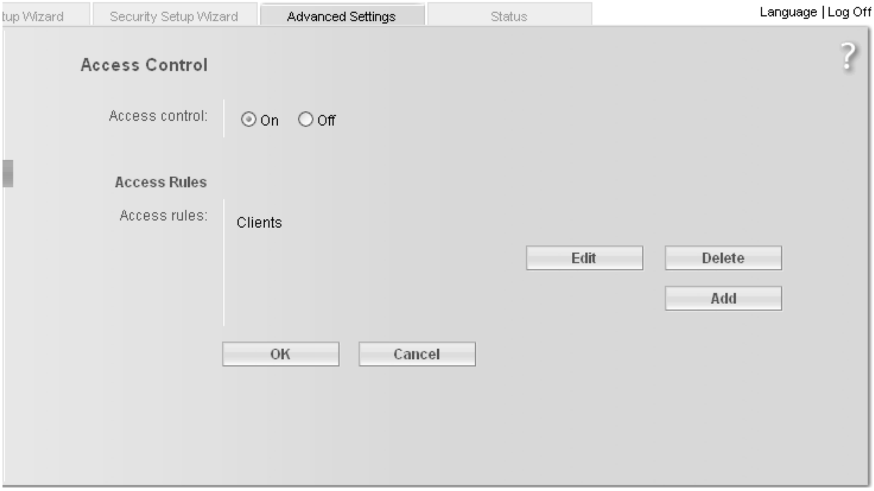
- The ***Medium*** default level offers high security and hardly limits functionality of certain applications.
- The ***High*** level offers maximum security and may limit functionality for certain applications.
- The ***Low*** level offers maximum functionality but may provide low security.

Setting up access control to the Internet

The ***Access Control*** function allows you to block access to various services for one or more PCs. You can permit or block access to services at certain times.

➙ In the ***Advanced Settings*** – ***Internet*** – ***Firewall*** menu, select ***Access Control***.

➙ Activate the ***Access Control*** function by selecting ***On***.



Access Control

Access control: ● On ○ Off

Access Rules

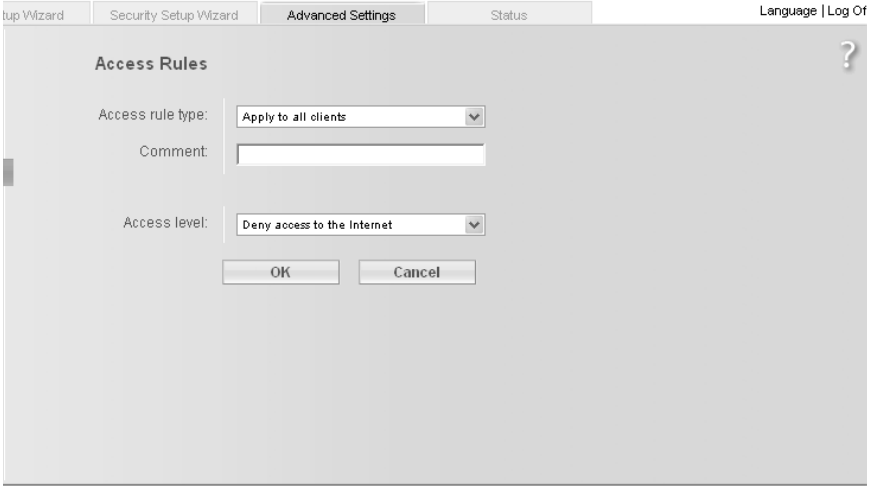
Access rules: Clients

You have the following setting options for ***Access Control***:

Access Rules

You can limit access to the Internet for all or only for certain clients in the network.

➙ Click ***Add*** to create an access rule.



Access Rules

Access rule type: Apply to all clients

Comment:

Access level: Deny access to the Internet

➙ Select the ***Access rule type*** from the list:

- ***Apply to all clients***: The rule applies to all PCs in the network.
- ***Specify IP address range***: You select the PCs to which the rule is to be applied by entering an IP address block.
- ***Specify IP address*** or ***Specify MAC address***: The rule applies to a PC you have selected via the IP address or MAC address.

➙ Enter a name for the ***Comment*** for the access rule.

➙ Define the ***Access level***.
You can choose ***Deny access to the Internet***, ***Allow web browsing***. If you select ***Custom***, you can make the following settings:

➙ If you wish to create a ***Service filter***, choose one of the following options.

- In ***Filtering mode***, specify whether the selected services are to be allowed or blocked.
- Select the ***Services*** that are to be allowed or blocked.

  Select the ***Protocol*** and enter the appropriate ***Port*** (a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example `80.90-140.180`). The ***Description*** that is displayed helps you to identify different services.
- Activate the ***Filter*** option to use the relevant service for the service filter.
- You can also select services from the ***Predefined applications*** list.

- Click ***Add*** to create a new entry with the entered data or for the selected, predefined application.
- Click ***Delete*** to delete an entry.

➜ Click ***OK*** to apply the settings.

Setting up the NAT function

The Gigaset SX763 WLAN dsl comes equipped with the NAT (Network Address Translation) function. With address mapping, several users in the local network can access the Internet via one or more public IP addresses. All the local IP addresses are assigned to the router's public IP address by default.

One of the characteristics of NAT is that data from the Internet is not allowed into the local network unless it has been explicitly requested by one of the PCs in the network. Most Internet applications can run behind the NAT firewall without any problems. For example, if you request Internet pages or send and receive e-mails, the request for data from the Internet comes from a PC in the local network, and so the router allows the data through. The router opens precisely **one** port for the application. A port in this context is an internal PC address, via which the data is exchanged between the Internet and a client on a PC in the local network. Communicating via a port is subject to the rules of a particular protocol (TCP or UDP).

If an external application tries to send a call to a PC in the local network, the router will block it. There is no open port via which the data could enter the local network.

Some applications, such as games on the Internet, require several links, i.e. several ports so that the players can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to users in the local network. These applications cannot be run if Network Address Translation (NAT) has been activated.

Using port forwarding (the forwarding of requests to particular ports) the router is forced to send requests from the Internet for a certain service, for example a game, to the appropriate port(s) on the PC on which the game is running.

When the Gigaset SX763 WLAN dsl is supplied, the NAT function (Network Address Translation) is activated, i.e. all IP addresses of PCs in the local network are converted to the router's public IP address when accessing the Internet.

You can use the NAT settings to configure the Gigaset SX763 WLAN dsl to carry out the following tasks:

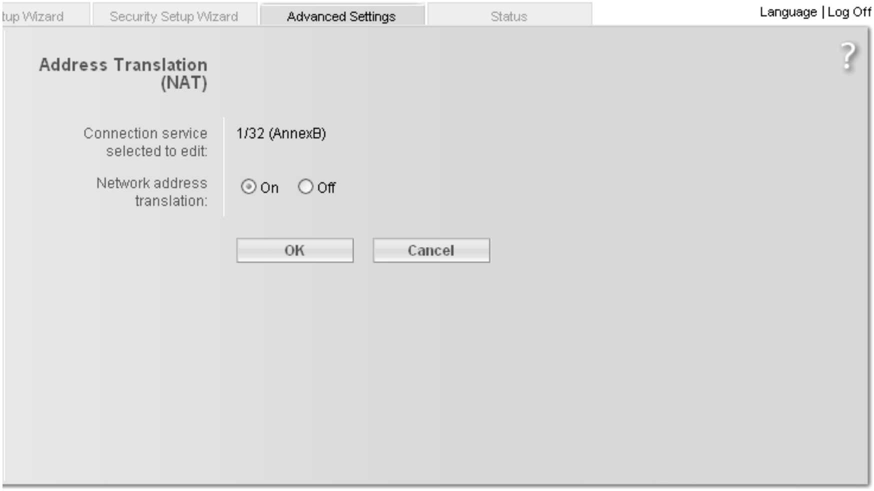
- Set up the Gigaset SX763 WLAN dsl as a virtual server by configuring Port Forwarding (see page 68),
- Open the firewall for selected PCs (page 69).

Note:

For the functions described below, the IP addresses of the PCs must remain unchanged. If the IP addresses of the PCs are assigned via the DHCP server of the Gigaset SX763 WLAN dsl, you must select ***Never expires*** (page 76) as the setting in the ***Local Network*** menu entry for the ***Lease time*** or assign static IP addresses for the PCs.

You can activate or deactivate the NAT function (by default the NAT function is activated).

➙ In the ***Advanced Settings*** – ***Internet*** menu, select ***Address Translation (NAT)*** and then select the required option.



Address Translation (NAT)

Connection service selected to edit: 1/32 (AnnexB)

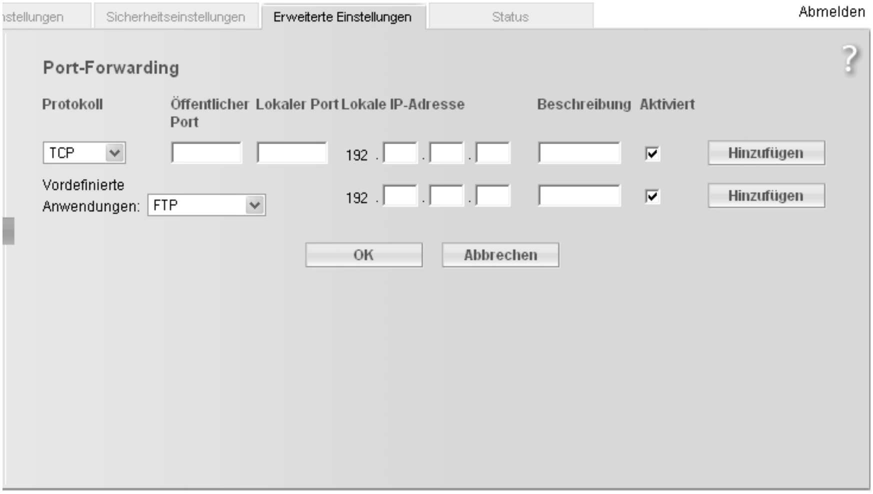
Network address translation: ● On ○ Off

Port Forwarding

If you configure Port Forwarding, the Gigaset SX763 WLAN dsl outwardly assumes the role of the server. It receives requests from remote users under its public IP address and automatically redirects them to local PCs. The private IP addresses of the servers on the local network remain protected.

Internet services are addressed via defined port numbers. The Gigaset SX763 WLAN dsl needs a mapping table of the port numbers to redirect the service requests to the servers that actually provide the service.
Port Forwarding has been configured for this purpose.

→ To set up port forwarding for a service, select ***Port Forwarding*** from the ***Advanced Settings*** – ***Internet*** – ***Address Translation (NAT)*** menu.



Protokoll: TCP | 192 . . . | ☑

Vordefinierte Anwendungen: FTP | 192 . . . | ☑

→ Select the required application from the ***Predefined applications*** list.

→ Activate ***Enabled*** by ticking the check box.

→ Click the ***Add*** button. The data for the required service is entered on the screen.

→ Click the ***Delete*** button to delete an entry.

If the application you require is not in the list, you must manually enter the relevant data on the screen:

→ Select the protocol for the service you are providing from the ***Protocol*** list.

→ Under ***Public port***, enter the port number of the service you are providing.

→ In the ***Local port*** field, enter the internal port number to which service requests are to be forwarded.

➭ In the ***Local IP address*** field, enter the IP address of the PC that provides the service.

Example: The Web server has been configured to react to requests on port 8080. However, the requests from web sites enter the Web server via port 80 (standard value). If you add the PC to the forwarding table and define port 80 as the public port and port 8080 as an internal port, all requests from the Internet are diverted to the service with the port number 80 on the Web server of the PC you have defined with port 8080.

Note:

You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example **`80.90-140.180`**.

➭ ***Comment***: Enter a description that makes it easy to identify different entries.

➭ Activate ***Enabled*** by ticking the check box.

➭ Click the ***Add*** button to add a new entry.

➭ Click the ***Delete*** button to delete an entry.

➭ Click ***OK*** to apply the settings.

Opening the firewall for selected PCs (Exposed Host)

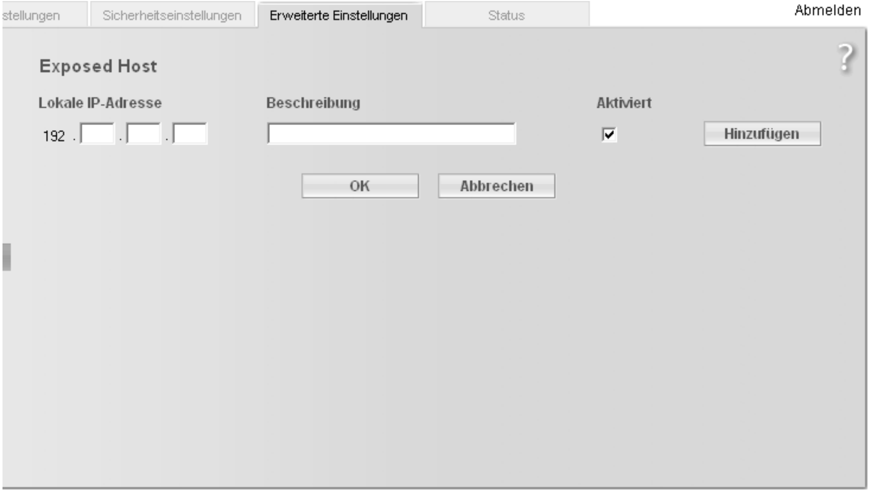
You can set up a client in your local network to be a so-called "exposed host" (DMZ). Your device will then forward all incoming data traffic from the Internet to this client. You can then, for example, operate your own Web server on one of the clients in your local network and make it accessible to Internet users.

As the exposed host, the local client is directly visible to the Internet and therefore particularly vulnerable to attacks (e.g. hacker attacks). Only activate this function if it is absolutely necessary (e.g. to operate a Web server) and other functions (e.g. port forwarding) are not adequate. In this case you should take appropriate measures for the clients concerned.

Note:

Only one PC per public IP address can be set up as an Exposed Host (see also the section entitled Port Forwarding on page 68).

➭ To set up a PC as an exposed host, select ***Exposed Host*** from the ***Advanced Settings*** – ***Internet*** – ***Address Translation (NAT)*** menu.



→ Enter the ***Local IP address*** of the PC that is to be enabled as an Exposed Host.

→ Enter a name for the PC in the ***Comment*** field.

→ Activate ***Enabled*** by ticking the check box.

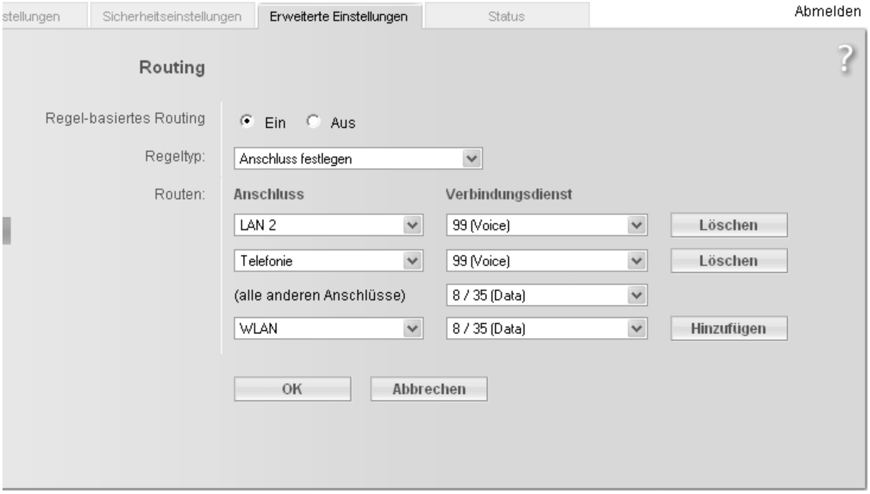
→ Click the ***Add*** button to add the entry to the list.

→ Click the ***Delete*** button to delete the entry from the list.

→ Apply the settings by clicking ***OK***.

Routing

Your Internet service provider can permit you to set up a number of connection services. The entire data traffic between your local network and the Internet uses the first connection service (route) by default. After setting up various connection services (page 54), you can change this default route and set up additional routes by assigning data traffic to other connection services. Rules are provided to assist you in doing this, which define criteria for deciding which data traffic is assigned to which connection service.



Routing

Regel-basiertes Routing ● Ein ○ Aus

Regeltyp: Anschluss festlegen

Routen:

Anschluss	Verbindungsdienst	
LAN 2	99 (Voice)	Löschen
Telefonie	99 (Voice)	Löschen
(alle anderen Anschlüsse)	8 / 35 (Data)	
WLAN	8 / 35 (Data)	Hinzufügen

➙ Activate or deactivate ***Policy-based routing*** for your Internet connection.

➙ Choose the ***Policy type***, i.e. how you would like to define the various routes for data traffic between your local network and the Internet:

- Choose ***Specify interface*** to specify routes for clients in your local network depending on the port used for connecting to your device (e.g. LAN port or wireless network connection).
- Choose ***Specify IP address*** or ***Specify MAC address*** to specify routes for clients depending on your IP address or MAC address.

➭ Specify the routes for data traffic between your local network and the Internet:

– Enter the ***Connector***, the local IP address or the MAC address of the clients in the local network that are to use the respective route.

  If you specify routes by entering the MAC address, you can also enter the device name in order to identify the individual clients.

– For each route, choose the ***Connection service*** that the respective client is to use to connect to the Internet.

  A default route is used for all non-listed clients.

➭ Click the Delete button to delete an entry.

➭ Click Add to create a new entry with the entered data or for the selected client.

➭ Click OK to save and apply the changes.

➭ Click Cancel to reject the changes.

Dynamic DNS

Any service you provide on the Internet can be accessed by a Domain name. Your router's Public IP address is assigned to this domain name. If your Internet service provider assigns the IP address for your local network's WAN connection dynamically, the IP address of the router can change. The assignment to the domain name will no longer be valid and your service will no longer be available.

In this case you must ensure that the assignment of the IP address to the domain name is updated regularly. This task is performed by the dynamic DNS service (DynDNS). You can use the DynDNS service to assign the Gigaset SX763 WLAN dsl an individual static domain name on the Internet even if it does not have a static IP address.

Various Internet providers offer a free DynDNS service.
If you use the service of a DynDNS provider, your service can be reached on the Internet as a subdomain of one of the DynDNS service domains.

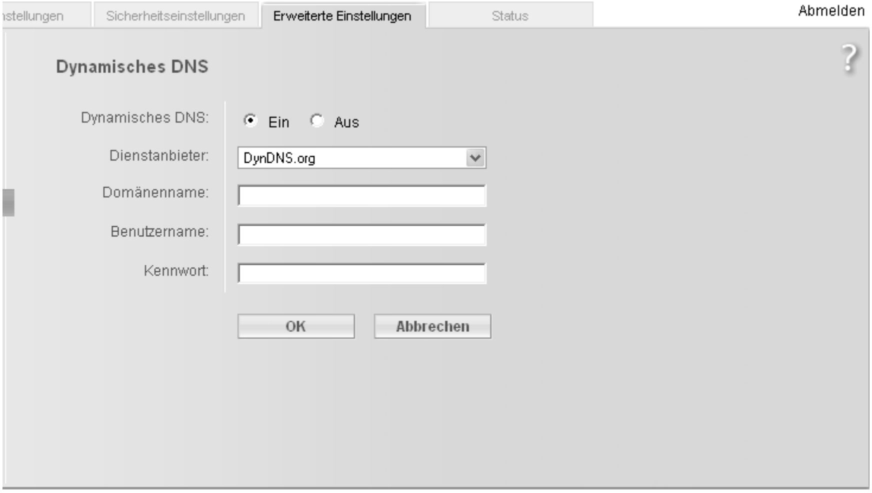
One possible service is **DynDNS.org** (http://www.DynDNS.org). If you have activated the device's DynDNS function, it will monitor its public IP address. When this changes, the device will open a connection to DynDNS.org and update its IP address there.

Note:

You must have an account with the service you have chosen (e.g. DynDNS.org) before you can use the DynDNS function. Follow the instructions on the provider's web site. Then enter the user data when configuring the router.

To use the router's DynDNS function, select ***Dynamic DNS*** from the ***Advanced Settings*** – ***Internet*** menu.

➙ Activate the ***Dynamic DNS*** function.



Dynamisches DNS

Dynamisches DNS: ● Ein ○ Aus

Dienstanbieter: DynDNS.org

Domänenname:

Benutzername:

Kennwort:

➙ Select a service from the ***Service provider*** list.

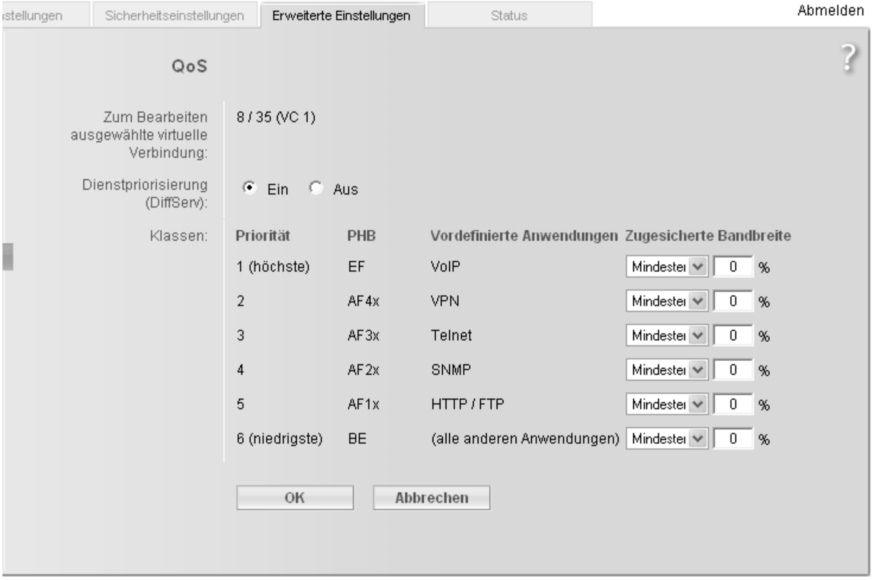
➙ Enter ***Domain name***, ***User name*** and ***Password***. You will have received all the necessary information when you registered with your ***Service provider***.

➙ Click ***OK*** to apply the settings.

QoS (Quality of Service)

Many communication and multimedia applications require large, high-speed bandwidths to transfer data between the local network and the Internet. However, for many applications there is often only one Internet connection available with limited capacity. ***QoS*** (Quality of Service) divides this capacity between the different applications and provides undelayed, continuous data transfer where data packets with higher priority are given preference.

➙ In the ***Advanced Settings*** – ***Internet*** menu, select ***QoS***.



QoS

Zum Bearbeiten ausgewählte virtuelle Verbindung: 8 / 35 (VC 1)

Dienstpriorisierung (DiffServ): ● Ein ○ Aus

Klassen:

Priorität	PHB	Vordefinierte Anwendungen	Zugesicherte Bandbreite
1 (höchste)	EF	VoIP	Mindester 0 %
2	AF4x	VPN	Mindester 0 %
3	AF3x	Telnet	Mindester 0 %
4	AF2x	SNMP	Mindester 0 %
5	AF1x	HTTP / FTP	Mindester 0 %
6 (niedrigste)	BE	(alle anderen Anwendungen)	Mindester 0 %

All settings apply for the displayed connection service that you selected for editing on the ***Advanced Settings*** – ***Internet*** (page 54) screen.

→ Select ***Differentiated services***, i.e. the prioritisation of certain services for data transfer between your network and the Internet.

Via ***Priority*** you can determine which data packets are to be given preferential transmission. By means of ***PHB*** (Per Hop Behaviours) a decision is also made about whether data packets are to be forwarded immediately before all others (***EF***, Expedited Forwarding), guaranteed and without data loss (***AF***, Assured Forwarding) or normally (***BE***, Best Effort). If your application already supports QoS, it will determine the priority automatically. Your device will note this for forwarding. In addition, the device recognises certain ***Predefined applications*** and assigns each packet the relevant priority. You can also determine which proportion of the bandwidth for your Internet connection is to be made available for a certain class as ***Allocated bandwidth***.

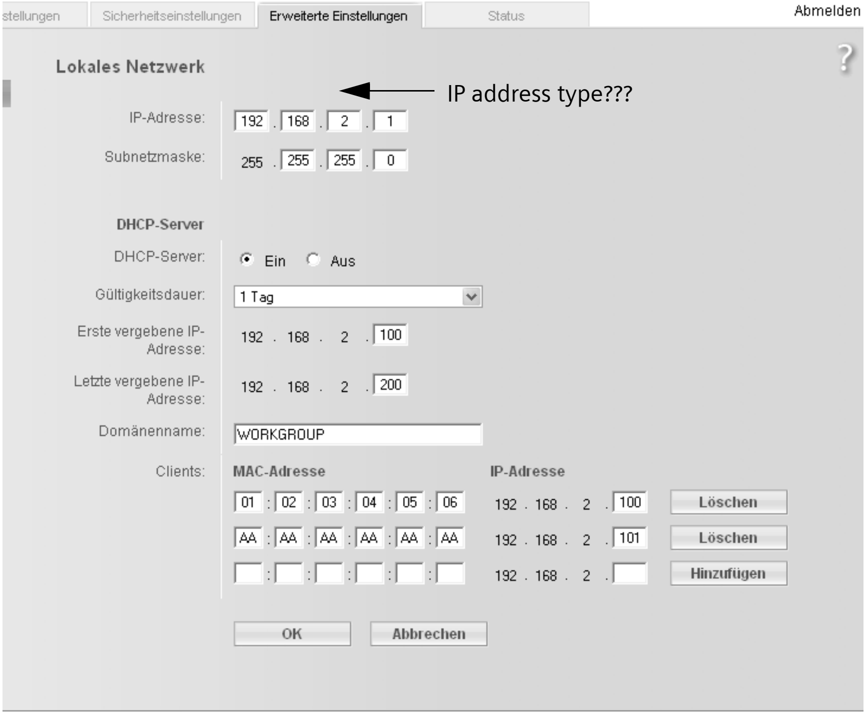
→ Select ***Allocated bandwidth*** for ***Predefined applications*** and for ***(all other applications)***.

→ Click ***OK*** to save and apply the changes.

LAN configuration

You can use the LAN configuration to define an IP address for the Gigaset SX763 WLAN dsl and configure the DHCP server.

→ Select ***Advanced Settings*** – ***Local Network***.



IP address type???

Lokales Netzwerk

IP-Adresse: 192 . 168 . 2 . 1

Subnetzmaske: 255 . 255 . 255 . 0

DHCP-Server

DHCP-Server: ● Ein ○ Aus

Gültigkeitsdauer: 1 Tag

Erste vergebene IP-Adresse: 192 . 168 . 2 . 100

Letzte vergebene IP-Adresse: 192 . 168 . 2 . 200

Domänenname: WORKGROUP

Clients:

MAC-Adresse	IP-Adresse
01 : 02 : 03 : 04 : 05 : 06	192 . 168 . 2 . 100
AA : AA : AA : AA : AA : AA	192 . 168 . 2 . 101
: : : : :	192 . 168 . 2 .

Defining the private IP address for the Gigaset SX763 WLAN dsl

On this screen you can change the device's IP address. The preset IP address is 192.168.2.1. This is the Private IP address of the Gigaset SX763 WLAN dsl. This is the address under which the device can be reached in the local network. It can be freely assigned from the block of available addresses. The IP address under which the Gigaset SX763 WLAN dsl can be reached from outside is assigned by the Internet service provider.

→ If you want to assign a different IP address to the Gigaset SX763 WLAN dsl, enter it in the fields next to ***IP address***.

→ Adjust the ***Subnet mask*** if necessary.

We recommend that you use an address from a block that is reserved for private use. This address block is 192.168.1.1 to 192.168.255.254.

> **Note:**
>
> New settings can only be made after the Gigaset SX763 WLAN dsl has been rebooted. If necessary, reconfigure the IP address on your PC (including one that is statically assigned) so that it matches the new configuration.

Configuring the DHCP server

The Gigaset SX763 WLAN dsl has a DHCP server for which the factory setting is active. Consequently, the IP addresses of the PCs are automatically assigned by the Gigaset SX763 WLAN dsl.

> **Note:**
>
> ◆ If the DHCP server for the Gigaset SX763 WLAN dsl is activated, you can configure the network setting on the PC so that the option ***Obtain an IP address automatically*** is set up. Further information about this can be found in the section entitled "Das lokale Netzwerk konfigurieren" on page 127.
>
> ◆ If you deactivate the DHCP server, you will have to assign a static IP address for the PCs that use the network settings.

→ To activate the DHCP server, select ***On***.

→ If the DHCP server is active, you can define a ***Lease time***. The Lease time determines the period for which the PCs retain the IP addresses assigned to them without changing them.

> **Note:**
>
> If you select ***Never expires***, the IP addresses are never changed. Activate this option if you want to make NAT or firewall settings using the IP addresses of the PCs; otherwise you have to assign static IP addresses to these PCs.

→ Define the range of IP addresses the Gigaset SX763 WLAN dsl should use to automatically assign IP addresses to the PCs. Define the ***First issued IP address*** and the ***Last issued IP address***.

→ You can define the name of a domain (Windows workgroup) in the ***Domain name*** field.

Assigning static IP addresses to individual PCs

Even if you have activated the DHCP server you can still assign a static IP address to individual PCs (e.g. when setting up these PCs for NAT functions).

→ Enter the ***MAC address*** and the name of the PC in the ***Device name*** field.

→ Enter the ***IP address*** you wish to assign to the PC in the field below.

→ Click the ***Add*** button to add the entry to the list.

→ Click the ***Delete*** button to delete the entry from the list.

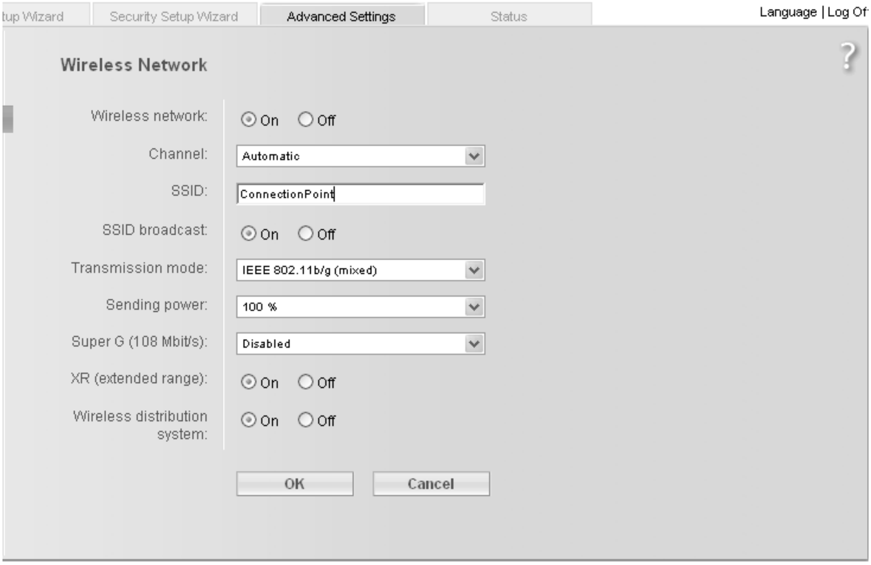
→ Apply the settings by clicking ***OK***.

Configuring wireless connections

If PCs are communicating wirelessly via the Gigaset SX763 WLAN dsl, you should also improve the security of your wireless network. This configuration is made via the ***Advanced Settings*** – ***Wireless Network*** menu. You can carry out the following here:

- Activate the wireless module of the Gigaset SX763 WLAN dsl (for information see below)
- Set up the channel and SSID (page 78)
- Set up Encryption for wireless transmissions (page 80)
- Restrict access to the LAN of the Gigaset SX763 WLAN dsl (page 80) and
- Configure the repeater function on the Gigaset SX763 WLAN dsl.

→ In the ***Advanced Settings*** menu, select ***Wireless Network***.



Wireless Network

Wireless network: ● On ○ Off

Channel: Automatic

SSID: ConnectionPoint

SSID broadcast: ● On ○ Off

Transmission mode: IEEE 802.11b/g (mixed)

Sending power: 100 %

Super G (108 Mbit/s): Disabled

XR (extended range): ● On ○ Off

Wireless distribution system: ● On ○ Off

➡ Select ***On*** for the ***Wireless Network*** (default setting).

Devices can only log in wirelessly if the WLAN module of the Gigaset SX763 WLAN dsl is activated.

You can now make the settings for the wireless network.

Channel

All clients in the network use the set radio channel for wireless data transfer. You can choose between various channels, depending on your current location.

➡ Select ***Automatic*** so that the best channel for transmitting the data is used automatically.

SSID

For the wireless network components to be able to communicate with one another, you must use the same SSID (Service Set Identifier).

The default SSID for the Gigaset SX763 WLAN dsl is **ConnectionPoint**. For security reasons you should change this SSID and deactivate SSID broadcast (for information see below).

Enter a character string of your choice. The SSID is case sensitive. It can contain up to 32 alphanumeric characters.

Note:
The connection to the wireless network adapters will be interrupted until you have entered the new SSID in them as well.

SSID broadcast

If this option is enabled (default setting), the Gigaset SX763 WLAN dsl will send the SSID in all data transfers and the SSID of your Gigaset SX763 WLAN dsl will be displayed on PCs that have a wireless network adapter. In this case, hackers could use the SSID to detect your network.

If you deactivate ***SSID broadcast***, the SSID of the Gigaset SX763 WLAN dsl will not be displayed. This increases the protection against unauthorised access to your wireless network. Make a note of the SSID. You will need it to log on to the PC.

➡ Select ***Off*** to deactivate ***SSID broadcast***.

Transmission mode

This function is only shown in the window if the Super G transmission mode is deactivated (page 79).

The IEEE 802.11g standard permits data transfer up to 54 Mbit/s, and the IEEE 802.11b standard up to 11 Mbit/s. Choose ***IEEE 802.11g only*** to ensure the best possible data transfer rates in your network. To operate clients with older wireless network adapters in your network, select ***IEEE 802.11b/g (mixed)***.

➡ Select the required transmission mode for your wireless network.

Sending power

→ Select the required sending power for your device.
It is recommended that you select a sending power with a range to suit the spatial environment of your local network. A much greater range makes it easier to eavesdrop on your wireless data transfer.

Super G (108 Mbit/s)

With the help of channel bundling, the Super G transmission mode enables wireless data transfer up to 108 Mbps. The channel for wireless data transfer cannot be changed. You can only use Super G if this function is supported by at least one client in your wireless network. For the best possible data transfer rates, all clients in your LAN should support Super G.

Please ensure the following:

If you activate Super G as the transmission mode, but it is not supported by all components in your wireless network, then for technical reasons the transfer rate in the network may be significantly lower than the possible maximum of 108 Mbit/s.

→ Select ***Dynamic*** to use ***Super G (108 Mbit/s)*** for your wireless network to increase the data transfer rate. If you select this transmission mode, the router accepts participants that communicate at different transfer rates and adjusts to the slowest client in the network.

In the default setting, ***Super G (108 Mbit/s)*** is deactivated.

XR (extended range)

By activating XR, wireless data transfer is also enabled in the border areas of your wireless network, though at a very slow data transfer rate. The switch to XR mode happens automatically if there is a weak signal and if the remote station is likewise XR-enabled.

→ Activate or deactivate XR for your wireless network to increase the range.

→ Click ***OK*** to apply the settings.

WDS (repeater function)

If you use a repeater to extend the range in your wireless network, you must activate the Wireless Distribution System (WDS) function.

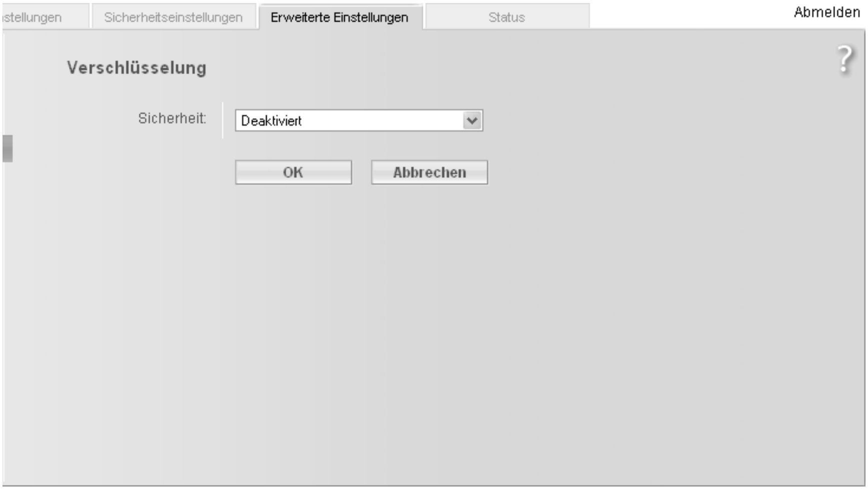
Setting up wireless security

If you are sending data over radio channels, we recommend that you activate encryption (WEP or WPA) on the components in the wireless network. WPA offers greater security than WEP. You should therefore select WPA encryption if it is supported by all components in your wireless network.

WPA is a more efficient method than WEP for protecting wireless networks. Dynamic keys, based on TKIP (Temporal Key Integration Protocol) offer increased security. The new WPA2 standard is based on AES.

WPA also supports the use of an authentication server.

→ In the ***Wireless Network*** menu, select ***Encryption & Authentication***.



Verschlüsselung

Sicherheit: Deaktiviert

The following security mechanisms are currently available:

- WPA2-PSK and WPA2-PSK/WPA-PSK (page 81)
- WAP2 and WPA2/WPA with authentication server (page 82)
- WEP encryption (Wired Equivalent Privacy, see page 83)

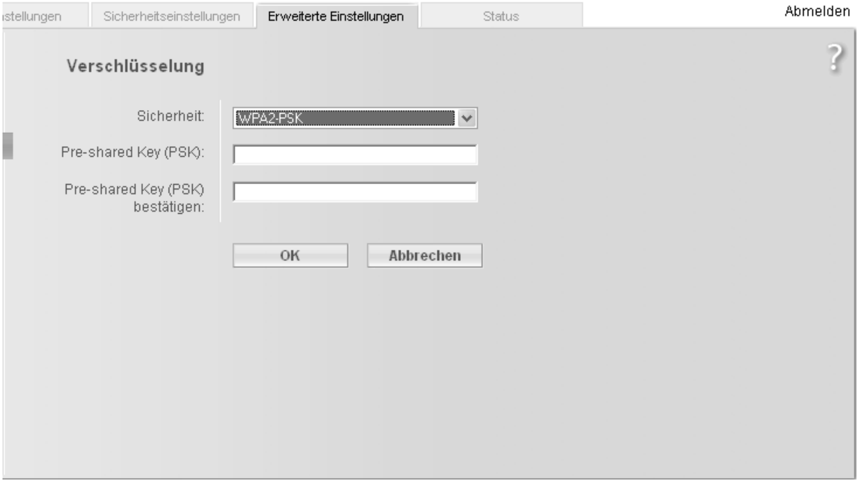
WPA2-PSK and WPA2-PSK / WPA-PSK

WPA with pre-shared key (WPA-PSK)

WPA-PSK is a special WPA mode for private users and users in small companies without their own authentication server. After a certain period of time (Rekey interval), encryption keys are automatically generated with the pre-shared key, automatically changed ("rekeying") and authenticated between the devices.

The standard of encryption available to you depends on the components in the wireless network. Every PC (network adapter) that requires access to a WPA-protected wireless network must also support WPA. To find out whether and how you can use WPA on your PC, read your network adapter's user guide. If all components support WPA2, select ***WPA2-PSK***. If you are using network adapters that only support WPA, select ***WPA2-PSK / WPA-PSK***. The entries described below are identical for both options.

→ Select the required option in the ***Security*** field.



Verschlüsselung

Sicherheit: WPA2-PSK

Pre-shared Key (PSK):

Pre-shared Key (PSK) bestätigen:

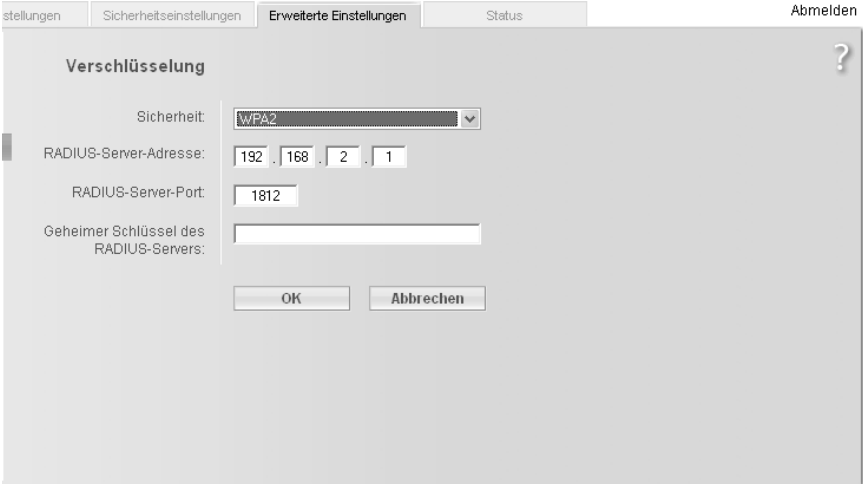
→ Enter a key in the ***Pre-shared key*** field (up to 32 alphanumerical characters) and confirm it by entering it again.

→ Apply the settings by clicking ***OK***.

WPA and WPA2 with authentication server

In large networks (e.g. in companies) WPA enables the use of an additional authentication service. In this case, user access is controlled by user accounts and passwords, in addition to WPA encryption. A RADIUS server acts as an authentication server. You can select the new ***WPA2*** standard if it is supported by all components in your wireless network. Select ***WPA2 / WPA*** if you are using devices that only support WPA.

→ Select the required option in the ***Security*** field.



Verschlüsselung

Sicherheit: WPA2

RADIUS-Server-Adresse: 192 . 168 . 2 . 1

RADIUS-Server-Port: 1812

Geheimer Schlüssel des RADIUS-Servers:

→ Enter the IP address of the RADIUS server in the ***RADIUS server IP address*** field.

→ Enter the port of the RADIUS server in the ***RADIUS server port*** field.

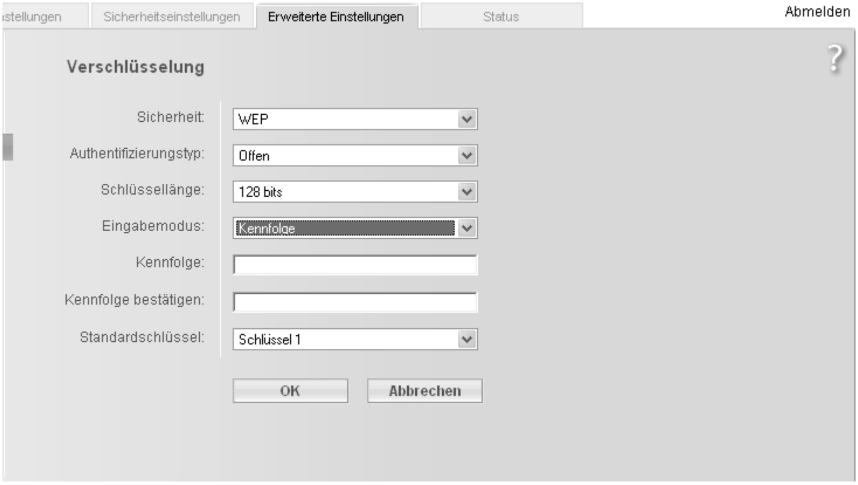
→ In the ***RADIUS server secret key*** field, enter a keyword that conforms to the conventions of the RADIUS servers that the server is to use for authentication.

→ Click ***OK*** to apply the settings.

WEP encryption

If WPA is not supported by all components in your wireless network, we recommend that you activate WEP Encryption on the components.

→ In the ***Security*** field, select ***WEP***.



Verschlüsselung

Sicherheit: WEP

Authentifizierungstyp: Offen

Schlüssellänge: 128 bits

Eingabemodus: Kennfolge

Kennfolge:

Kennfolge bestätigen:

Standardschlüssel: Schlüssel 1

→ Select the ***Authentication type***:

- Select ***Shared*** to require that each client logs in to the network with a specified key.
- Select ***Open*** to permit data transfer within the wireless network without the need to enter a key.

You can choose either the standard 64-bit key or the more robust 128-bit key. The keys are generated in hexadecimal or in ASCII format. You must use the same keys for encryption and decryption for the Gigaset SX763 WLAN dsl and all your wireless network adapters.

→ Select the ***Key length***: 64 bits or 128 bits.

→ Select the ***Input type***, i.e. whether the key is to be entered manually or generated automatically by means of a ***Passphrase***.

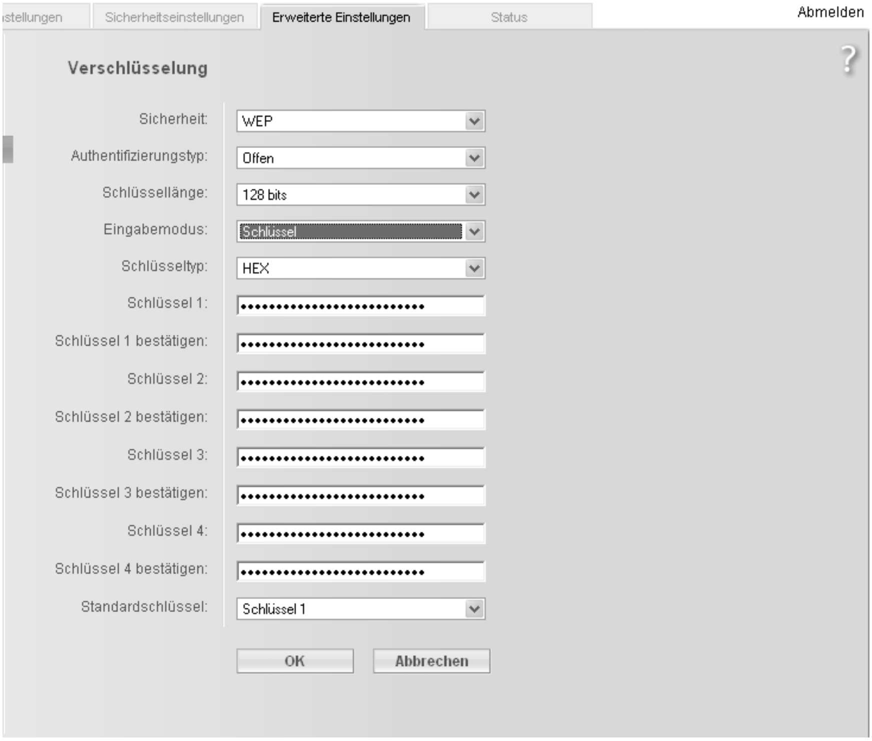
Generating a key by means of a Passphrase

→ Enter a ***Passphrase*** (up to 32 characters) and confirm it by entering it again. Four keys are generated.

→ Select one of the four keys as the ***Default key***.

Manual key entry

➙ Select the ***Key type***, ***Hex*** or ***ASCII***.



Verschlüsselung

Sicherheit: WEP

Authentifizierungstyp: Offen

Schlüssellänge: 128 bits

Eingabemodus: Schlüssel

Schlüsseltyp: HEX

Schlüssel 1: ••••••••••••••••••••••••••

Schlüssel 1 bestätigen: ••••••••••••••••••••••••••

Schlüssel 2: ••••••••••••••••••••••••••

Schlüssel 2 bestätigen: ••••••••••••••••••••••••••

Schlüssel 3: ••••••••••••••••••••••••••

Schlüssel 3 bestätigen: ••••••••••••••••••••••••••

Schlüssel 4: ••••••••••••••••••••••••••

Schlüssel 4 bestätigen: ••••••••••••••••••••••••••

Standardschlüssel: Schlüssel 1

If you select ***Hex*** as the key type you can use the characters **0** to **9** and **A** to **F**.

- With a 64-bit encryption depth, the key is 10 characters long.
  An example of a valid key: 1234567ABC
- With a 128-bit encryption depth, the key is 26 characters long.
  An example of a valid key: 234567ABC8912345DEF1234567

If you select ***ASCII*** as the key type, you can use the characters **0** to **9**, **A** to **Z**, and **a** to **z** plus the special characters in the ASCII character set.

- With a 64-bit encryption depth, the key is 5 characters long.
  An example of a valid key: GIGA1
- With a 128-bit encryption depth, the key is 13 characters long.
  An example of a valid key: GIGASET_SE551

➙ Enter up to four keys in fields ***Key 1*** to ***Key 4*** and confirm them by entering them again in fields ***Confirm key 1*** to ***Confirm key 4***.

→ Select one of the four keys as the ***Default key***.

Note:

- ◆ It is very **important** that you make a note of the key(s) that have been entered or generated. You will need this information to configure the wireless network adapters properly.
- ◆ When you have concluded the configuration, you must change the WEP encryption in the wireless network adapters for the connected PCs in the same way as they will not otherwise be given access to the wireless network of the Gigaset SX763 WLAN dsl.

→ Click ***OK*** to apply the settings.

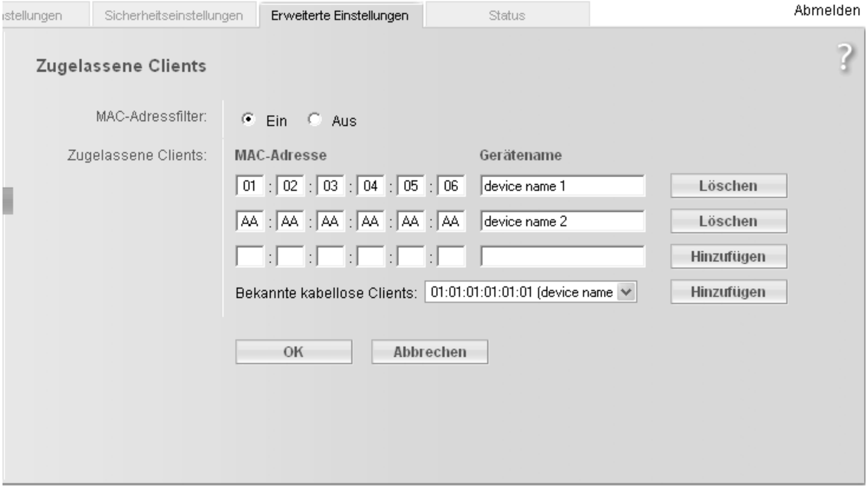
Permitted clients

On this screen you can specify the PCs that are to have wireless access to the Gigaset SX763 WLAN dsl and hence to your LAN.

In the ***Advanced Settings*** – ***Wireless Network*** menu, select ***Allowed Clients***.
The default setting for access control is deactivated. This means that all PCs that use the correct SSID can be logged in.

Access control is based on the MAC addresss of the PC network adapters.

→ Activate access control by selecting ***On*** in the ***MAC address filter*** field.



Zugelassene Clients

MAC-Adressfilter: ● Ein ○ Aus

Zugelassene Clients:

MAC-Adresse	Gerätename
01 : 02 : 03 : 04 : 05 : 06	device name 1
AA : AA : AA : AA : AA : AA	device name 2
: : : : :	

Bekannte kabellose Clients: 01:01:01:01:01:01 (device name

Entering PCs manually:

→ Enter the ***MAC address*** and ***Device name*** of the required PCs in the appropriate fields.

→ Click the ***Add*** button to add the entry to the list.

➞ Click the ***Delete*** button to delete the entry from the list.

➞ Apply the settings by clicking ***OK***.

Selecting from the list of logged-in PCs

➞ Select the required PC from the ***Known wireless clients*** list. All PCs that were already entered manually on the router with the MAC address are displayed.

➞ Click the ***Add*** button to add the selected PC to the list.

➞ Apply the settings by clicking ***OK***.

Note:

If you activate MAC access control, you must at least add the PC, on which you are configuring the Gigaset SX763 WLAN dsl, to the list. Otherwise, you will have no access to the user interface and will receive a corresponding error message.

If you have inadvertently denied all PCs access to the Gigaset SX763 WLAN dsl, you have two options:

◆ You can completely reset the Gigaset SX763 WLAN dsl (page 20).

◆ You can connect a PC to the Gigaset SX763 WLAN dsl using one of the LAN connections. As MAC access control only affects PCs that are connected wirelessly, you can use this PC to change the configuration.

Setting up Internet telephony (VoIP)

The Gigaset SX763 WLAN dsl allows you to make telephone calls via the Internet using an analogue telephone and, if required, via the fixed network as usual. For Internet telephony (VoIP), you require access authorisation from your service provider and the relevant access data. To make calls you must enter this data along with other configuration settings in Advanced Settings in the ***Telephony*** menu.

You can connect a base station for handsets or fax machines to the two telephone ports of the Gigaset SX763 WLAN dsl analogue phone. In addition, you can set up additional extensions for Internet and fixed network calls with SIP clients (as WLAN handsets or in wired or wireless mode on PCs).

The menu comprises the following entries:

- VoIP settings: Enter the basic data from your service provider here (page 88).
- Extensions: Set up the functions for two extensions here (page 90).
- Dialling rules: Specify numbers here that are to be dialled only via the fixed network or only via the Internet.

Note:

If you do not specify any of your own dialling rules, then the default settings will be used as entered in the ***Telephony*** menu under ***Dialing Plans***. Emergency numbers are directed via the fixed network, while all other calls are made via the Internet.

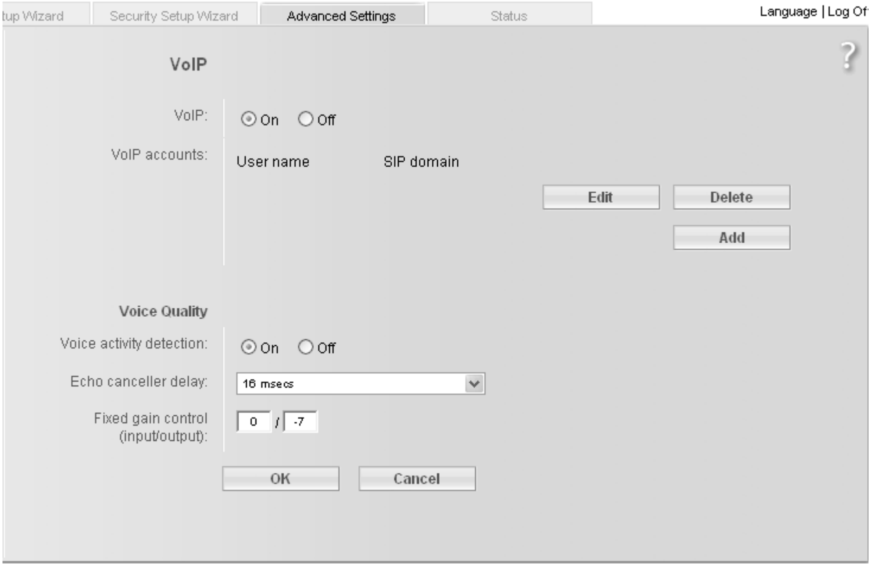
Important information:

- You cannot make calls if there is a power failure, **even the emergency numbers are not accessible then**.
- If VoIP is not set up you will always make calls via the fixed network. The dialling rules will not apply in this case (page 94).
- Check these dialling rules (page 94) and change them if you have agreed special phone tariffs with another provider.
- Do not change the default setting for the Internet connection mode (= "permanent connection") if you are using VoIP (page 37). You can only be called via VoIP if this setting is used. Remember, though, that this setting can result in high connection costs if you have agreed a time-based tariff with your Internet provider.

VoIP settings

You will receive the access and configuration data for Internet telephony from your service provider.

→ In the ***Advanced Settings*** – ***Telephony*** menu, select ***VoIP***.



VoIP

VoIP: ● On ○ Off

VoIP accounts: User name SIP domain

Voice Quality

Voice activity detection: ● On ○ Off

Echo canceller delay: 16 msecs

Fixed gain control (input/output): 0 / -7

→ Select ***On*** if you wish to use Internet telephony (default setting).

→ If you have already configured Internet telephony in the ***Basic Setup Wizard***, your VoIP account will be shown with ***User name*** and ***SIP domain*** in addition to ***VoIP accounts***. If you want to change a previously configured VoIP account, click ***Edit*** (see page 89).

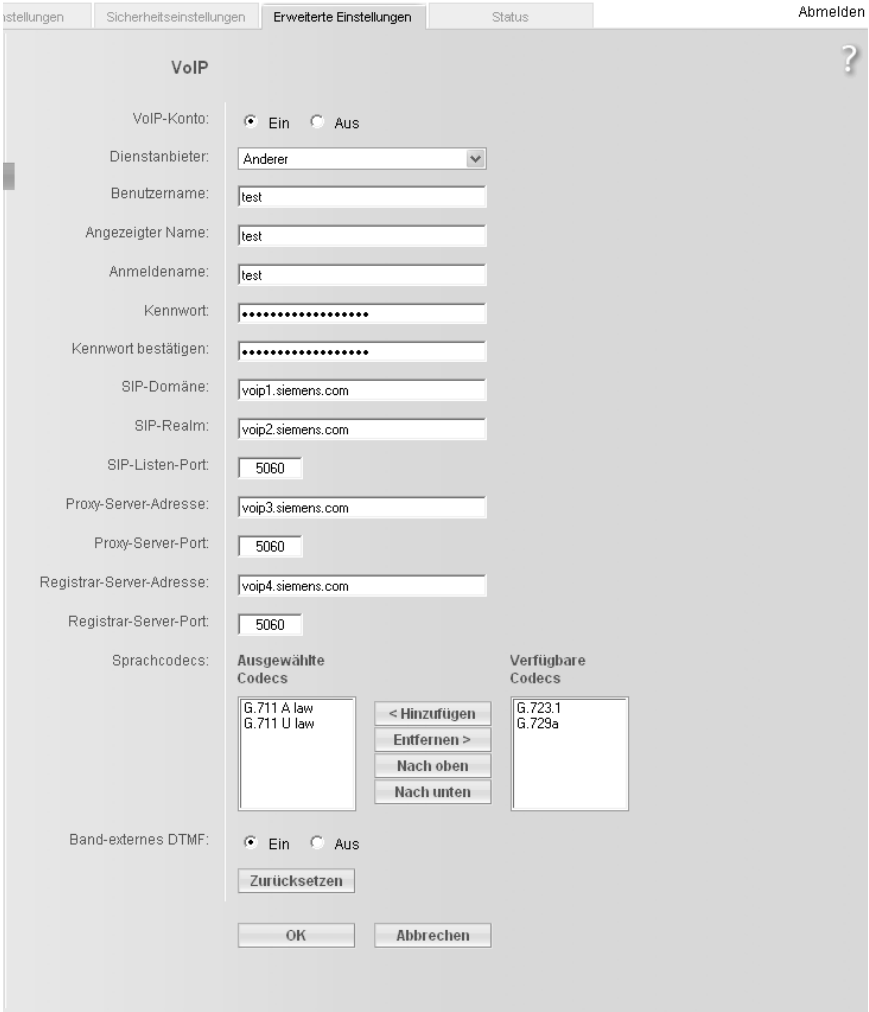
→ If you want to configure additional ***VoIP accounts***, click ***Add*** (see page 89).

If you have configured VoIP settings in the Basic Setup Wizard the data for your VoIP account is shown in this line. You can edit this data or add new data for additional accounts.

→ You can generally accept the default settings for ***Voice Quality***:

- ***Voice activity detection***: If this function is activated, no data will be transmitted during breaks in speech during a telephone call.
- ***Echo canceller delay***: If you want to hear your own voice as an echo during VoiP telephone calls, you should choose a different value from the list.
- ***Fixed gain control (input/output)***.

Setting up or modifying a VoiP account



VoIP

VoIP-Konto: ● Ein ○ Aus

Dienstanbieter: Anderer

Benutzername: test

Angezeigter Name: test

Anmeldename: test

Kennwort: ••••••••••••••••••

Kennwort bestätigen: ••••••••••••••••••

SIP-Domäne: voip1.siemens.com

SIP-Realm: voip2.siemens.com

SIP-Listen-Port: 5060

Proxy-Server-Adresse: voip3.siemens.com

Proxy-Server-Port: 5060

Registrar-Server-Adresse: voip4.siemens.com

Registrar-Server-Port: 5060

Sprachcodecs:

Ausgewählte Codecs	Verfügbare Codecs
G.711 A law G.711 U law	G.723.1 G.729a

Band-externes DTMF: ● Ein ○ Aus

- To set up a new account, select ***On***.
- In the ***Service provider*** menu, select the ***Other*** option or else select one of the already preconfigured providers.
- Enter the data you have received from your service provider:

  If you choose a preconfigured service provider, the only options are generally ***User name*** and ***Password***.

  If you wish to add or modify data, click the ***Show Additional Settings*** button.

If you have selected the ***Other*** option, enter the data for ***Displayed name***, ***Authorization user name***, ***SIP domain***, ***SIP realm***, ***Proxy server address*** and ***Registrar server address***.

→ Leave the default settings for the parameters ***SIP listen port***, ***Proxy server port***, ***Registrar server port***, ***Voice codecs*** and ***Out-of-band DTMF*** unless your service provider has provided you with other data.

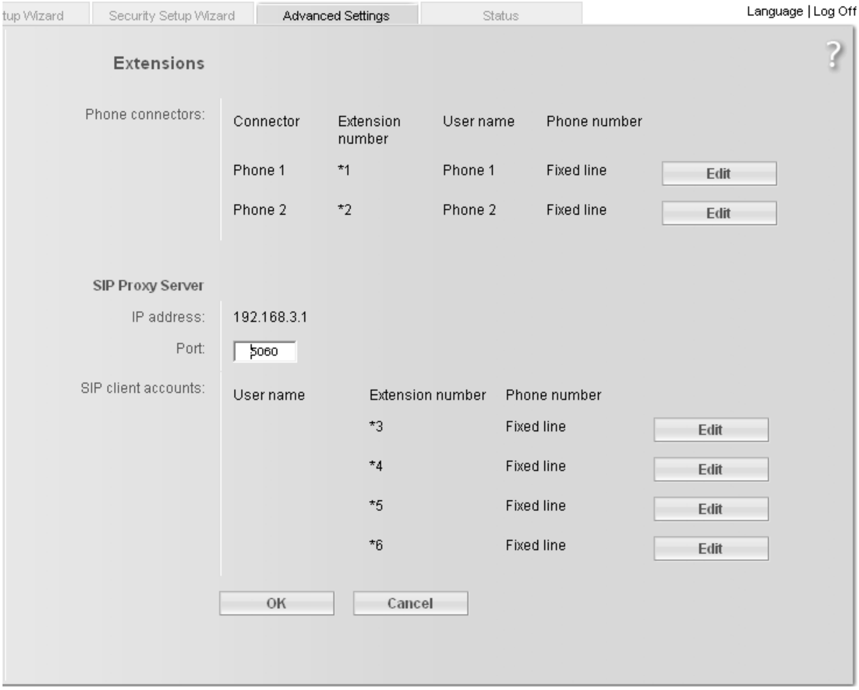
→ Click the ***OK*** button to apply the settings.

Extensions

Your Gigaset SX763 WLAN dsl allows you to configure up to six internal extensions that you can use for making calls via the fixed network or via VoIP. Two of these extensions are the Phone 1 and Phone 2 ports for your Gigaset SX763 WLAN dsl, while the remaining extensions are connections for SIP clients. You can assign each extension the relevant line (fixed network or VoiP account) for incoming and outgoing calls and make other settings for each extension (e.g. call waiting, call forwarding, caller display).

The process for configuring extensions, which uses the two telephone ports of the Gigaset SX763 WLAN dsl, is somewhat different to that for the SIP extensions. The latter must be VoIP telephones, which are connected in wired or wireless mode to the Gigaset SX763 WLAN dsl, or PCs with a SIP client, which are connected to the Gigaset SX763 WLAN dsl.

→ In the ***Advanced Settings*** – ***Telephony*** menu, select ***Extensions***.



Extensions

Phone connectors:

Connector	Extension number	User name	Phone number
Phone 1	*1	Phone 1	Fixed line
Phone 2	*2	Phone 2	Fixed line

SIP Proxy Server

IP address: 192.168.3.1

Port: 5060

SIP client accounts:

User name	Extension number	Phone number
	*3	Fixed line
	*4	Fixed line
	*5	Fixed line
	*6	Fixed line

Phone connectors

The two telephone ports Phone 1 and Phone 2 of the Gigaset SX763 WLAN dsl have the internal phone number ***1** or ***2**.

→ Click Edit to adapt the settings for an entry (page 92).

SIP Proxy Server

In addition to the telephones connected to your Gigaset SX763 WLAN dsl, you can configure wireless VoIP phones (WLAN handsets) or PCs with SIP clients in your local network with the assistance of the SIP proxy servers integrated as internal extensions in your device and then use these to make calls via the fixed network or via VoIP.

Use the IP address displayed in your local network for registering your wireless VoIP phones or your other SIP clients with your SIP proxy server.

Port

The default port via which wireless VoIP phones or other SIP clients register with the SIP proxy server is entered here.

SIP client accounts

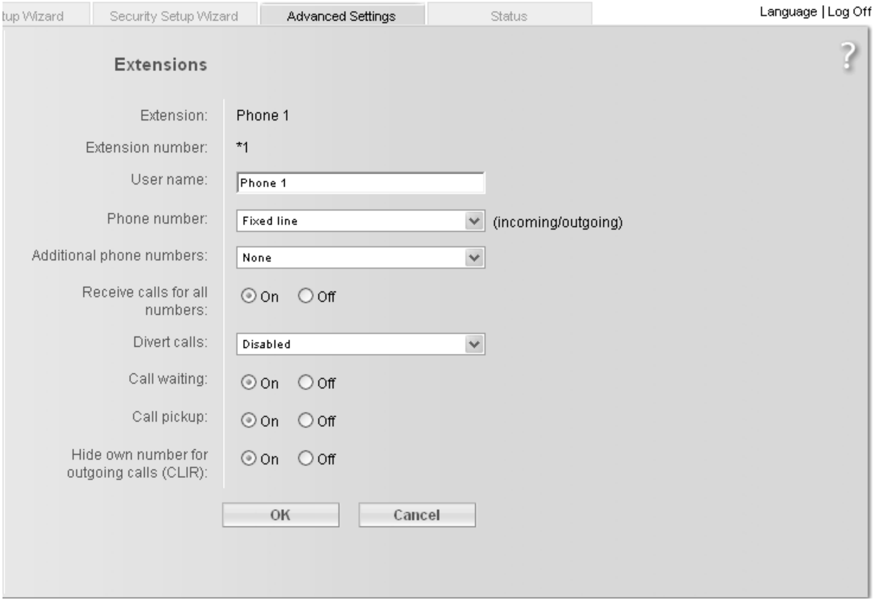
→ Make the extension settings for each SIP user account, which is used for registering wireless VoIP phones and other SIP clients with the SIP proxy server of your device. The ***User name*** and ***Extension number*** are displayed for identifying the individual telephone ports. These extensions have the internal phone numbers ****3*** to ****6***.

→ Click ***Edit*** to adjust the settings for an entry (page 92).

→ Click ***Delete*** to delete an entry.

→ Click ***Add*** to create a new entry and to adjust the settings for this entry.

Configuring extensions



Extensions

Extension: Phone 1

Extension number: *1

User name: Phone 1

Phone number: Fixed line (incoming/outgoing)

Additional phone numbers: None

Receive calls for all numbers: ● On ○ Off

Divert calls: Disabled

Call waiting: ● On ○ Off

Call pickup: ● On ○ Off

Hide own number for outgoing calls (CLIR): ● On ○ Off

The Extension shows either the selected port of the Gigaset SX763 WLAN dsl (Phone 1 or Phone 2) or the SIP client. The ***Extension number*** for the extension is preset and is displayed as a call number.

→ Enter a name for identifying the port in the ***User name*** field. You can also leave the default setting for Phone 1 and Phone 2.

→ Select the ***Phone number*** from the list (your VoIP service provider or one of your VoIP service providers or fixed network) for this extension.

The list of numbers for Internet telephony is the one you set up in the ***VoIP*** menu (page 88). All outgoing calls are directed by default via this phone number. Incoming calls for the selected phone number are signalled.

- ➞ In the ***Additional phone numbers*** fields, you can select which numbers you want to use for calls on this extension with a prefix. You can choose up to two other connection options from the configured fixed network numbers and VoIP accounts. Outgoing calls are directed via this number if . Incoming calls for the selected phone number are signalled.
- ➞ Select ***Receive calls for all numbers*** if you wish to receive all incoming calls on all extensions.
- ➞ You can configure ***Divert calls*** with the following options for the Phone 1 and Phone 2 ports:
  - – ***Divert always***: Each call for the extension is forwarded to the other extensions.
  - – ***When busy***: A call for the extension is forwarded to the other extensions if this extension is busy.
  - – ***No reply***: A call for the extension is forwarded to the other extensions if the call is not answered.
- ➞ Select the ***Call waiting*** option if you want to permit a signal for an incoming call while you are on a call. (only for the Phone 1 and Phone 2 ports).
- ➞ Select the ***Call pickup*** option to have the option to accept all incoming calls on this extension.
- ➞ Select ***Hide own number for outgoing calls (CLIR)*** if you want to prevent the number of this extension being displayed for outgoing calls. (only for the Phone 1 and Phone 2 ports).

Note:

Many service providers either do not support this function or may be unreliable. Contact your service provider if you want to be certain that CLIR, for example, is actually supported.

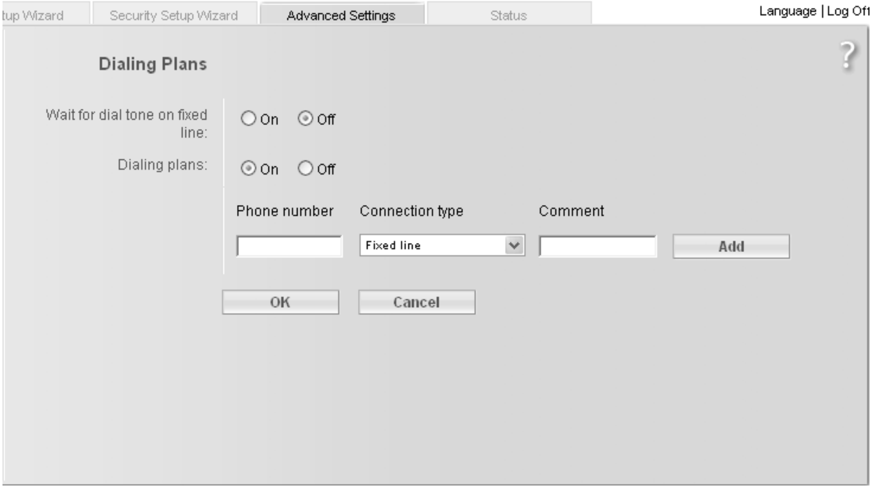
- ➞ Click ***OK*** to apply the settings.

Dialing Plans

On this screen you can enter the following:

- Specify whether certain phone numbers or prefixes are to be dialled via the Internet or the fixed network,
- Block numbers.

→ To make these settings, in the ***Advanced Settings*** – ***Telephony*** menu, select the menu entry ***Dialing Plans***.



Dialing Plans

Wait for dial tone on fixed line: ○ On ● Off

Dialing plans: ● On ○ Off

Phone number	Connection type	Comment
	Fixed line	

→ ***Wait for dial tone on fixed line***:

Only activate this function if it is necessary for the smooth functioning of your Gigaset SX763 WLAN dsl within the telephone network.

→ Choose whether you want to use dialling rules.

→ The emergency number is already entered as a dialling rule in the relevant fields. You can accept these default settings, overwrite them, delete them or add new ones.

Note

It is recommended to leave the settings for emergency numbers on fixed line. There can sometimes be problems determining the location with VoIP emergency calls if you are no longer in a position to state your current location.

→ In the ***Connection type*** selection field, you can specify whether the entered number is always to be called via the fixed network or the selected VoIP account.

→ You can enter a description for the dialling rule in the ***Comment*** field.

→ Click ***Delete*** to delete the dialling rule. You can add a new dialling rule by clicking the ***Add*** button.

You can define up to a maximum of 32 dialling rules.

→ Click ***OK*** to apply the settings.

Note:

- If you do not specify any dialling rules, the default settings will be used.
- If VoIP (Internet telephony) is not set up you will always make calls via the fixed network. The dialling rules will not apply in this case.

USB

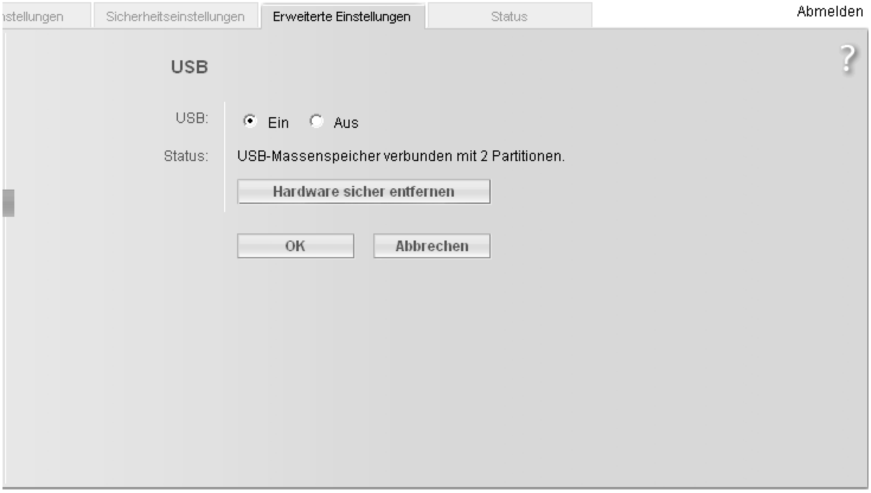
Using your device's USB port, you and other users in the local network can

- share a USB memory (page 97) or
- use a USB printer (page 98).

Notes:

- If you connect a USB hub to the USB port of the Gigaset SX763 WLAN dsl, you can connect and use a USB memory and a USB printer at the same time.
- By connecting a device without its own power supply directly to the USB port, please note that the power consumption must not exceed 100mA.
- The Gigaset SX763 WLAN dsl supports USB V 2.0. Devices that support USB V 1.1 may also be connected.

→ Select ***Advanced Settings*** – ***USB***.



USB

USB: ● Ein ○ Aus

Status: USB-Massenspeicher verbunden mit 2 Partitionen.

→ Activate the USB port on the device.

If a USB device is connected, its ***Status*** is displayed.

Safely Remove Hardware

→ Click this button and wait until any connected USB memory or USB printer is fully deactivated before disconnecting it from the device.

→ Click ***OK*** to save the changes.

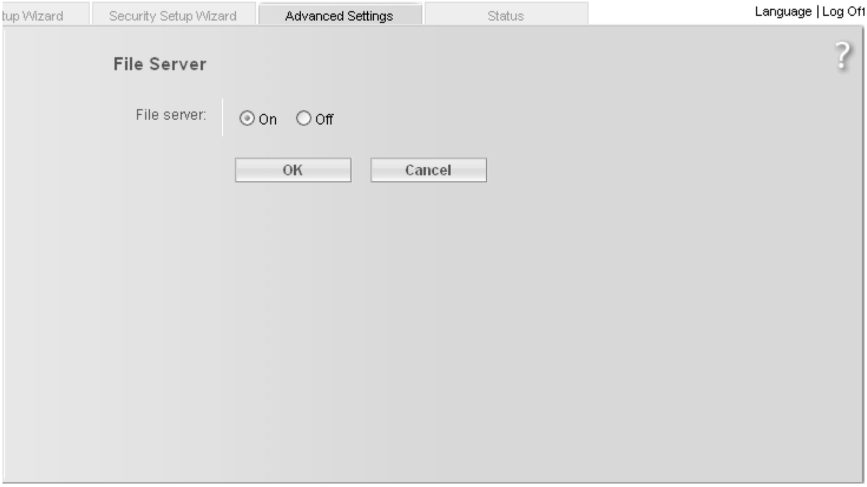
File Server

The device's integrated file server allows you to manage folders and files in a connected USB memory (for example, a USB stick or a USB hard disk) and make them available to all users in the local network.

→ Connect a USB data carrier to the Gigaset SX763 WLAN dsl via the USB port.
The Gigaset SX763 WLAN dsl only supports hard disks with the FAT 16/ 32 file system; it does not support NTFS.

Note:
The USB interface of the Gigaset SX763 WLAN dsl supplies 100 mA of power. Some hard disks, however, need more power. In this case the device must have its own mains adapter.

→ In the ***Advanced Settings*** – ***USB*** menu, select ***File Server***.



File Server

File server: ● On ○ Off

→ Select the ***On*** option for the ***File Server***.

→ Click ***OK*** to save the settings.

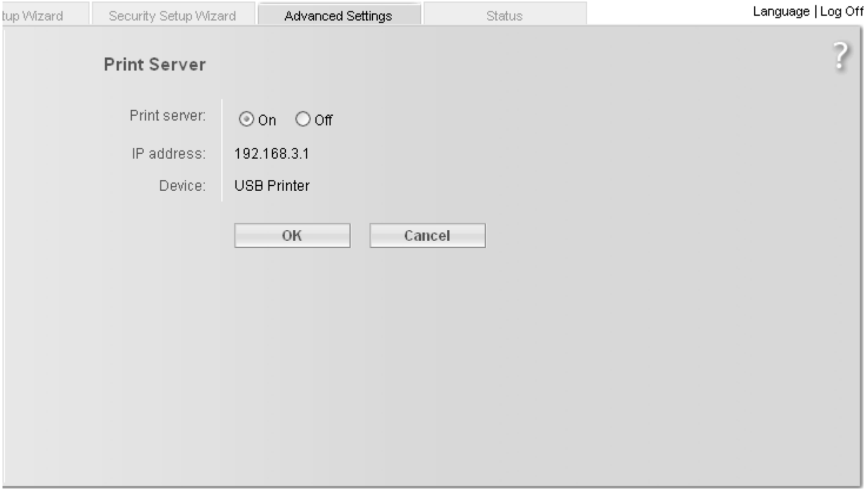
Print Server

Your device's integrated print server allows you to offer a USB printer to all users in the local network.

Note:
Not all functions of the print server may be supported in the case of special printers, especially combi devices (printers, scanners, faxes). You can obtain additional information by contacting the hotline or else on the Internet (see Quick Start Guide).

If you wish to use this function, you must first connect a USB printer to your device's USB port. The device must be shown on the screen. You can check the status of the connection to the USB printer in the ***Advanced Settings*** – ***USB*** menu entry.

→ Activate your device's integrated print server.



Print Server

Print server: ● On ○ Off

IP address: 192.168.3.1

Device: USB Printer

Users can set up the connected printer by entering the current IP address of the Gigaset SX763 WLAN dsl on the PC.

→ Click ***OK*** to save the changes.

You will find information on setting up a printer connected to the Gigaset SX763 WLAN dsl in Section "Installing the printer port for network printers" on page 123.

Call guide

Your Gigaset SX763 WLAN dsl allows you to make calls via the Internet (VoIP) and your fixed line. A description of how to configure your Gigaset SX763 WLAN dsl for using the telephone functions is provided in sections "Telephony" on page 40 and "Setting up Internet telephony (VoIP)" on page 87.

This chapter describes the function keys on your phone and the Internet telephony settings with which you can use the various telephony options. Please note that the functions described are only fully available if you have configured Internet telephony and have registered with your service provider.

External connections are calls via your fixed line or via the Internet (VoIP).

Internal connections are calls between the phones connected to the router or calls on PCs or cordless phones, which are registered as software SIP clients on the device.

Making calls

Key combination	Effect	Description
***1 ...*6**	Call for an internal extension	Choose the phone number of the desired extension (analogue phone or SIP extension, *1,..*6) to make an internal call.
**	Call for all internal numbers	Choose ** to call all internal extensions.
99	Answer a call from a different phone	If a call arrives at a different telephone set or on a port configured as an answering machine, you can accept this call on your phone by pressing the key combination ***99***.
***31#number**	Calling line identification restriction	Dial *31# before the number if you want to prevent your number being displayed to the other party for the current call.
***51#**	Calling line identification restriction as default	Dial 51# to prevent your number being displayed to the other party permanently.
#51#	Cancel calling line identification restriction as default	You have opted to suppress the display of your number by default (see above): Dial #51# to cancel this default.

Advanced options

The functions described in this section, which are available to you when making calls via your Gigaset SX763 WLAN dsl, apply both for external calls and for internal calls.

Toggling telephone calls

Key combination	Effect	Description

`R`
`Phone number`
	Consultation	Press **`R`** to initiate a consultation with another phone number during a call.
		Dial the desired (internal or external) number for the consultation.

R2	Accept call waiting/ toggle between two calls	Press **`R2`** to accept an incoming call during a call. The connection to the first call is put on hold. If you terminate the first call beforehand, your phone rings and you can take the second call as usual. By pressing **`R2`** again, you can toggle to the waiting caller.
R0	Reject call waiting	Press **`R0`** to reject an incoming call during a call. The second caller then hears the busy tone. The second call is rejected automatically after 30 seconds has elapsed.
R1	End a call	Press **`R1`** to end the current call. You then switch to the waiting call. The second call is ended automatically when you replace the receiver.

Conference call between three participants

Key combination	Effect	Description
R3	Conference call	When you are making a call and a second call is waiting (see above), press **R3** to enable a conference call between you and the two call parties.
R2	End the conference call and continue calls separately	Press **R2** to end the conference call. You are then connected to the previously active call again and the previous waiting call is now in the wait state again.
R4	End conference call and set up the connection between call parties	If you press **R4** during a conference call, you end your call and set up a connection between the other two call parties. You can then replace the receiver. In the case of an internal conference call, you simply need to hang up.
	End conference call	Replace the receiver to terminate all calls.

Call answering and forwarding

Key combination	Effect	Description
`*21*[number]#`	Forward to **internal** phone number	Dial **`*21*`** and the desired internal phone number to which all calls are to be forwarded that are received on this extension and then press the **#** key.
`#21#`	Delete call forwarding	Use the key combination **`#21#`** to delete internal call forwarding, which you set up as described above.
`*61*[number]#`	Call forwarding to internal number if absent	Dial **`*61*`** and the desired internal phone number to which all calls are to be forwarded that are received on this extension and then press the **#** key. The call is forwarded after 20 seconds with this key combination.
`#61#`	Delete call forwarding if absent	Use the key combination **`#61#`** to delete internal call forwarding (if absent), which you set up as described above.
`*67*number#`	Call forwarding to internal number if line busy	Dial **`*67*`** and the desired internal phone number to which all calls are to be forwarded that are received on this extension and then press the **#** key. The call is forwarded with this key combination if the line is busy.
`#67#`	Delete call forwarding if absent	Use the key combination **`#67#`** to delete internal call forwarding (if line busy), which you set up as described above.
`#77#`	Delete all call forwarding settings	Use the key combination **`#77#`** to delete all call forwarding settings described above.

Call waiting and call reject if busy

***43#**	Allow call waiting	Use the key combination ***43#** to allow call waiting when the line is busy.
#43#	Delete call waiting	Dial **#43#** to disable call waiting if busy again.
***26#**	Reject calls	Use the key combination ***26#** to specify that calls are to be rejected.
#26#	Delete the reject call if busy setting	Use the key combination **#26#** to delete the reject call setting.

Administration

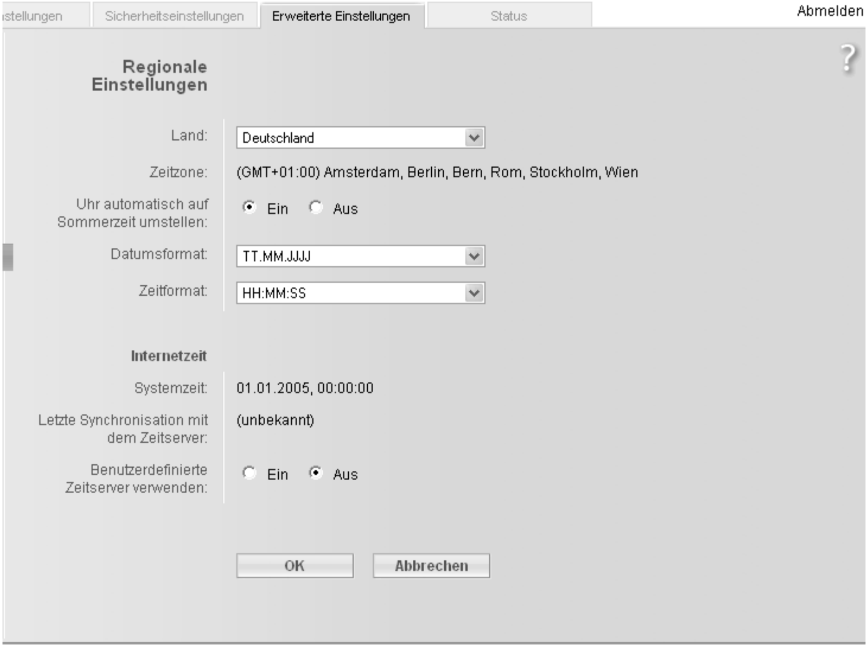
The Gigaset SX763 WLAN dsl user interface includes several helpful functions for administration. You can:

- Make regional settings (see below)
- Change the system password (page 105)
- Set up system management (page 106)
- Back up and, if necessary, restore configuration data (page 107)
- Gigaset SX763 WLAN dsl Reset to the factory settings (page 108)
- Reboot the device (page 108)
- Update firmware (page 109)
- Make the settings for the system log (page 110)
- View information about the configuration and status of the Gigaset SX763 WLAN dsl (page 111)

Regional Options

For operating your Gigaset SX763 WLAN dsl, you can select the location, time zone and format for entering the time and date, and you can also configure a time server for the Internet time (system time).

→ In the ***Advanced Settings*** – ***Administration*** menu, select ***Regional Options***.



Regionale Einstellungen

Land: Deutschland

Zeitzone: (GMT+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

Uhr automatisch auf Sommerzeit umstellen: ● Ein ○ Aus

Datumsformat: TT.MM.JJJJ

Zeitformat: HH:MM:SS

Internetzeit

Systemzeit: 01.01.2005, 00:00:00

Letzte Synchronisation mit dem Zeitserver: (unbekannt)

Benutzerdefinierte Zeitserver verwenden: ○ Ein ● Aus

→ Select the country you are currently in from the list. You can set the time so that it automatically switches to summer time or the ***Time zone***, as required.

If you have already configured the basic settings, you can change these here.

→ Select the required option or choose the ***Time zone*** for your location.

→ Select the required format for entering the date and time from the ***Date format*** and ***Time format*** lists.

Internet Time

The ***System time*** of the device is automatically synchronised with the time server on the Internet. The time of the ***Last synchronization with time server*** is displayed for your information.

→ If you would like to use your own time server, activate the ***On*** option next to the ***Use custom time servers*** field.

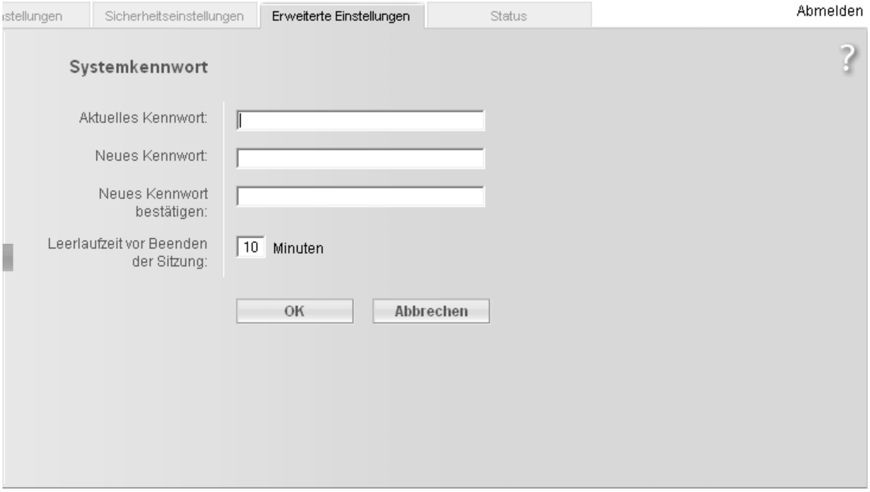
→ Enter the Internet address of the time server in the ***Preferred time server*** or ***Alternate time server*** fields.

→ Click ***OK*** to apply the settings.

System Password

You can assign a System Password to the Gigaset SX763 WLAN dsl user interface and specify the period after which a session is to be automatically ended if no further entry is made.

→ In the ***Advanced Settings*** – ***Administration*** menu, select ***System Password***.



Systemkennwort

Aktuelles Kennwort:

Neues Kennwort:

Neues Kennwort bestätigen:

Leerlaufzeit vor Beenden der Sitzung: 10 Minuten

After installation, the Gigaset SX763 WLAN dsl user interface is protected by the System Password **admin**. To prevent unauthorised changes being made to the configuration, you should set a new System Password from time to time. You may already have set a System Password when you set up the ***Security Setup Wizard***. If so, you can change it here.

➡ Enter the old System Password in the ***Current password*** field.

➡ Enter a new system password in the ***New password*** field and repeat it in the ***Confirm new password*** field.

The System Password may contain up to 20 characters. The System Password is case sensitive. Avoid proper names and all too obvious words. Use a combination of letters, digits and special characters.

Note

If you forget your System Password, you have to reset the Gigaset SX763 WLAN dsl (page 20). This returns **all** your settings to the factory configuration. This means the system password is changed back to **admin**.

Idle time before log off setting:

➡ Enter the number of minutes after which the configuration program is to be ended if no further entry is made. The default setting is 10 minutes. If you enter 0, the program will never be ended automatically.

➡ Click ***OK*** to apply the settings.

System management

Your Gigaset SX763 WLAN dsl offers you the possibility of using phone-based management in addition to the configuration program that you access via a PC in your local network.

Using the ***Phone-based Management*** option, you can configure and monitor specific functions of your Gigaset SX763 WLAN dsl, for example the wireless network via a telephone connected to an extension.

➡ Activate the ***Phone-based Management*** function.

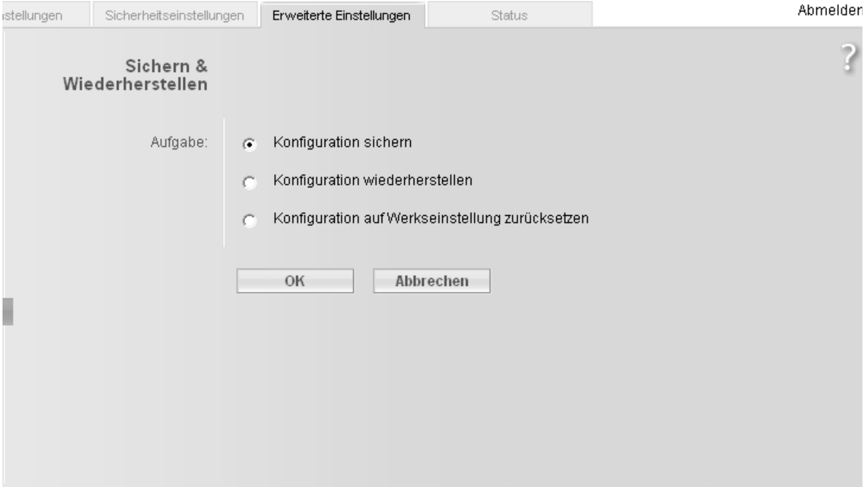
➡ Click ***OK*** to apply the settings.

Backing up and restoring a configuration

When the Gigaset SX763 WLAN dsl has been configured, it is recommended that you back up the settings. This means you can restore the settings at any time if they are accidentally deleted or overwritten.

You can also reset the configuration to the factory settings. You should always do this before handing the device to an external person.

◆ In the ***Advanced Settings*** – ***Administration*** menu, select ***Save & Restore***.



Sichern & Wiederherstellen

Aufgabe:

● Konfiguration sichern

○ Konfiguration wiederherstellen

○ Konfiguration auf Werkseinstellung zurücksetzen

Backing up configuration data

→ For ***Task,*** activate the ***Save configuration*** option.

You can then set the location in which the backup file is to be saved in a file selection window.

→ Select a local directory on your PC where you want to save the configuration file and enter a file name.

→ Click ***Save***.

The current configuration data is now saved in the specified file.

Restoring the saved data

→ For ***Task,*** activate the ***Restore configuration*** option.

→ In the file system, select the backup file that you want to use to restore the configuration.

A window will appear, prompting you to confirm the procedure.

→ Click ***OK***. The configuration will now be updated.

Restoring factory settings

You can reset the Gigaset SX763 WLAN dsl to the factory settings. You should do this before making the device available to others or exchanging it through the dealer. Otherwise unauthorised persons may use the Internet access data at your expense.

→ Select ***Reset configuration to factory default settings*** and click ***OK***.

A window will appear, prompting you to confirm the procedure.

Note:

If the Gigaset SX763 WLAN dsl is not operating properly, you can reboot it. It should then be ready for use again (page 20).

Please remember that when the device is fully reset, **all** the configuration settings are returned to the factory settings. This means that you will have to completely reconfigure the Gigaset SX763 WLAN dsl.

Reboot

If the Gigaset SX763 WLAN dsl is not operating properly, you can reboot it. It should then be ready for use again.

In the ***Administration*** menu, select ***Reboot***.

Click ***OK*** to reboot the device.

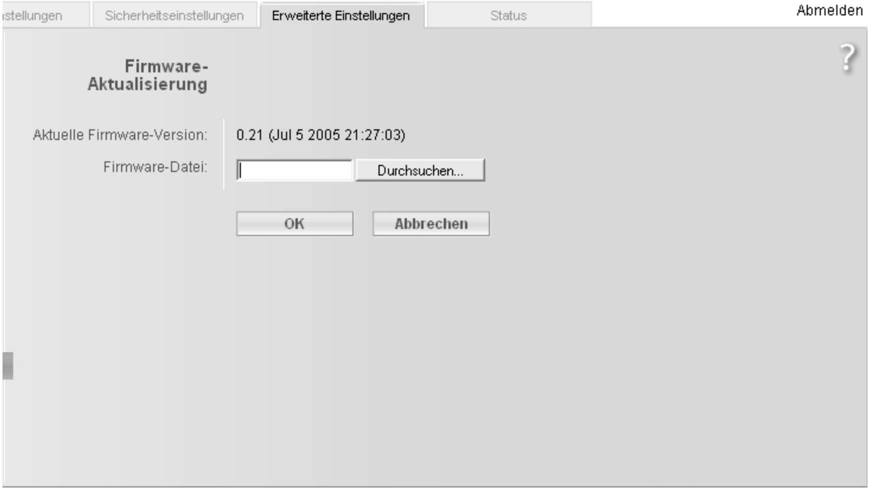
Updating firmware

If Siemens or your Internet service provider release a new version of the firmware, you can update the firmware of the Gigaset SX763 WLAN dsl. To do this you must first load the new firmware onto your PC.

Carry out the following steps:

→ End all network activities in the local network.

→ In the ***Advanced Settings*** – ***Administration*** menu, select ***Firmware Update***.



Firmware-Aktualisierung

Aktuelle Firmware-Version: 0.21 (Jul 5 2005 21:27:03)

Firmware-Datei:

The firmware version that is currently installed on the device is displayed in the ***Current firmware version*** line.

→ In the ***Firmware update file*** field, enter the file with the new firmware that you have downloaded from the Internet or click ***Browse*** to search for the file in your PC's file system.

→ Click ***OK***. The firmware will now be updated.

Warning:

Do not turn off the Gigaset SX763 WLAN dsl during the updating procedure and do not interrupt the power supply. Turning off the device can make it unusable. The update can take several minutes.
Siemens Home and Office Communication Devices GmbH & Co. KG accepts no liability for damage that occurs through improper use.

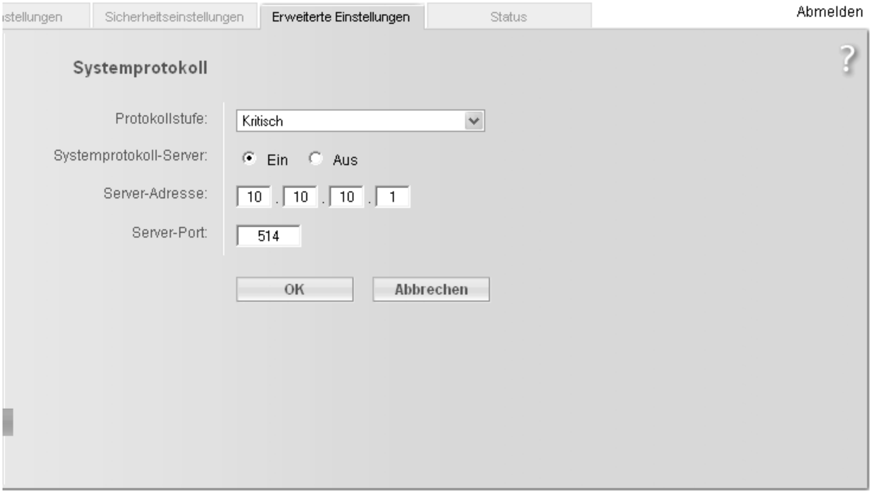
After a successful update, the device is automatically rebooted. All LEDs go out. The login screen is displayed again.

To see whether the upgrade procedure was successfully completed, check the current software version displayed in the overview of the ***Status*** menu (page 112).

System Log

The System Log is displayed in the ***Status*** – ***Device*** menu. It contains important information about how the device functions and possible problems. This information can also be automatically transferred to a system log server.

→ In the ***Advanced Settings*** – ***Administration*** menu, select ***System Log*** to make the settings for the log:



Systemprotokoll

Protokollstufe: Kritisch

Systemprotokoll-Server: ● Ein ○ Aus

Server-Adresse: 10 . 10 . 10 . 1

Server-Port: 514

→ ***Log level***: Specify how much information is to be contained in the system log. You can choose between four levels:

– ***Critical***: Log file of the most important information for possible device functionality problems

– ***Debugging***: Complete and detailed information on all device functions

– ***Warning*** and ***Informational*** are intermediate levels.

→ ***System log server***

– Activate this function if the device system log is to be automatically transferred to a system log server in the local network.

– ***Server address***:
Enter the IP address for the system log server.

– ***Server port***:
Enter the port of the system log server that is to be used to transfer the system log.

→ Click ***OK*** to save and apply the changes.

Status information

Information about configuration and the status of the Gigaset SX763 WLAN dsl is displayed in the ***Status*** of the Gigaset SX763 WLAN dsl. On the first screen you will find an overview of the status of the Internet connection, the local and wireless networks and the device.

Detailed information is available on the following status screens:

- ***Security***
- ***Internet***
- ***Local Network***
- ***Wireless Network***
- ***Telephony***
- ***Device***

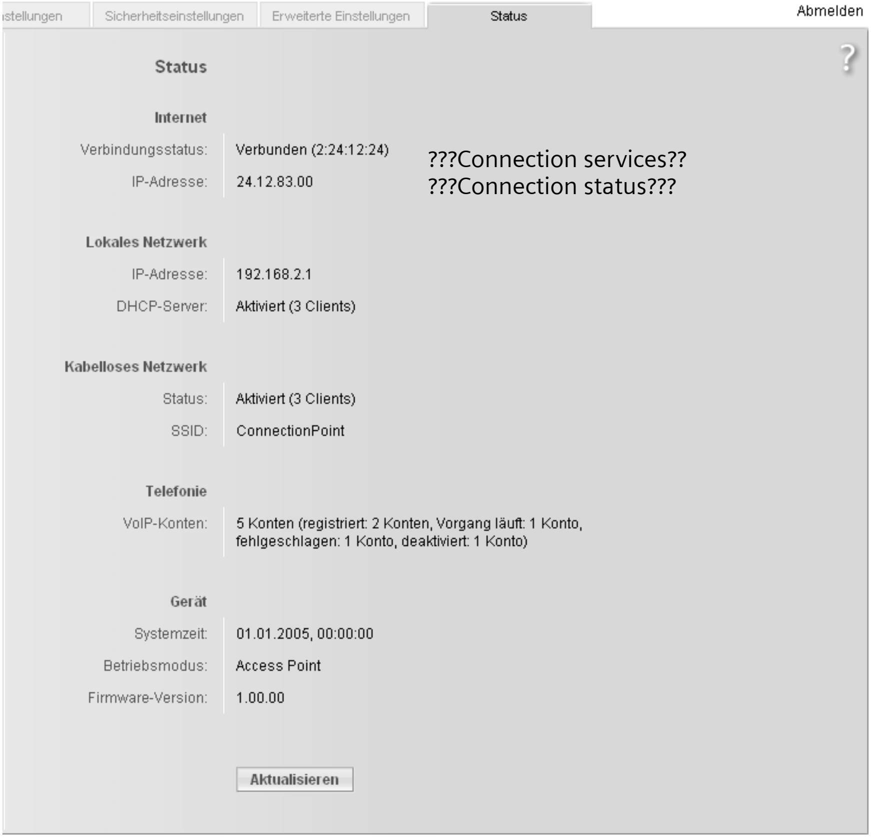
To display a status screen:

→ Select ***Status*** on the start screen.

→ Select the entry with the information you require.

Overview

On the first screen you will find an overview of the current operating status and the most important device data.



Status

Internet

Verbindungsstatus: Verbunden (2:24:12:24)

IP-Adresse: 24.12.83.00

???Connection services??
???Connection status???

Lokales Netzwerk

IP-Adresse: 192.168.2.1

DHCP-Server: Aktiviert (3 Clients)

Kabelloses Netzwerk

Status: Aktiviert (3 Clients)

SSID: ConnectionPoint

Telefonie

VoIP-Konten: 5 Konten (registriert: 2 Konten, Vorgang läuft: 1 Konto, fehlgeschlagen: 1 Konto, deaktiviert: 1 Konto)

Gerät

Systemzeit: 01.01.2005, 00:00:00

Betriebsmodus: Access Point

Firmware-Version: 1.00.00

Internet

- ***Connection status***

  The status of the Internet connection and, if connected, the duration of the connection.

- ***IP address***

  The public IP address of the device.

Local network

- ***IP address***

  The local IP address of the device.

- ***DHCP Server***

  The status of the DHCP server of the device and, if activated, the number of clients in the network that have been assigned an IP address.

Wireless network

- ***Status***

  The status of the wireless network connection of the device and, if activated, the number of clients in the wireless network connected to the device.

- ***SSID***

  The wireless network ID.

- ***Telephony***

  Shows the status and the data of the VoIP accounts.

Device

- ***System time***

  The system time of the device.

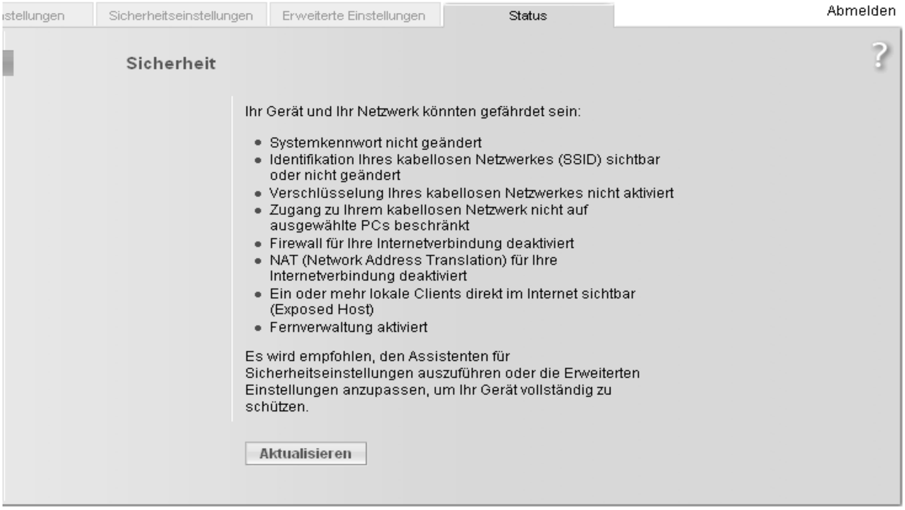
- ***Firmware version***

  The firmware version currently installed on the device.

➛ Click ***Refresh*** to refresh this screen and update the displayed data.

Security

You will find information about possible security risks for the device and the network on the ***Security*** screen in the ***Status*** menu.



Sicherheit

Ihr Gerät und Ihr Netzwerk könnten gefährdet sein:

- Systemkennwort nicht geändert
- Identifikation Ihres kabellosen Netzwerkes (SSID) sichtbar oder nicht geändert
- Verschlüsselung Ihres kabellosen Netzwerkes nicht aktiviert
- Zugang zu Ihrem kabellosen Netzwerk nicht auf ausgewählte PCs beschränkt
- Firewall für Ihre Internetverbindung deaktiviert
- NAT (Network Address Translation) für Ihre Internetverbindung deaktiviert
- Ein oder mehr lokale Clients direkt im Internet sichtbar (Exposed Host)
- Fernverwaltung aktiviert

Es wird empfohlen, den Assistenten für Sicherheitseinstellungen auszuführen oder die Erweiterten Einstellungen anzupassen, um Ihr Gerät vollständig zu schützen.

◆ ***System password not changed***
The configuration program of the device is not sufficiently protected against unauthorised access either because you have not changed the system password since setting up the device or you have not assigned any system password at all. Information on how to avoid this security risk is given in Section "System Password" on page 105.

◆ ***Identification of your wireless network visible or not changed***
Unauthorised users can also find the wireless network easily as you have not changed the ID of the wireless network (SSID) since setup and have not deactivated SSID broadcasting. Information on how to avoid this security risk is given in Section "Configuring wireless connections" on page 77.

◆ ***Encryption for your wireless network not activated***
None of the data in the wireless network is encrypted during transfer and can therefore easily be intercepted. Unauthorised users will also have easy access to your network, your PCs and your Internet connection. Information on how to avoid this security risk is given in Section "Setting up wireless security" on page 80.

◆ ***Access to your wireless network not restricted to allowed clients***
Users can access the wireless network from any PC. Information on how to avoid this security risk is given in Section "Permitted clients" on page 85.

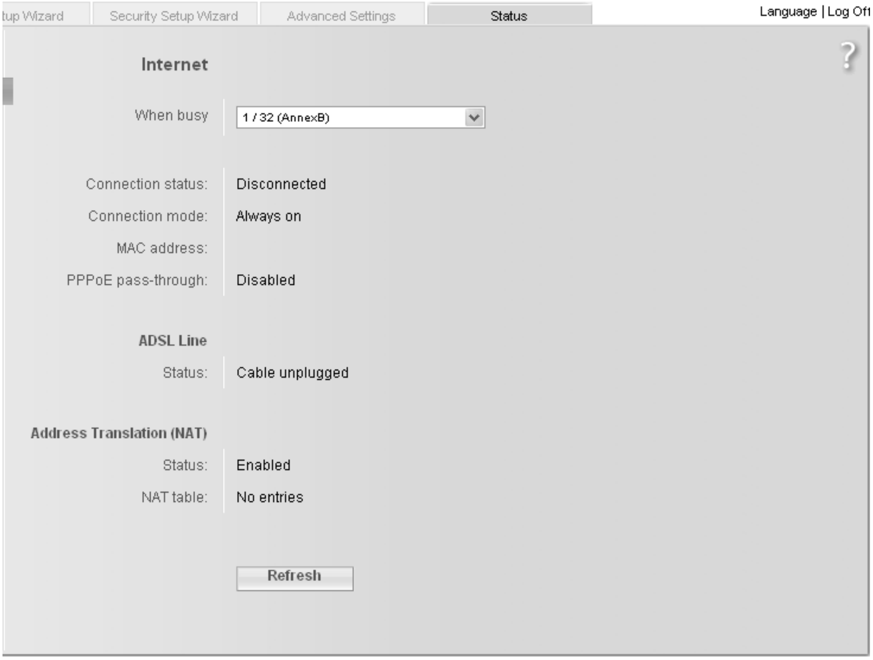
◆ ***Firewall for your Internet connection turned off***
The network is not protected against hackers who gain unauthorised access via the Internet. Information on how to avoid this security risk is given in Section "Firewall" on page 62.

- ***Address translation for your Internet connection turned off***
  The clients in the network are not protected against unauthorised access via the Internet. Information on how to avoid this security risk is given in Section "Setting up the NAT function" on page 66.
- ***One or more of your local clients directly exposed to the Internet***
  At least one client in the network is directly visible on the Internet as an exposed host and is therefore particularly exposed to the risk (e.g. through hacker attacks). Only activate this function if it is absolutely necessary (e.g. to operate a Web server) and other functions (e.g. Port forwarding) are not suitable. In this case, you should take the appropriate measures on the clients concerned. Information on how to avoid this security risk is given in Section "Opening the firewall for selected PCs (Exposed Host)" on page 69.

→ Click ***Refresh*** to refresh the screen and the displayed data.

Internet

You will find information about the status of the Internet connection of the device on the ***Internet*** screen in the ***Status*** menu.



Internet

When busy: 1 / 32 (AnnexB)

Connection status: Disconnected

Connection mode: Always on

MAC address:

PPPoE pass-through: Disabled

ADSL Line

Status: Cable unplugged

Address Translation (NAT)

Status: Enabled

NAT table: No entries

- ***Connection service***
  You can select the ***Connection service,*** for which the following information is to be displayed.
- ***Connection status***
  Shows the status of the Internet connection and, if connected, the duration of the connection. If you have set ***Connect on demand*** or ***Connect manually*** as the connection mode (page 56), you can ***Connect*** or ***Disconnect*** the connection to the Internet manually here.
- ***Connection mode***
  Shows the connection mode set for connecting to the Internet.
- ***MAC address***
  Shows the public MAC address of the device.
- ***PPPoE pass-through***
  Shows the status of PPPoE pass-through for the DSL or cable connection for establishing an Internet connection directly between a PC and the network.

- ***ADSL Line***
  - ***Status***

    The status of the cable connection from your device to your DSL port.
  - ***Line mode***

    The current line mode used by your DSL port.
  - ***Maximum line rate***

    The maximum possible data transfer rate of your DSL port for incoming and outgoing data traffic.
  - ***Noise margin***

    The maximum signal-to-noise ratio of your DSL port for incoming and outgoing data traffic.
  - ***Line attenuation***

    The line attenuation of your DSL port for incoming and outgoing data traffic.
  - ***Output power***

    The output power of your DSL port for incoming and outgoing data traffic.
- ***Address Translation (NAT)***
  - ***Status***

    Shows the status of the NAT (Network Address Translation) for the Internet connection.
  - ***NAT table***

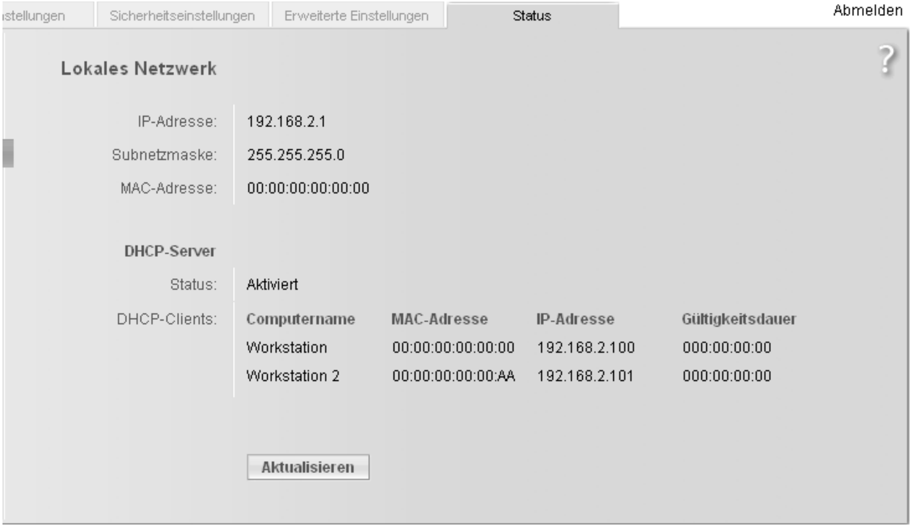
    Shows the current number of entries in the NAT table.

    Click ***Empty*** to delete all the current entries in the NAT table.

→ Click ***Refresh*** to refresh this screen and update the displayed data.

Local Network

You will find information about the local network settings on the ***Local Network*** screen in the ***Status*** menu.



Lokales Netzwerk

IP-Adresse: 192.168.2.1

Subnetzmaske: 255.255.255.0

MAC-Adresse: 00:00:00:00:00:00

DHCP-Server

Status: Aktiviert

DHCP-Clients:

Computername	MAC-Adresse	IP-Adresse	Gültigkeitsdauer
Workstation	00:00:00:00:00:00	192.168.2.100	000:00:00:00
Workstation 2	00:00:00:00:00:AA	192.168.2.101	000:00:00:00

- ***IP address***

  Shows the local IP address of the device.

- ***Subnet mask***

  Shows the subnet mask used in the local network.

- ***MAC address***

  Shows the local MAC address of the device for wired data transfer.

- ***DHCP Server***

  – ***Status***

    Shows the status of the DHCP server of the device for automatic assignment of IP addresses to clients in the local network.

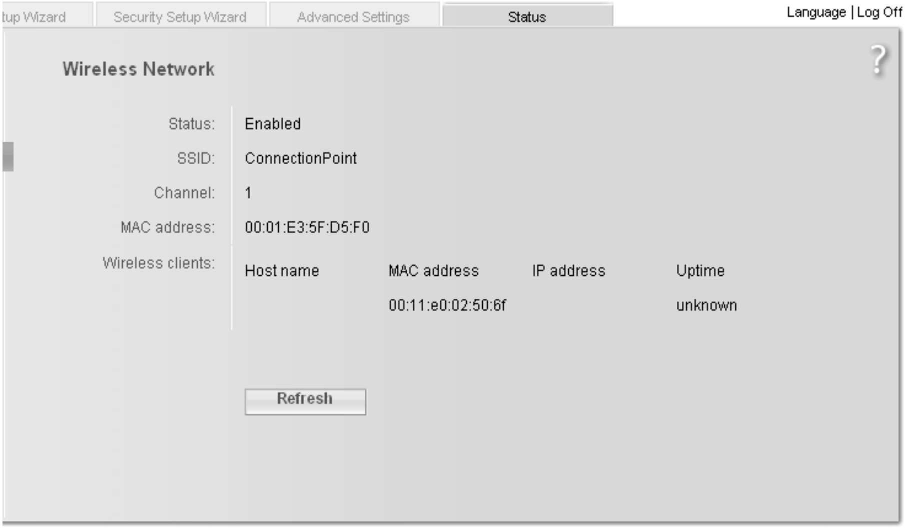
- ***DHCP clients***

  Shows all the clients in the network that have been assigned an IP address. The ***Host name*** and the ***MAC address*** are listed as identification for each client. You are also given information about the ***IP address*** assigned to each client and about the ***Lease time*** remaining for the IP address before the client will be assigned a new address by the DHCP server.

→ Click ***Refresh*** to refresh this screen and update the displayed data.

Wireless Network

You will find information about the wireless network settings on the ***Wireless Network*** screen in the ***Status*** menu.



Wireless Network

Status: Enabled

SSID: ConnectionPoint

Channel: 1

MAC address: 00:01:E3:5F:D5:F0

Wireless clients:

Host name	MAC address	IP address	Uptime
	00:11:e0:02:50:6f		unknown

- ***Status***

  Shows the status of the connection between the device and the wireless network.

- ***SSID***

  Shows the wireless network ID.

- ***Channel***

  Shows the radio channel that is currently being used for data transfer in the wireless network.

- ***MAC address***

  Shows the local MAC address of the device for wireless data transfer.

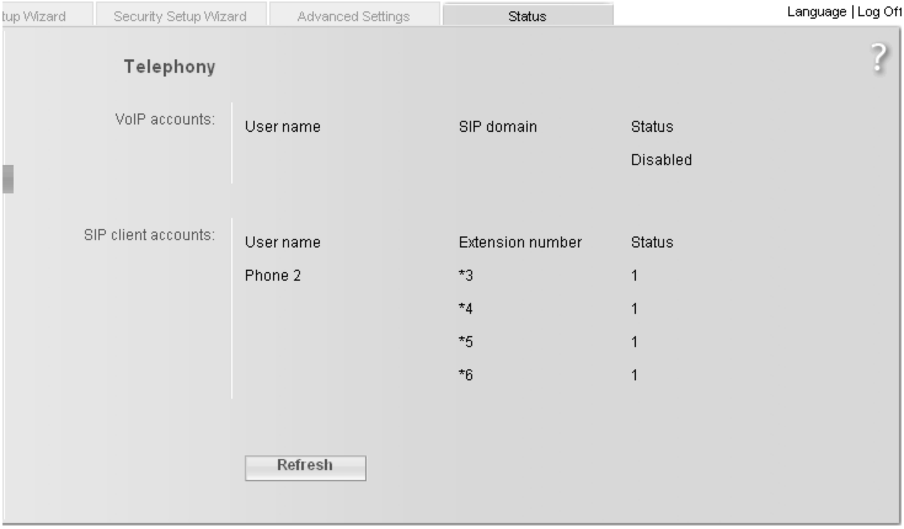
- ***Wireless clients***

  Shows all clients in the wireless network that are currently connected to the device. The ***Host name***, ***MAC address*** and ***IP address*** are specified for identifying each client. You will also see information about the ***Uptime*** to date of the current connection for each client in the wireless network.

→ Click ***Refresh*** to refresh this screen and update the displayed data.

Telephony

You will find information about the VoIP accounts and a statistic of the phone calls on the ***Telephony*** screen in the ***Status*** menu.



Telephony

VoIP accounts:

User name	SIP domain	Status
		Disabled

SIP client accounts:

User name	Extension number	Status
Phone 2	*3	1
	*4	1
	*5	1
	*6	1

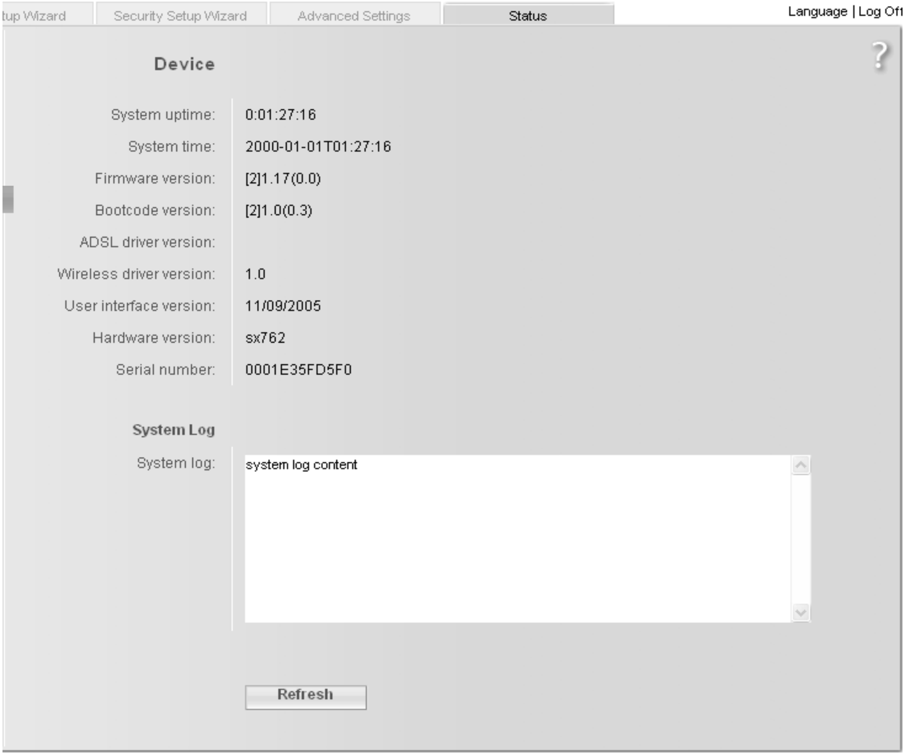
- ***VoIP accounts***
  Shows the data and the status of the VoIP accounts.
- ***SIP client accounts***
  All WLAN handsets currently set up as extensions or other SIP clients in your local network are displayed. The user name and internal phone number of each SIP user account are displayed for identification purposes. In addition, you are shown information about the status of the respective account.

→ Click ***Refresh*** to refresh this screen and update the displayed data.

Device

Note:
All data will be lost if there is a power failure.

You will find information about the most important device data on the ***Device*** screen in the ***Status*** menu.



Device

System uptime: 0:01:27:16
System time: 2000-01-01T01:27:16
Firmware version: [2]1.17(0.0)
Bootcode version: [2]1.0(0.3)
ADSL driver version:
Wireless driver version: 1.0
User interface version: 11/09/2005
Hardware version: sx762
Serial number: 0001E35FD5F0

System Log

System log: system log content

- ***System uptime***
  Show's your device's operating time since the last time the system was started.
- ***System time***
  Shows the system time for your device.
- ***Firmware version***
  Shows the firmware version currently installed on your device.
- ***Bootcode version***
  Shows the version of the bootcode currently installed on your device.
- ***Wireless driver version***
  Shows the version of the WLAN driver currently installed on your device.

- ***Hardware version***

  Shows your device's hardware version.

- ***Serial number***

  Shows your device's serial number.

- ***System Log***

  The system log contains important information about how the device functions and possible problems. You can edit the scope of the system log to suit your requirements (see "System Log" on page 110).

➡ Click ***Refresh*** to refresh this screen and update the displayed data.

Installing the printer port for network printers

Your Gigaset SX763 WLAN dsl is equipped with a USB port that you can use, for example, to connect a printer for use as the network printer.

Introduction

A network printer is a printer on which you can print your documents without it being connected to your PC, for example to LPT1, the parallel interface. The advantage of this is that you only need this printer once in your network. All PCs for which it is released can access it and work with it.

Note:

For multifunction devices (combination of printer, copier or fax) only the printer functionality is supported.

In most cases a printer of this type is connected to another PC in the network. While this offers the advantage referred to above, it has serious disadvantages:

- The printer can only be used by others if the PC to which it is connected is switched on.
- The print job you send to the PC on which the printer depends reduces the performance (resources) of this PC.

If you use the USB port on the Gigaset SX763 WLAN dsl for your printer, you have all the advantages of a network printer without the disadvantages referred to above:

- The network, and consequently also the printer, is always ready (the Gigaset SX763 WLAN dsl and the printer itself must be switched on, of course).
- As it is connected to the USB printer port on your Gigaset SX763 WLAN dsl, it does not detract from the performance of any other PC in the network.

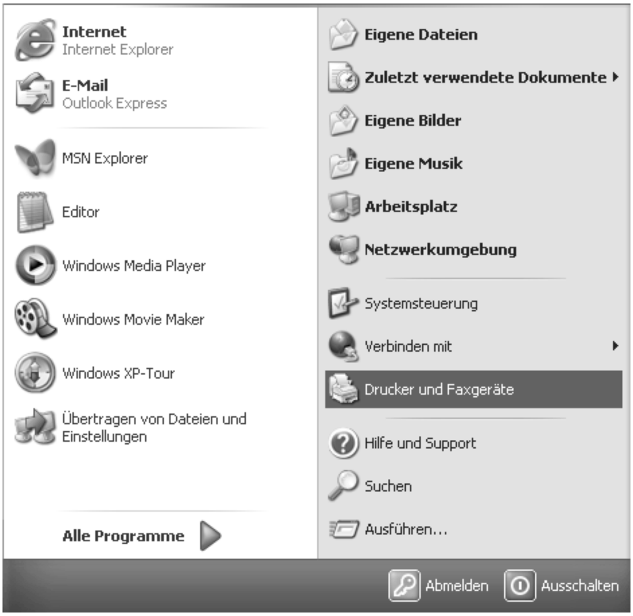
To facilitate this option you must first set up a **printer port** on each PC that is to use the network printer. A printer port is an interface on the PC that forwards the print job to an IP address within the network.

Once you have set up this port you must install the printer driver.

Installing a standard TCP/IP printer port under Windows XP/ 2000

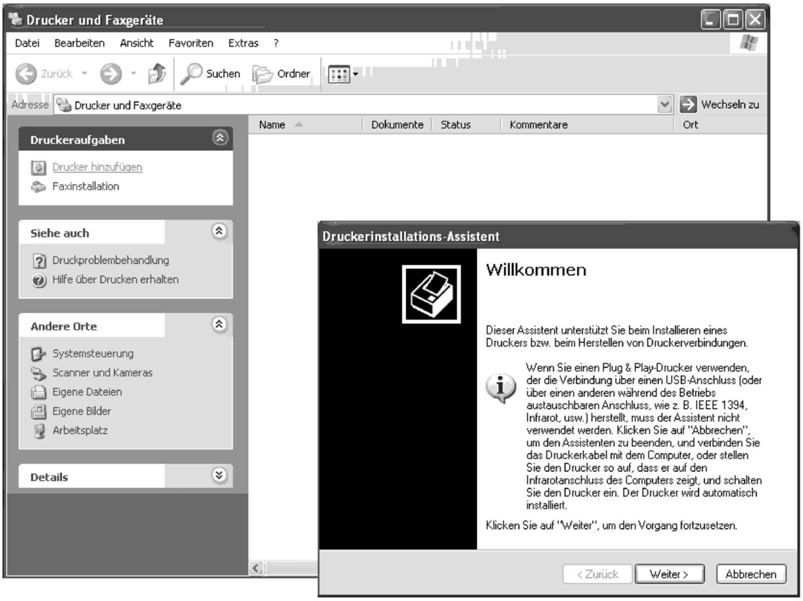
You can use the standard TCP/IP port driver available in this operating system. Make sure that the Gigaset SX763 WLAN dsl is connected and can be reached in the network. A printer need not be connected to the USB port on your Gigaset SX763 WLAN dsl at this point. The following illustrations show installation on Windows XP. Installation on Windows 2000 is essentially the same.

➞ Click ***Start*** and in the window that opens, click ***Printers and Faxes***.



➞ In the window that opens, double-click ***Add a printer***.

The wizard for installing a printer is opened.



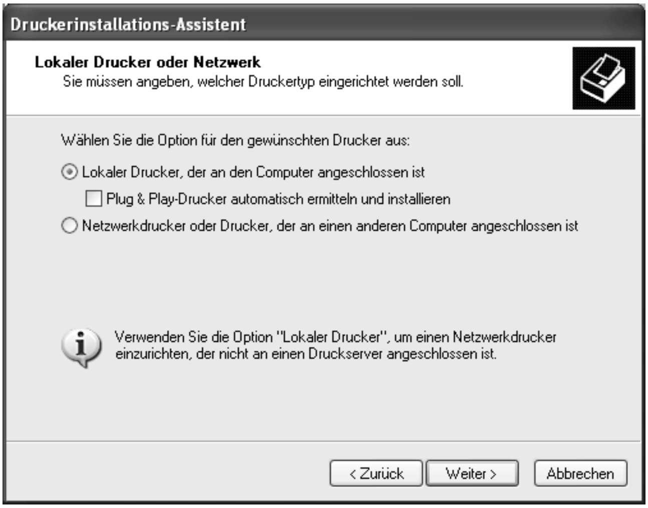
Willkommen

Dieser Assistent unterstützt Sie beim Installieren eines Druckers bzw. beim Herstellen von Druckerverbindungen.

Wenn Sie einen Plug & Play-Drucker verwenden, der die Verbindung über einen USB-Anschluss (oder über einen anderen während des Betriebs austauschbaren Anschluss, wie z. B. IEEE 1394, Infrarot, usw.) herstellt, muss der Assistent nicht verwendet werden. Klicken Sie auf "Abbrechen", um den Assistenten zu beenden, und verbinden Sie das Druckerkabel mit dem Computer, oder stellen Sie den Drucker so auf, dass er auf den Infrarotanschluss des Computers zeigt, und schalten Sie den Drucker ein. Der Drucker wird automatisch installiert.

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

→ In the Add Printer Wizard, click ***Next***.



Lokaler Drucker oder Netzwerk

Sie müssen angeben, welcher Druckertyp eingerichtet werden soll.

Wählen Sie die Option für den gewünschten Drucker aus:

● Lokaler Drucker, der an den Computer angeschlossen ist

□ Plug & Play-Drucker automatisch ermitteln und installieren

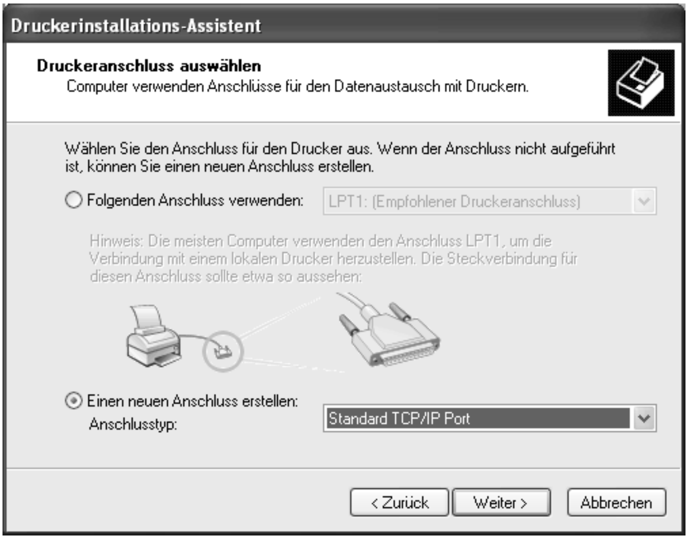
○ Netzwerkdrucker oder Drucker, der an einen anderen Computer angeschlossen ist

Verwenden Sie die Option "Lokaler Drucker", um einen Netzwerkdrucker einzurichten, der nicht an einen Druckserver angeschlossen ist.

The printer port you are installing will behave like an additional parallel port on the PC. For this reason you must click the option button next to ***Local printer*** in this window.

The ***Automatically detect and install my Plug and Play printer*** check box must not be selected.

→ Click ***Next***.



Druckerinstallations-Assistent

Druckeranschluss auswählen
Computer verwenden Anschlüsse für den Datenaustausch mit Druckern.

Wählen Sie den Anschluss für den Drucker aus. Wenn der Anschluss nicht aufgeführt ist, können Sie einen neuen Anschluss erstellen.

○ Folgenden Anschluss verwenden: LPT1: (Empfohlener Druckeranschluss)

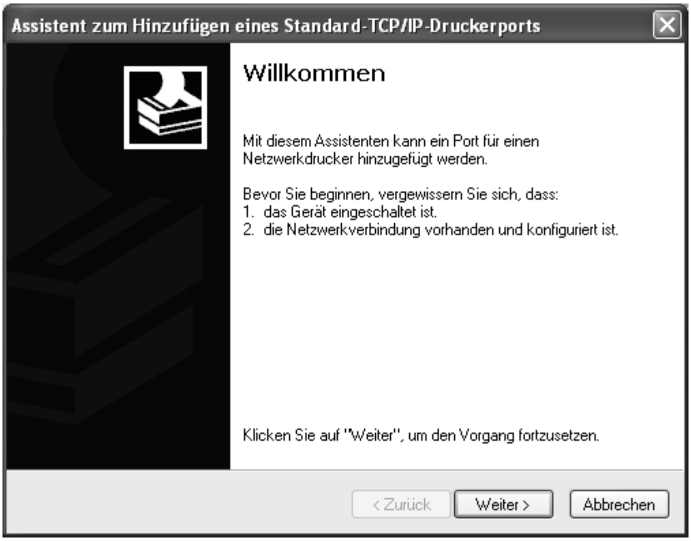
Hinweis: Die meisten Computer verwenden den Anschluss LPT1, um die Verbindung mit einem lokalen Drucker herzustellen. Die Steckverbindung für diesen Anschluss sollte etwa so aussehen:

● Einen neuen Anschluss erstellen:
Anschlusstyp: Standard TCP/IP Port

→ Click the ***Create a new port*** option button.

→ Then select ***Standard TCP/IP Port*** from the selection menu in the field next to this option.

→ Click ***Next***.



Assistent zum Hinzufügen eines Standard-TCP/IP-Druckerports

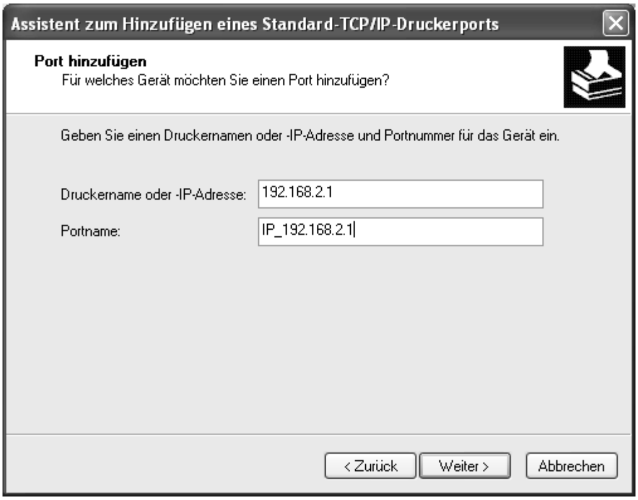
Willkommen

Mit diesem Assistenten kann ein Port für einen Netzwerkdrucker hinzugefügt werden.

Bevor Sie beginnen, vergewissern Sie sich, dass:
1. das Gerät eingeschaltet ist.
2. die Netzwerkverbindung vorhanden und konfiguriert ist.

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

→ In the wizard for setting up a standard TCPI/IP port, click ***Next***.


Assistent zum Hinzufügen eines Standard-TCP/IP-Druckerports
Port hinzufügen
Für welches Gerät möchten Sie einen Port hinzufügen?

Geben Sie einen Druckernamen oder -IP-Adresse und Portnummer für das Gerät ein.

Druckername oder -IP-Adresse: 192.168.2.1

Portname: IP_192.168.2.1

< Zurück
Weiter >
Abbrechen

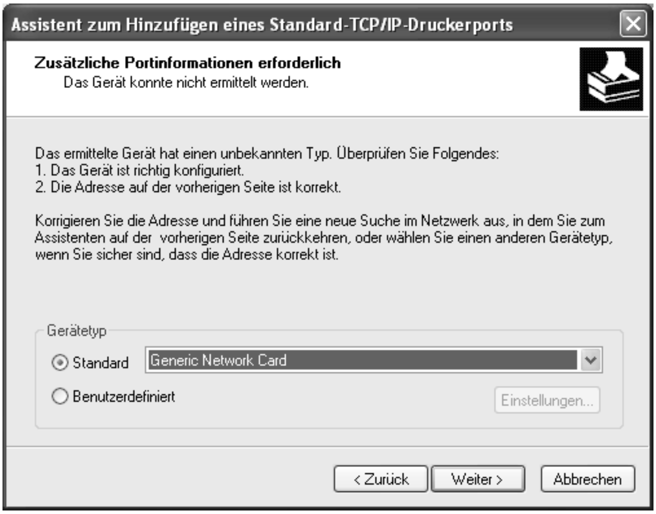
→ In the ***Printer Name or IP Address*** input field, enter the IP address of the print server (Gigaset SX763 WLAN dsl): e.g. 192.168.2.1.

A copy of your entry is displayed in the second field.

→ Double-click in the ***Port Name*** field and enter a name. This name will appear in the list of printer ports. Name this port, for example, **Gigaset_printerport**.

→ Click ***Next***.

As Windows XP usually first looks for a network card when a printer port is installed, the ***Additional Port Information Required*** window is displayed.


Assistent zum Hinzufügen eines Standard-TCP/IP-Druckerports
Zusätzliche Portinformationen erforderlich
Das Gerät konnte nicht ermittelt werden.

Das ermittelte Gerät hat einen unbekannten Typ. Überprüfen Sie Folgendes:
1. Das Gerät ist richtig konfiguriert.
2. Die Adresse auf der vorherigen Seite ist korrekt.

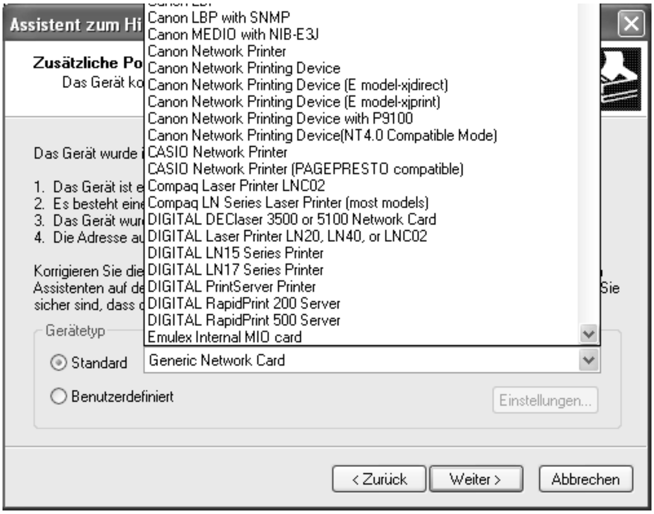
Korrigieren Sie die Adresse und führen Sie eine neue Suche im Netzwerk aus, in dem Sie zum Assistenten auf der vorherigen Seite zurückkehren, oder wählen Sie einen anderen Gerätetyp, wenn Sie sicher sind, dass die Adresse korrekt ist.

Gerätetyp

● Standard: Generic Network Card

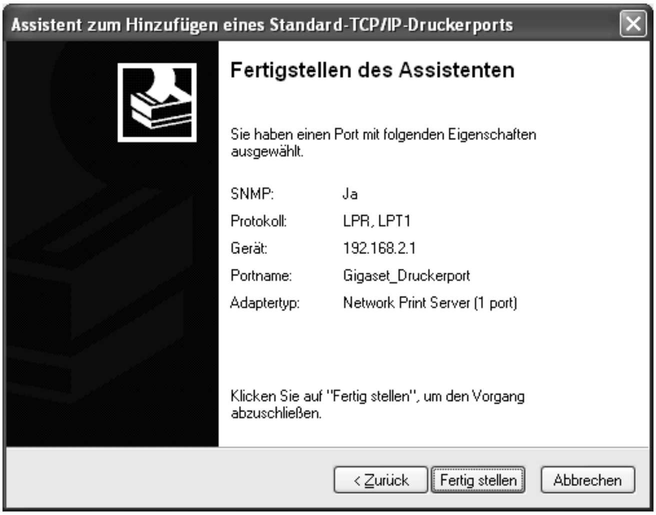
○ Benutzerdefiniert

→ From the list of standard device types, select the offered type ***Network Print Server (1 port)*** (print server with a printer port).


Assistent zum Hi
Zusätzliche Po
Das Gerät ko
Das Gerät wurde i
1. Das Gerät ist e
2. Es besteht eine
3. Das Gerät wur
4. Die Adresse au
Korrigieren Sie die
Assistenten auf de
sicher sind, dass d
Sie
Canon LBP with SNMP
Canon MEDIO with NIB-E3J
Canon Network Printer
Canon Network Printing Device
Canon Network Printing Device (E model-xjdirect)
Canon Network Printing Device (E model-xjprint)
Canon Network Printing Device with P9100
Canon Network Printing Device(NT4.0 Compatible Mode)
CASIO Network Printer
CASIO Network Printer (PAGEPRESTO compatible)
Compaq Laser Printer LNC02
Compaq LN Series Laser Printer (most models)
DIGITAL DEClaser 3500 or 5100 Network Card
DIGITAL Laser Printer LN20, LN40, or LNC02
DIGITAL LN15 Series Printer
DIGITAL LN17 Series Printer
DIGITAL PrintServer Printer
DIGITAL RapidPrint 200 Server
DIGITAL RapidPrint 500 Server
Emulex Internal MIO card
Gerätetyp
● Standard
Generic Network Card
○ Benutzerdefiniert
Einstellungen...
< Zurück
Weiter >
Abbrechen

→ Click ***Next***.

The window for finishing the wizard is opened and shows you all the settings you have made.


Assistent zum Hinzufügen eines Standard-TCP/IP-Druckerports

Fertigstellen des Assistenten

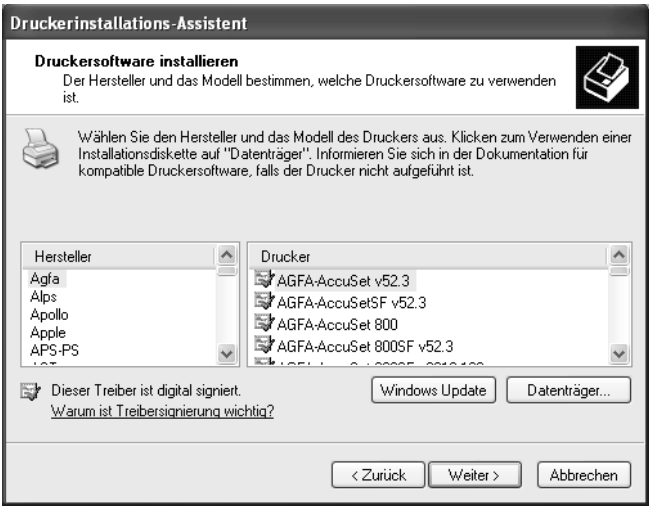
Sie haben einen Port mit folgenden Eigenschaften ausgewählt.

SNMP: Ja
Protokoll: LPR, LPT1
Gerät: 192.168.2.1
Portname: Gigaset_Druckerport
Adaptertyp: Network Print Server (1 port)

Klicken Sie auf "Fertig stellen", um den Vorgang abzuschließen.

→ Click ***Finish***.

Once the wizard for installing the printer port is finished, the ***Add Printer Wizard*** is opened.



Druckerinstallations-Assistent

Druckersoftware installieren

Der Hersteller und das Modell bestimmen, welche Druckersoftware zu verwenden ist.

Wählen Sie den Hersteller und das Modell des Druckers aus. Klicken zum Verwenden einer Installationsdiskette auf "Datenträger". Informieren Sie sich in der Dokumentation für kompatible Druckersoftware, falls der Drucker nicht aufgeführt ist.

Hersteller	Drucker
Agfa	AGFA-AccuSet v52.3
Alps	AGFA-AccuSetSF v52.3
Apollo	AGFA-AccuSet 800
Apple	AGFA-AccuSet 800SF v52.3
APS-PS	

Dieser Treiber ist digital signiert.

Warum ist Treibersignierung wichtig?

→ If you wish to install a printer for this port immediately, click ***Next*** and follow the instructions of the Add Printer Wizard.

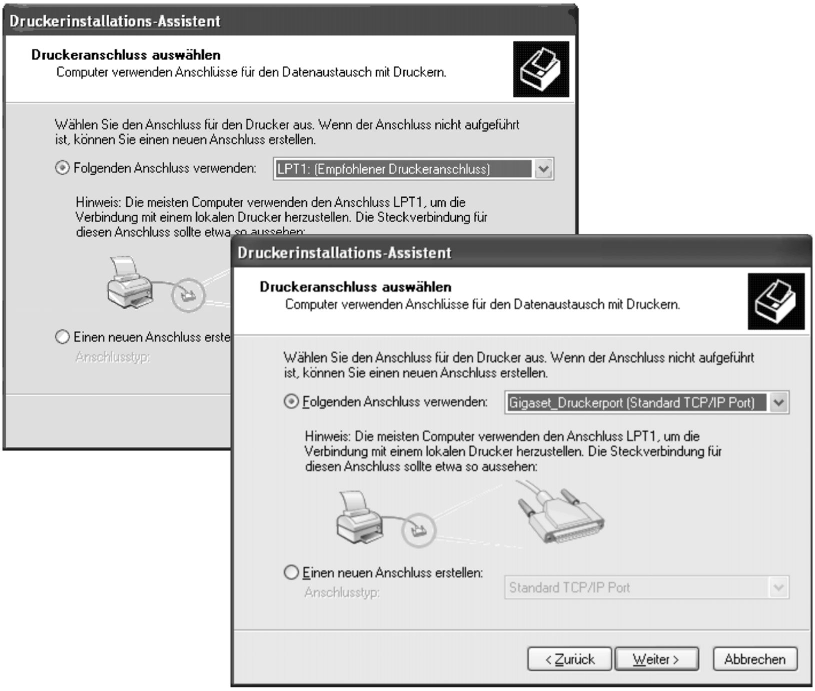
→ If you do not wish to install a printer until later, click ***Cancel***.

Note:

The print server of the Gigaset SX763 WLAN dsl does not work bidirectionally. It does not evaluate any of the printer's response messages. For this reason please make sure that your printer is also configured unidirectionally. You can make the relevant printer settings for your printer by choosing ***Start*** – ***Settings*** – ***Printers***.

Installing a printer on the TCP/IP port retrospectively

If you connect a printer to this port at a later stage, start the installation procedure for the printer port as above.



Druckerinstallations-Assistent

Druckeranschluss auswählen
Computer verwenden Anschlüsse für den Datenaustausch mit Druckern.

Wählen Sie den Anschluss für den Drucker aus. Wenn der Anschluss nicht aufgeführt ist, können Sie einen neuen Anschluss erstellen.

● Folgenden Anschluss verwenden: LPT1: (Empfohlener Druckeranschluss)

Hinweis: Die meisten Computer verwenden den Anschluss LPT1, um die Verbindung mit einem lokalen Drucker herzustellen. Die Steckverbindung für diesen Anschluss sollte etwa so aussehen:

○ Einen neuen Anschluss erste

Anschlusstyp:

Druckerinstallations-Assistent

Druckeranschluss auswählen
Computer verwenden Anschlüsse für den Datenaustausch mit Druckern.

Wählen Sie den Anschluss für den Drucker aus. Wenn der Anschluss nicht aufgeführt ist, können Sie einen neuen Anschluss erstellen.

● Folgenden Anschluss verwenden: Gigaset_Druckerport (Standard TCP/IP Port)

Hinweis: Die meisten Computer verwenden den Anschluss LPT1, um die Verbindung mit einem lokalen Drucker herzustellen. Die Steckverbindung für diesen Anschluss sollte etwa so aussehen:

○ Einen neuen Anschluss erstellen:
Anschlusstyp: Standard TCP/IP Port

- ➙ In this case, however, you should click the selection menu in the ***Select a Printer Port*** window.
- ➙ From the list, select the connection you have set up: e.g. ***Gigaset_printerport (Standard TCP/IP Port)***.
- ➙ Click ***Next*** and finish installing the printer driver as instructed in the windows that follow.

Installing a printer driver under Windows 98 SE or ME

The following section describes how to install a printer driver under the Windows 98 SE or ME operating systems as the procedure and windows shown for these operating systems are very similar. The printer driver does not need to be installed on Windows XP and 2000.

You have installed your network and it is ready for use.

- Insert the CD-ROM that was included with the delivery into the CD-ROM or DVD drive of your PC.
- Wait until the CD-ROM welcome window appears.
- Click Gigaset SX763 WLAN dsl.
- Click ***Printer Port Driver*** for Windows 98 SE or ME.

  The welcome window for installing the port driver is opened.
- Read the information it contains carefully.
- Click ***Next***.

  The necessary files are copied to your PC and executed. Once all the data has been transferred to your PC, you will be prompted to complete the installation of the port driver.
- Click ***Finish***.
- Reboot your PC.

You have now installed the printer port and effectively installed an extra printer port on your PC. **This port is universal**. You can control any printer that has a USB port via this port.

You must carry out this installation on every PC with Windows 98 or ME that is to use this printer in the network.

You might possibly still have to correct the IP address for the printer.

- Select ***Start*** – ***Settings*** – ***Printers***; select the printer and right-click to open the pop-up menu.
- Select ***Properties*** and open the ***Details*** tab.
- Select the port and click ***Connection Settings***.
- Change the IP address if necessary. It must be the same as that for the Gigaset SX763 WLAN dsl.

Instructions for setting up a printer on the PC

Once you have installed the printer port you still cannot start printing. The printer port is nothing more than an additional interface on your PC, comparable with the USB port. It means that any printer you install on this port is also regarded as a local printer even though it is located in the network and possibly not directly near you.

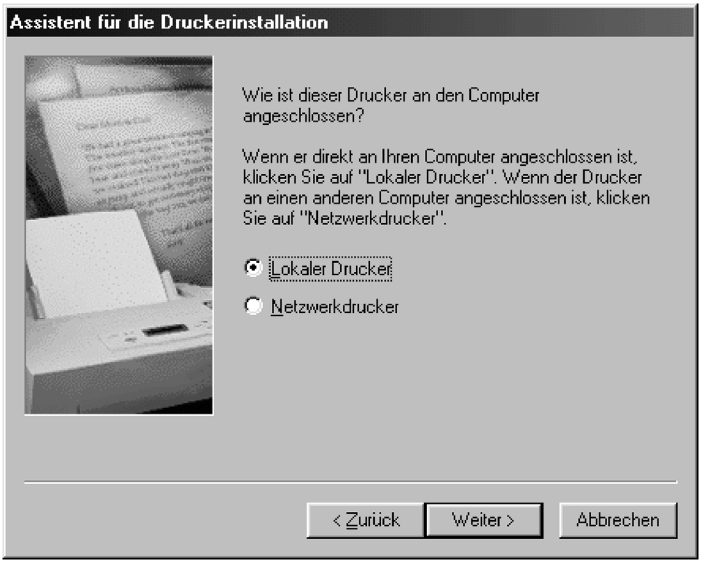
You still need to connect the printer to this port and configure it.

→ Connect the printer to the USB port on your Gigaset SX763 WLAN dsl.

The printer is installed in the same way as any other printer:

→ Go through ***Start*** – ***Settings*** – ***Printers*** and click ***Add Printer***.

→ In the window that opens, click ***Next***.



Assistent für die Druckerinstallation

Wie ist dieser Drucker an den Computer angeschlossen?

Wenn er direkt an Ihren Computer angeschlossen ist, klicken Sie auf "Lokaler Drucker". Wenn der Drucker an einen anderen Computer angeschlossen ist, klicken Sie auf "Netzwerkdrucker".

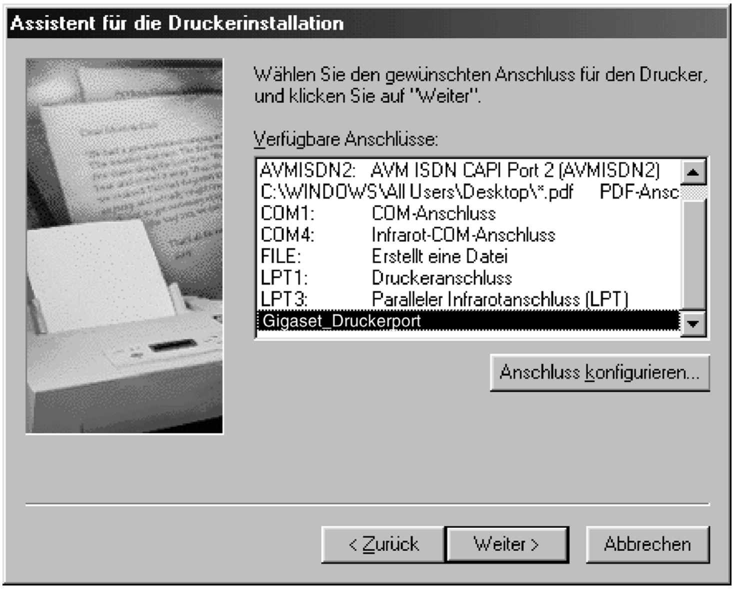
● Lokaler Drucker

○ Netzwerkdrucker

→ Proceed as instructed by the Add Printer Wizard. Please note:
In the window in which you are prompted to specify the location of the printer you should select ***Local printer*** (usually the default setting).

→ Then click ***Next***.

→ Continue to install the printer. Select your printer and click ***Next***.



Assistent für die Druckerinstallation

Wählen Sie den gewünschten Anschluss für den Drucker, und klicken Sie auf "Weiter".

Verfügbare Anschlüsse:

```
AVMISDN2:   AVM ISDN CAPI Port 2 (AVMISDN2)
C:\WINDOWS\All Users\Desktop\*.pdf     PDF-Ansc
COM1:       COM-Anschluss
COM4:       Infrarot-COM-Anschluss
FILE:       Erstellt eine Datei
LPT1:       Druckeranschluss
LPT3:       Paralleler Infrarotanschluss (LPT)
Gigaset_Druckerport
```

- ➙ When the window in which you are prompted to enter the type of connection appears, double-click the port name ***Gigaset_printerport***.
- ➙ Then continue to install the printer and finish the installation.

Note:

The print server of the Gigaset SX763 WLAN dsl does not work bidirectionally. It does not evaluate any of the printer's response messages. For this reason, please make sure that your printer is also configured unidirectionally.

Appendix

Troubleshooting

This section describes common problems and their solution. Any problems can be identified from the different LED displays. If you cannot solve the connection problem after checking the LED displays, please consult the sections of the following table. Further information is available on the Internet at
www.siemens.com/gigasetcustomercare.

Make sure the firmware on your device is up-to-date. The latest version can be found on the product page on the Internet.

Symptom	Possible cause and solutions
Power LED does not light up.	No power supply. → Check whether the mains adapter is connected to the Gigaset SX763 WLAN dsl and a power outlet. → Check whether the power outlet and the mains adapter are working properly. If the mains adapter is not working properly, contact our customer service unit (see Quick Start Guide).
The LAN LED on a connected device does not light up.	No LAN connection → Make sure the connected device is turned on. → Check whether the Ethernet cable is plugged in. → Check that you are using the right cable type (CAT5) and that the cable is not too long (100m). → Check that the network card on the connected device and the cables are not defective. If necessary, replace a defective network card or cable. → Use the Windows device manager (***My Computer*** – ***Properties***) to check whether the network card is functioning. If you see a red cross or a question mark, the driver may not have been installed or there is a resource conflict. Follow the Windows instructions to remedy the problem.
ADSL LED flashes	→ Wait until the integrated DSL modem has completed its synchronisation. This procedure can take up to 10 minutes.
The DSL LED does not light up after synchronisation.	→ Check the DSL cable. Check that the DSL cable is properly connected to the DSL port and the splitter.

Symptom	Possible cause and solutions
You cannot connect to the Internet.	➙ Check whether the ***Connect on demand*** option is deactivated. If it is, connections cannot be opened automatically. ➙ Select ***Connect on demand***. Remember that this setting may lead to higher costs if you are billed on the time used. ➙ The connection may have been terminated manually with the ***Connect on demand*** option selected. – Restore the connection again manually using the ***Connect*** button or – Restart the Gigaset SX763 WLAN dsl. In both cases, the ***Connect on demand*** setting will be active again.
You cannot open a connection from a wireless device to the Gigaset SX763 WLAN dsl.	◆ The wireless network adapter is not using the correct SSID. ➙ Change the SSID on the network adapter. ◆ Either WEP encryption has been activated on the Gigaset SX763 WLAN dsl but not on the wireless network adapter or it is using the wrong WEP key. ➙ Activate WEP encryption on the network adapter with the correct key. If you do not know the key, you will have to reset the Gigaset SX763 WLAN dsl (page 20). **Warning**: Please bear in mind that this will return **all** the configuration settings to the factory settings. ◆ WPA protection is activated on the Gigaset SX763 WLAN dsl but not on the wireless network adapter of the appropriate PC. ➙ Install and configure WPA protection on the PC.

Symptom	Possible cause and solutions
The Gigaset SX763 WLAN dsl or other PCs cannot be reached by a PC in the connected LAN using a **`ping`** command.	➞ Make sure that TCP/IP has been installed and configured on all the PCs in the local network. ➞ Check that the IP addresses have been correctly configured. In most cases you can use the DHCP function of the Gigaset SX763 WLAN dsl to assign dynamic addresses to the PCs in the LAN. In this case, you have to configure the TCP/IP settings of all the PCs so that they obtain the IP address automatically. If you configure the IP addresses in the LAN manually, remember to use the subnet mask 255.255.255.x. This means that the first three parts of the IP address on each PC and on the Gigaset SX763 WLAN dsl have to be identical. The device also has to be configured as a DNS server.
No connection to the configuration environment of the Gigaset SX763 WLAN dsl.	➞ Use the **`ping`** command to check whether you can establish a network connection to the Gigaset SX763 WLAN dsl. ➞ Check the network cable between the PC you want to use to administer the device and the Gigaset SX763 WLAN dsl. ➞ If the PC you want to use is in the router's local network, make sure that you are using the correct IP address administration (see above). ➞ If the PC you want to use is not in the router's local network, it must be authorised via remote management.
You cannot conduct VoIP telephone calls.	➞ The phone or the Gigaset SX763 WLAN dsl is not connected properly to the DSL port. Check the cabling and the ports. ➞ The access data for your VoIP phones is not entered correctly. Check the access data. ➞ You have not assigned the VoIP phone numbers to the telephone port. Check the configuration of the telephone ports and the extensions.
Password forgotten or lost.	➞ Reset the Gigaset SX763 WLAN dsl (page 20). **Warning**: Please bear in mind that this will return **all** the configuration settings to the factory settings.

Symptom	Possible cause and solutions
You cannot access a resource (drive or printer) on a different PC.	→ Make sure that TCP/IP has been installed and configured on all the PCs in the local network and that the PCs all belong to the same workgroup. → Check whether the resource has been released on the PC in question and whether you have the necessary access rights. → Printing: Check whether the printer has been set up as a network printer.

Operating information:

- USB port

  By connecting a device without its own power supply directly to the USB port, please note that the power consumption must not exceed 100mA.

- LAN ports

  The LAN ports may only be used for in-house networks. The ports are destroyed externally if there is a power surge.

- Phone ports

  The phone ports are only suitable for connecting in-house phones/phone systems. The ports are destroyed externally if there is a power surge.

Specifications

Interfaces

1 DSL	RJ-11, Annex A
4 LAN	RJ45, 10Base-T/100Base-TX, Auto-sensing
1 USB	USB 2.0, for printer server or file server (max. 100 mA)
1 FXO	RJ45, for connecting to the analogue telephone network
2 FXS	RJ11, for connecting analogue terminals (phone, fax, answering machine)
WLAN	802.11g, for wireless connection of up to 252 PCs Atheros Super G
External network adaptor	Input 230 V AC, output 12 V/1500 mA DC

Wireless properties

Frequency range	2400 to 2484 GHz ISM band (subject to local regulations)
Spreading	Direct Sequence Spread Spectrum (DSSS)
Modulation	CCK, OFDM
Number of channels	IEEE 802.11b: 13 (Europe, ETSI) IEEE 802.11g: 13 (Europe, ETSI)
Transfer rate	IEEE 802.11b: 1, 2, 5.5, 11 Mbps IEEE 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps Super G: 54, 72, 108 Mbps
Range	Up to 300 m outdoors, up to 30 m indoors

Operating environment

Temperature	Operating temperature 0 to 40 °C Storage temperature -25 to 70°C
Humidity	5% to 90% (non-condensing)
LED displays	Power (on/off) ADSL (operation, synchronisation) Online (activity, Internet) WLAN (activity, wireless) LAN1... LAN4 (connection to PC, activity, wired) USB (device connection) VoIP (connection, activity, Internet telephony) Phone1/Phone2 (FXS activity) Line (FXO activity, fixed network)

Compliance with security conditions and regulations

CE, EN60950

Software	Browser-based configuration environment
	NAT, PPPoE, PPPoA
	VPN pass-through, L2TP, IPSec
	DHCP server and client, DynDNS
	NAT, virtual server, DMZ
	Security setup
	Firewall, prevention of hacker attacks
	MAC address filtering
	Domain blocking
	DoS blocking, SPI
	Log file
	WEP encryption
	WPA encryption
	WPA2 encryption
	IEEE 802.1x
	Integrated SIP client

Open source licenses

Information in relation to free software can be found on the CD-ROM provided.

FCC / ACTA Information

Warning: Changes or modifications to this unit not expressly approved by Siemens Cordless Products could void the FCC authority to operate the equipment. This includes the addition of any external antenna device.

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of the base station is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

A plug and jack used to connect this equipment to the premises wiring and telephone network nust comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (*e.g.*, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance, that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you belive it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service. If you experience trouble with this telephone system, disconnect it from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

If trouble is experienced with this equipment, for repair or warranty information, please contact Siemens Customer Care, Tel. 1-888-777-0211. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved. This equipment is of a type that is not intented be repaired by the Customer (user).

This telephone system may not be used on coin service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information. Privacy of communications may not be ensured when using this phone.

If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this equipment does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

This telephone system equipment has been tested and found to comply with the limits for Class B digital device, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation. These limits are designed to provide reasonable protection against harmful interference in a residential installation. Some cordless telephones operate at frequencies that may cause interference to nearby TV's and VCR's; to minimize or prevent such interference, the system base should not be placed near or on top of a TV or VCR; and, if interference is experienced, moving the base farther away from the TV or VCR will often reduce or eliminate the interference.

However, there is no guarantee that interference will not occur in a particular installation. If this telephone system does cause harmful interference to radio or television reception, which can be determined by turning the system off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the base station and receiver.
3. Connect the base station into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio TV technician for help.

Notice for Direct Inward Dialing ("DID")

ALLOWING THIS EQUIPMENT TO BE OPERATED IN SUCH A MANNER AS TO NOT PROVIDE FOR PROPER ANSWER SUPERVISION AS A VIOLATION OF PART 68 OF THE FCC'S RULES.

Notice to Hearing Aid Wearers:

This phone system is compatible with inductively coupled hearing aids.

Power Outage:

In the event of a power outage, your cordless telephone will not operate. The cordless telephone requires electricity for operation. You should have a telephone that does not require electricity available for use during power outages.

Notice:

The installation of the base unit should allow at least 8 inches between the base and persons to be in compliance with FCC RF exposure guidelines.

For body worn operation, the portable part (handset) has been tested and meets FCC RF exposure guidelines. Use with an accessory that contains metal parts may not ensure compliance with FCC RF exposure guidelines.

Notice to telephone company service:
If you need service from your telephone company, please provide them with the information

– Facility interface Code (FIC)
– Service Order Code (SOC)
– Universal Service Order Code (USOC) Jack

as indicated on the label on the bottom side of the base station.

Industry Canada Certification

Operation is subject to the folowing two conditions (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network, protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together.

This precaution may be particularly important in rural areas

NOTE: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.
This product meets the applicable Industry Canada technical specifications.

The Ringer Equivalence Number is an indication of the maximum number of devices allowed to be connected to a telephone interface. The termination of an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all devices does not exceed five.

Safety precautions

Before using your telephone equipment, basic safety instructions should always be followed to reduce the risk of fire, electric shock and injury to persons.

1. Read and understand all instructions.

2. Follow all warnings and instructions marked on the product.

3. Unplug this product from the wall telephone jack and power outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use damp cloth for cleaning.

4. Do not use this product near water, for example, near a bathtub, wash bowl, kitchen sink, or laundry tub, in a wet basement or near a swimming pool.

5. Place this product securely on a stable surface. Serious damage and/or injury may result if the unit falls.

6. Slots or openings in the cabinet and the back and bottom are provided for ventilation, to protect it from overheating. These openings must not be blocked or covered. This product should never be placed near or over a radiator or heat register, or in a place where proper ventilation is not provided.

7. This product should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power supply to your home, consult your dealer or local power company.

8. Do not place objects on the power cord. Install the unit where no one can step or trip on the cord.

9. Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.

10. Never push objects of any kind into this product through cabinet slots as they may touch dangerous voltage points or short out parts that could result in the risk of fire or electric shock. Never spill liquid of any kind on this product.

11. To reduce the risk of electric shock or burns, do not disassemble this product. Take it to a qualified service center when service is required. Opening or removing covers may expose you to dangerous voltages, dangerous electrical current or other risks. Incorrect reassembly can cause electric shock when the appliance is subsequently used.

12. Unplug the product from the wall outlet and refer servicing to qualified service personnel under the following conditions:

a.) When the power cord is damaged or frayed.
b.) If liquid has been spilled into the product.
c.) If the product has been exposed to rain or water.

d.) If the product does not operate normally by following the operating instructions. Adjust only those controls that are covered by the operating instructions because improper adjustment of other controls may result in damage and may require extensive work by a qualified technician to restore the product to normal operation.
e.) If the product has been dropped or physically has been damaged.
f.) If the product exhibits a distinct change in performance.

13. Avoid using a telephone (other than a cordless type) during a thunderstorm. There may be a remote risk of electrical shock from lightning. Therefore we suggest a surge arrestor.

14. Do not use the telephone to report a gas leak in the vicinity of the leak.
15. Emergency/911 numbers may not be dialed if the keypad is locked.

BATTERY SAFETY PRECAUTIONS

To reduce the risk of fire, injury or electric shock, and to properly dispose of batteries, please read and understand the following instructions.
CONTAINS ALKALINE NICKEL METAL HYDRIDE BATTERY. BATTERY MUST BE RECYCLED OR DISPOSED OF PROPERLY. DO NOT DISPOSE OF IN MUNICIPAL WASTE.
1. Only use the batteries specified for use with this product.
2. DO NOT USE ALKALINE NICKEL CADMIUM OR ALKALINE LITHIUM BATTERIES, or mix batteries of different sizes or from different manufacturers in this product. DO NOT USE NONRECHARGEABLE BATTERIES.
3. Do not dispose of the batteries in a fire; the cells may explode. Do not expose batteries to water. Check with local codes for special disposal instructions.
4. Do not open or mutilate the batteries. Released electrolyte is corrosive and may cause damage to the eyes or skin. The electrolyte may be toxic if swallowed.
5. Exercise care in handling the batteries in order not to short the batteries with conducting materials such as rings, bracelets, and keys. The batteries or conducting material may overheat and cause burns or fire.
6. Charge the batteries provided with, or identified for use with, this product only in accordance with the instructions and limitations specified in the user's manual. Do not attempt to charge the batteries with any means other than that specified in the users manual.
7. Periodically clean the charge contacts on both the charger and handset.

Customer Care Warranty for Cordless Products
To obtain Siemens Customer Care Warranty service,
product operation information, or for problem resolution, call:
Toll Free: 1-888-777-0211
9:00 a.m. – 8:00 p.m. Central Standard Time seven days a week

www.siemens.com/gigasetcustomercare

Limited Warranty

This limited, non-transferable warranty is provided to the original purchaser. The product is warranted to be free from defects in materials and workmanship under normal installation, use, and service for period of one (1) year from the date of purchase as shown on the purchaser's receipt.

Our obligation under this warranty is limited to repair or replacement (at our option) of the product or any part(s), that are defective, provided that the product is returned to Siemens during the warranty period. A copy of the dated purchase receipt must accompany products returned. In the absence of a purchase receipt, the warranty period shall be one (1) year from the date of manufacture. Repair or replacement of the product is your sole and exclusive remedy.

If the product is repaired, reconditioned component parts or materials may be used. If the product is replaced, we may choose to replace it with a new or reconditioned product of the same or similar design. The repaired or replacement product will be warranted for either (a) 90 days or (b) the remainder of the original one (1) year warranty period, whichever is longer. Batteries are warranted to be free from defects at the time of purchase.

EXCLUSIONS: This warranty does not cover (a) the adjustment of customer-operated controls as explained in the appropriate model's instruction manual, or (b) the repair of any product, which has been altered or defaced. This warranty shall not apply to the cabinet or cosmetic parts, antenna, buttons, batteries, or routine maintenance.

This warranty does not apply to repairs or replacements necessitated by any cause beyond the control of SIEMENS including, but not limited to, any malfunction, defect or failure caused by or resulting from unauthorized service or parts, improper maintenance, damage from leaking batteries, operation contrary to furnished instructions, shipping or transit accidents, modification or repair by the user, abuse, misuse, neglect, accident, incorrect line voltage, fire, floor or other Acts of God, or normal wear and tear.

This warranty shall be void if the product is damaged as a result of defacement, misuse, abuse, neglect, accidents, destruction, or alteration of the serial number, improper electrical voltages or currents, repair, alteration or maintenance by any person or party other than our authorized service facility or any violation of instructions furnished by us.

The warrantor is not liable for incidental or consequential damages resulting from the use of this product, or arising out of any breach of this limited warranty. (As examples, this excludes damages for lost time, lost calls or messages, cost of having someone remove or re-install an installed unit if applicable, travel to and from servicer. The items listed are not exclusive, but are for illustration only.)

This warranty is also void if this product is removed from the country in which the original purchaser purchased it, if it is used in a country, which it not registered for use, or if it is used in a country for which it was not designed. Due to variations in telephone systems and communications laws, this product may be illegal for use in some countries. We assume no responsibility for damages or penalties incurred resulting from the use of this product in a manner or location other than that for which it is intended.

THIS ONE-YEAR LIMITED WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED. ANY IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, SHALL BE LIMITED IN DURATION TO THE ONE-YEAR DURATION OF THIS WRITTEN LIMITED WARRANTY. EXCEPT AS EXPRESSLY SET FORTH HEREIN, WE DISCLAIM ANY LIABILITY FOR DAMAGES ARISING FROM OWNERSHIP, USE, OR LOSS OF USE OF THE PRODUCTS, LOSS OF TIME, INCONVENIENCE, INJURY TO CUSTOMER OR ANY OTHER PERSON, OR DAMAGE TO CUSTOMER PROPERTY CAUSED BY THE PRODUCT, LOSS OF REVENUE OR PROFIT, OR DAMAGES FOR ANY FAILURE TO PERFORM. IN NO EVENT SHALL WE BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES EVEN IF WE ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL SIEMENS' LIABILITY EXCEED THE COST OF REPAIRING OR REPLACING THE DEFECTIVE PRODUCT AS PROVIDED HEREIN, AND ANY SUCH LIABILITIES WILL TERMINATE UPON EXPIRATION OF THE WARRANTY PERIOD.

Some states do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of incidental or consequential damages, so the above limitations may not apply to you.

This limited warranty is the sole and exclusive warranty provided for the product. This limited warranty is valid only in Canada and the United States (excluding all U.S. territories and protectorates). This limited warranty gives you specific legal rights, and you may also have other rights, which vary from state to state or province to province.

If you want to learn more about Siemens Gigasets, or for technical assistance with your Gigaset, visit our web site at http://www.my-siemens.com or, please call (888) 777-0211, or for TDD access (888) 777-0209.

Issued by Siemens Cordless Products
Siemens and Gigaset are registered trademarks of Siemens Home and Office Communication Devices GmbH & Co. KG.
Siemens Cordless Products is a division of Siemens Home and Office Communication Devices GmbH & Co. KG.
Product attributes subject to change.
Siemens reserves the right, to make changes without notice in equipment design and/or components.
Part Number: A31008-M1714-B101-1-19

Glossary

Access point

An access point, such as the Gigaset SX763 WLAN dsl, is the centre of a wireless local network (WLAN). It handles the connection of the wireless linked network components and regulates the data traffic in the wireless network. The access point also serves as an interface to other networks, for example an existing Ethernet LAN or via a modem to the Internet. The operating mode of wireless networks with an access point is called Infrastructure mode.

Ad-hoc mode

Ad-hoc mode describes wireless local networks (WLANs), in which the network components set up a spontaneous network without an Access point, for example several Notebooks in a conference. All the network components are peers. They must have a wireless Network adapter.

ADSL /ADSL2+

Asymmetric Digital Subscriber Line (ADSL) and ADSL 2+ are special types of DSL data transfer technology.

AES

Advanced Encryption Standard

AES is an encryption system, which was published as a standard in October 2000 by the National Institute of Standards and Technology (NIST). It is used for WPA encryption. A distinction is made between the three AES variants AES-128, AES-192 and AES-256 on the basis of the key length.

Auto connect

Auto connect means that applications such as Web browser, Messenger and E-mail automatically open an Internet connection when they are launched. This can lead to high charges if you are not using Flat rate. This function can be deactivated on the Gigaset SX763 WLAN dsl to save call charges.

Bridge

A bridge connects several network segments to form a joint network, for example to make a TCP/IP network. The segments can have different physical characteristics, for example different connections such as Ethernet and wireless LANs. Linking individual segments via bridges allows local networks of practically unlimited size.

See also: Switch, Hub, Router, Gateway

Broadcast

A broadcast is a data packet not directed to a particular recipient but to all the network components in the network. The Gigaset SX763 WLAN dsl does not pass on broadcast packets; they always remain within the local network (LAN) it administers.

BSSID

Basic Service Set ID

BSSID permits unique differentiation of one wireless network (WLAN) from another. In Infrastructure mode, the BSSID is the MAC address of the Access point. In wireless networks in Ad-hoc mode, the BSSID is the MAC address of any one of the participants.

Client

A client is an application that requests a service from a server. For example, an HTTP client on a PC in a local network requests data, i.e. Web pages from an HTTP server on the Internet. Frequently the network component (e.g. the PC) on which the client application is running is also called a client.

DHCP

Dynamic Host Configuration Protocol

DHCP handles the automatic assignment of IP addresses to network components. It was developed because of the complexity involved in defining IP addresses in large networks – especially the Internet – as participants frequently move, drop out or new ones join. A DHCP server automatically assigns the connected network components (DHCP Clients) Dynamic IP addresses from a defined IP pool range thus saving a great deal of configuration work. In addition, the address blocks can be used more effectively: Since not all participants are on the network at the same time, the same IP address can be assigned to different network components in succession as and when required.

The Gigaset SX763 WLAN dsl includes a DHCP server and uses it to assign automatic IP addresses to PCs in the local network. You can specify that the IP addresses for certain PCs are never changed.

DHCP server

See DHCP

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 is useful if you want to offer Server services on the Internet that are not to be run from behind the firewall for security reasons or if Internet applications do not work properly behind a firewall. A DMZ permits unrestricted access from the Internet to only one or a few network components, while the other network components remain secure behind the firewall.

DNS

Domain Name System

DNS permits the assignment of IP addresses to computers or Domain names that are easier to remember. A DNS server must administer this information for each LAN with an Internet connection. As soon as a page on the Internet is called up, the browser obtains the corresponding IP address from the DNS server so that it can establish the connection.

On the Internet, the assignment of domain names to IP addresses follows a hierarchical system. A local PC only knows the address of the local name server. This in turn knows all the addresses of the PCs in the local network and the superordinate name servers, which again know addresses or the next superordinate name servers.

DNS server

See DNS

Domain name

The Domain name is the reference to one or more Web servers on the Internet. The domain name is mapped via the DNS service to the corresponding IP address.

DoS attack

Denial of Service

A DoS attack is a particular form of hacker attack directed at computers and networks with a connection to the Internet. The aim is not so much to steal data but to paralyse the computer or network so severely that the network resources are no longer available. A typical hacker attack involves making a remote computer announce that it is acting for the paralysed computer, for example, and receive the data intended for you.

DSL

Digital Subscriber Line

DSL is a data transfer technique in which a connection to the Internet can be run at 1.5 Mbps over normal telephone lines. A DSL connection is provided by an Internet service provider. It requires a DSL modem.

Dynamic IP address

A dynamic IP address is assigned to a network component automatically by DHCP. This means that the IP address of a network component can change with every login or at certain intervals.

See also: Static IP address

DynDNS

Dynamic DNS

The assignment of Domain names and IP addresses is handled by the Domain Name Service (DNS). This service is now enhanced with so-called Dynamic DNS (DynDNS) for Dynamic IP addresses. This enables 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.

Encryption

Encryption protects confidential information against unauthorised access. With an encryption system, data packets can be sent securely over a network. The Gigaset SX763 WLAN dsl offers WEP encryption and WPA for secure data transfer over wireless networks.

Ethernet

Ethernet is a network technology for local networks (LANs) defined by the IEEE as standard IEEE 802.3. Ethernet uses a base-band cable with a transfer rate of 10 or 100 Mbps.

Firewall

Firewalls are used by network operators as protection against unauthorised external access. This involves a whole bundle of hardware and software actions and technologies that monitor and control the data flow between the private network to be protected and an unprotected network such as the Internet.

See also: NAT

Flat rate

Flat rate is a particular billing system for Internet connections. The Internet service provider charges a monthly fee regardless of the duration and number of logins.

Full duplex

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

See also: Half duplex

Gateway

A gateway is a device for connecting networks with completely different architectures (addressing, protocols, application interfaces etc.). Although it is not totally correct, the term is also used as a synonym for Router.

Global IP address

See Public IP address

Half duplex

Operating mode for data transmission. Only one side can send and/or receive data at the same time.

See also: Full duplex

HTTP proxy

An HTTP proxy is a Server that network components use for their Internet traffic. All requests are sent via the proxy.

Hub

A hub connects several network components in a star-topology network by sending all the data it receives from one network component to all the other network components.

See also Switch, Bridge, Router, Gateway

IEEE

Institute of Electrical and Electronic Engineers

The IEEE is an international body for defining network standards, especially for standardising LAN technologies, transfer protocols, data transfer speeds and wiring.

IEEE 802.11

IEEE 802.11 is a standard for wireless LANs operating in the 2.4 GHz band. In so-called Infrastructure mode, terminals can be connected to a base station (Access point) or they can connect with each other spontaneously (Ad-hoc mode).

IGMP

Internet Group Management Protocol

IGMP is an Internet Protocol that enables an Internet computer to inform neighbouring routers that it is a member of a multicast group. With multicasting, a computer can send content on the Internet to several other computers that have registered an interest in the first computer's content. Multicasting can, for example, be used for multimedia programs for media streaming to recipients that have set up multicast group membership.

Infrastructure mode

Infrastructure mode is a way of operating wireless local networks (WLANs) in which an Access point handles the data traffic. Network components cannot establish a direct connection with each other as is the case in Ad-hoc mode.

Internet

The Internet is a wide-area network (WAN) linking several million users around the world. A number of Protocols have been created for exchanging data, and these are known collectively as TCP/IP. All participants on the Internet can be identified by an IP address. Servers are addressed by Domain names (e.g. siemens.com). Domain names are assigned to IP addresses by the Domain Name Service (DNS).

These are some of the main Internet services:

- Electronic mail (e-mail)
- The World Wide Web (WWW)
- File transfer (FTP)
- Discussion forums (Usenet / Newsgroups)

Internet service provider

An Internet service provider offers access to the Internet for a fee.

Internet telephony

Transmission of voice via the Internet (Voice over IP).

IP

Internet protocol

The IP Protocol is one of the TCP/IP protocols. It is responsible for addressing parties in a network using IP addresses and routes data from the sender to the recipient. It decides the paths along which the data packets travel from the sender to the recipient in a complex network (routing).

IP address

The IP address is the unique network-wide address of a network component in a network based on the TCP/IP protocol (e.g. in a local area network (LAN) or on the Internet). The IP address has four parts (each with up to three-position digit sequences) separated by full stops (e.g. 192.168.1.1). The IP address comprises the network number and the computer number. Depending on the Subnet mask, one, two or three parts form the network number; the remainder form the computer number. You can find out the IP address of your PC using the `ipconfig` command.

IP addresses can be assigned manually (see Static IP address) or automatically (see Dynamic IP address).

On the Internet Domain names are normally used instead of the IP addresses. The DNS is used to assign domain names to IP addresses.

The Gigaset SX763 WLAN dsl has a Private IP address and a Public IP address.

IPoA

IP over ATM

IP pool range

The Gigaset SX763 WLAN dsl's IP address pool defines a range of IP addresses that the router's DHCP server can use to assign Dynamic IP addresses.

ISP

(Internet Service Provider)

Internet service provider

LAN

Local network

A local area network (or local network) links network components so that they can exchange data and share resources. The physical range is restricted to a particular area (a site). As a rule the users and operators are identical. A local network can be connected to other local networks or to a wide-area network (WAN) such as the Internet.

With the Gigaset SX763 WLAN dsl you can set up a wired local Ethernet network and a wireless IEEE 802.11g standard network (WLAN).

Lease time

The lease time defines the period of time for which the PCs keep the Dynamic IP address assigned to them by the DHCP server without changing it.

Local IP address

See Private IP address

MAC address

Media Access Control

The MAC address is used for the globally unique identification of a Network adapters. It comprises six parts (hexadecimal numbers), e.g. 00-90-96-34-00-1A. The MAC address is assigned by the network adapter manufacturer and cannot be changed.

Mbps

Million bits per second

Specification of the transfer speed in a network.

MER

MAC Encapsulated Routing

MRU

Maximum Receive Unit

The MRU defines the maximum user data volume within a data packet.

MTU

Maximum Transmission Unit

The MTU defines the maximum length of a data packet that can be carried over the network at any one time.

NAT

Network Address Translation

NAT is a method for converting IP addresses (Private IP addresses) within a network into one or several Public IP addresses on the Internet. With NAT, several network components in a LAN can share the router's public IP address to connect to the Internet. The network components of the local network are hidden behind the router's IP address registered on the Internet. Because of this security function, NAT is frequently used as part of the Firewall of a network. If you want to make services on a PC in the local network available on the Internet despite NAT, you can configure the Gigaset SX763 WLAN dsl as a Virtual server.

Network

A network is a group of devices connected in wired or wireless mode so that they can share resources such as data and peripherals. A general distinction is made between local networks (LANs) and wide-area networks (WANs).

Network adapter

The network adapter is the hardware device that creates the connection between a network component and a local network. The connection can be wired or wireless. An Ethernet network card is an example of a wired network adapter. The Gigaset PC Card 108 and the Gigaset USB Adapter 108 are examples of wireless network adapters.

A network adapter has a unique address, the MAC address.

PBX

Private Branch Exchange

PBX is the English acronym for a public branch exchange, which allows connection and configuration of extensions and telephone functions.

Port

Data is exchanged between two applications in a network across a port. The port number addresses an application within a network component. The combination of IP address/port number uniquely identifies the recipient or sender of a data packet within a network. Some applications (e.g. Internet services such as HTTP or FTP) work with fixed port numbers; others are allocated a free port number whenever they need one.

Port forwarding

In port forwarding the Gigaset SX763 WLAN dsl directs data packets from the Internet that are addressed to a particular Port to the corresponding port of the appropriate network component. This enables servers within the local network to offer services on the Internet without them needing a Public IP address.

See also: Virtual server

PPPoA

Point-to-Point Protocol over ATM

PPPoA is a Protocol for connecting network components in a local Ethernet network to the Internet via an ATM network.

PPPoE

Point-to-Point Protocol over Ethernet

PPPoE is a Protocol for connecting network components in a local Ethernet network to the Internet via a modem.

Private IP address

The private IP address (also known as the local IP address) is a network component's address within the local network (LAN). The network operator can assign any address he or she wants. Devices that act as a link from a local network, such as the Gigaset SX763 WLAN dsl, have a private and a Public IP address.

Protocol

A protocol describes the agreements for communicating in a network. It contains rules for opening, administering and closing a connection, as well as about data formats, time frames and handling possible errors. Communication between two applications requires different protocols at various levels, for example the TCP/IP protocols for the Internet.

Public IP address

The public IP address (also known as the global IP address) is a network component's address on the Internet. It is assigned by the Internet service provider. Devices that create a link from a LAN to the Internet, such as the Gigaset SX763 WLAN dsl, have a public and a Private IP address.

PVC

Permanent Virtual Circuit

A permanent virtual circuit is a logical connection in an ATM network.

QoS

Quality of Service

QoS allows network traffic to be sorted according to priorities. When this parameter is activated, Internet telephony is given priority over other data traffic. This is a precondition for problem-free calls.

Radio network

See WLAN

Rekey interval

The rekey interval is the period after which new keys are automatically generated for data encryption with WPA-PSK.

Remote management

Remote management refers to the ability to manage a network from a network component that is actually outside the local network (LAN).

Repeater

A repeater extends the range of a wireless local network by relaying data from the Access point to additional PCs or Network adapters.

Roaming

Roaming extends the range of a wireless LAN by using several Access points that use the same SSID and the same radio channel and are linked via Ethernet. The PCs in the network can switch dynamically between several access points without losing the existing network connection.

Router

A router directs data packets from one local network (LAN) to another via the fastest route. A router makes it possible to connect networks that have different network technologies. For example, it can link a local network with Ethernet or WLAN technology to the Internet.

See also: Bridge, Switch, Hub, Gateway

Server

A server makes a service available to other network components (Clients). The term "server" is often used to refer to a computer or PC. However, it can also mean an application that provides a particular service such as DNS or a Web service.

SIP

Session Initiation Protocol

SIP is a standard for data transfer in Internet telephony (VoIP). It describes how a call is carried over the data network and which components plus which transport and signalling protocols are involved.

SIP proxy server

The SIP proxy server sets up the connection to the Internet for Internet telephony (VoIP) for all connected SIP clients.

SIP client

A SIP client enables Internet telephony (VoIP). It can be installed as software on a PC and thereby enable Internet telephony via the local network in wireless or wired mode. Wireless SIP phones (WLAN handsets) can likewise be used via the local network for Internet telephony.

SMTP

Simple Mail Transfer Protocol

The SMTP Protocol is part of the TCP/IP protocol family. It governs the exchange of electronic mail on the Internet. Your Internet service provider provides you with access to an SMTP server.

SNMP

Simple Network Management Protocol

The SNMP Protocol is part of the TCP/IP protocol family. It provides a simple procedure for administering the network based on a system of shared information for management data and network management messages (known as traps) and reports the occurrence of events within the monitored network (e.g. an alarm message or notification of configuration changes).

SSID

Service Set Identifier

The SSID is used to identify the stations in a wireless network (WLAN). All wireless network components with the same SSID form a common network. The SSID can be assigned by the network operator.

Static IP address

A static IP address is assigned to a network component manually during network configuration. Unlike the Dynamic IP address, a static (fixed) IP address never changes.

Subnet

A subnet divides a network into smaller units.

Subnet mask

The subnet mask determines how parts of IP addresses of a network represent the network number and how many the computer number.

The subnet mask in a network administered by the Gigaset SX763 WLAN dsl is always 255.255.255.0. That means the first three parts of the IP address form the network number and the final part is used for assigning computer numbers. The first three parts of the IP address of all network components are therefore always the same in this case.

Super G

Super G is an extension of the IEEE 802.11g mode. Channel bundling can be used to double the maximum transfer rate to 108 Mbps.

Switch

A switch, like a Hub, is an element used to link different network segments or components. Unlike a hub however, the switch has its own intelligence that enables it to forward packets to only the subnet or network component they are meant for.

See also: Bridge, Hub, Router, Gateway

TCP

Transmission Control Protocol

The TCP Protocol is part of the TCP/IP protocol family. TCP handles data transport between communication partners (applications). TCP is a session-based transfer protocol, i.e. it sets up, monitors and terminates a connection for transferring data.

See also: UDP

TCP/IP

Protocol family on which the Internet is based. IP forms the basis for every computer-to-computer connection. TCP provides applications with a reliable transmission link in the form of a continuous data stream. TCP/IP is the basis on which services such as WWW, Mail and News are built. There are other protocols as well.

UDP

User Datagram Protocol

UDP is a Protocol of the TCP/IP protocol family that handles data transport between two communication partners (applications). Unlike TCP, UDP is a non-session based protocol. It does not establish a fixed connection. The data packets, so-called datagrams, are sent as a Broadcast. The recipient is responsible for making sure the data is received. The sender is not notified about whether it is received or not.

UPnP

Universal Plug and Play

UPnP technology is used for the spontaneous linking of home or small office networks. Devices that support UPnP carry out their network configuration automatically once they are connected to a network. They also provide their own services or use services of other devices in the network automatically.

URL

Universal Resource Locator

Globally unique address of a domain on the Internet.

Vanity

The term vanity comes from the United States. Alphanumeric keypads on phones and other phone terminals allow you to represent phone numbers as words so that they can be remembered more easily. Instead of a combination of digits, you select a combination of letters.

VCI

Virtual Channel Identifier

Part of an address in an ATM network.

Virtual server

A virtual Server provides a service on the Internet that runs not on itself, but on another network component. The Gigaset SX763 WLAN dsl can be configured as a virtual server. It will then direct incoming calls for a service via Port forwarding directly to the appropriate Port of the network component in question.

VLAN
Virtual Local Area Network

A VLAN is a virtual local network within a physical network. A widely disseminated technical implementation of VLANs is defined partially in the Standard IEEE 802.1Q. VLAN allows preferred forwarding of voice data, for example. This functionality is important for VoIP (IP telephony). This also means that phone calls can be made without interruption with a restricted bandwidth.

VoIP

Voice over IP

See Internet telephony

VPI

Virtual Path Identifier

Part of an address in an ATM network.

WDS

Wireless Distribution System

WDS describes the wireless connection between a number of access points.

WAN

Wide Area Network

A WAN is a wide area network that is not restricted to one particular area, such as the Internet. A WAN is run by one or more public providers to enable private access. You access the Internet via an Internet service provider.

WEP

Wired Equivalent Privacy

WEP is a security protocol defined in the IEEE 802.11 standard. It is used to protect wireless transmissions in a WLAN against unauthorised access through Encryption of the data transmitted.

WLAN

Wireless LAN

Wireless LANs enable network components to communicate with a network using radio waves as the transport medium. A wireless LAN can be connected as an extension to a wired LAN or it can form the basis for a new network. The basic element of a wireless network is the cell. This is the area where the wireless communication takes place. A WLAN can be operated in Ad-hoc mode or Infrastructure mode.

WLAN is currently specified in Standard IEEE 802.11. The Gigaset SX763 WLAN dsl complies with Standard 802.11g.

WPA

WPA is a new standard-conformant solution for greater security in wireless networks. WPA is meant to replace the existing WEP standard (Wired Equivalent Privacy) and offers more reliable encryption and authentication methods.

WPA-PSK

WPA Pre-shared Key

Variant of WPA data encryption in which new keys are automatically generated at regular intervals by means of a keyword (pre-shared key). The key is updated after defined periods (Rekey interval).

XR

eXtended Range

XR technology extends the range in a WLAN and in so doing allows improved coverage of the desired range in home or small office networks. Activating this function at the access point can extend the range to the network adapters considerably, though the data transfer rate is reduced as a result.

Index