

SIEMENS

Gigaset SX686 WiMAX

User Guide



This device works in a frequency band for which a general licence might have to be obtained. Please contact your service provider or your National Authority for Frequency Management about licensing before putting this device into service.

Contents

For your safety	7
Safety precautions	7
Cleaning and care	7
Trademarks	7
Information on Specific Absorption Rate (SAR)	8
Information about the optional outdoor antenna	8
The Gigaset SX686 WiMAX	11
Product overview	13
The device	13
Features and applications	17
Local area networks with Gigaset products	19
Wired local area network (Ethernet)	20
Wireless local area network (WLAN)	21
Linking a wireless network to an Ethernet	23
Extending the wireless network coverage with a repeater	24
Internet telephony and connecting analogue phones	25
Setting up a wireless network via WPS	26
Installing the Gigaset SX686 WiMAX	28
System requirements	28
Choosing your location	29
Connecting and activating the Gigaset SX686 WiMAX	32
Installation overview	32
Connecting the outdoor antenna	33
Connecting a PC wired	34
Connecting a telephone, fax machine or answer machine	35
Connecting to the mains power supply	36
Connecting PCs wirelessly	37
Checking the operating state	39
Network configuration of the PCs	39
Making the basic settings	39
Connecting and configuring additional PCs (optional)	40
The user interface	41
Starting the user interface	41
The start screen	42
Selecting a language	44
Connecting to the Internet manually	44
Elements in the user interface	45
Basic Setup Wizard	46
Choosing the antenna	47
Aligning the antenna	48

Contents

Searching a WiMAX network	49
Antenna fine tuning	52
Regional Options	53
Configuring Internet connections	54
Telephony	56
WPS Registration	57
Summary	58

Security Setup Wizard 59

Assigning a password	60
Changing the SSID	61
Setting up security functions for the wireless network	62
WPA2/WPA with pre-shared key (PSK)	63
WEP encryption	64
Access control within the wireless network	66
Saving settings	68

Configuring Advanced Settings 69

Internet	70
Internet selection	71
Internet Connection	72
DNS server	75
Firewall	76
Attack Detection	77
Setting up access control to the Internet	78
Setting up the NAT function	80
Port Triggering	82
Port Forwarding	83
Opening the firewall for a selected PC (Exposed Host)	84
Dynamic DNS	85
Routing	87
LAN configuration	88
Assigning static IP addresses to individual PCs	90
Configuring wireless connections	91
Starting WPS registration and configuring WPS	93
Setting encryption	94
WPA2-PSK and WPA2-PSK / WPA-PSK	95
WEP encryption	98
Permitted clients	101
Repeater function (WDS)	103
Setting up Internet telephony (VoIP)	105
VoIP settings	106
Extensions	109
Dialing Plans	113
Quick dial	115

USB	116
File Server	117
Web Server	120
Print Server	123
Call guide	124
Making calls	124
Advanced options	125
Toggling telephone calls	125
Conference call between three participants	126
Call answering and forwarding	126
Call waiting and call reject if busy	127
Special functions	128
Confirmation tones	129
Administration	130
Regional Options	130
Internet Time	131
System Password	131
System management	132
Backing up and restoring a configuration	133
Backing up configuration data	133
Restoring the saved data	134
Restoring factory settings	134
Reboot	134
System Log	135
Status information	136
Overview	136
Security	137
Radio Status	138
Internet	139
Local Network	140
Wireless Network	141
Telephony	142
Device	142
Alarms	143
Functional Alarms	144
Physical Alarms	146
Using the USB port	147
Installing the printer port for network printers	147
Introduction	147
Installing a standard TCP/IP printer port under Windows Vista	148
Installing a standard TCP/IP printer port under Windows XP/2000	154
Installing a printer on the TCP/IP port retrospectively	160
Instructions for setting up a printer on the PC	161

Contents

- Using the data on a USB mass storage device 162
 - Checking network services 162
 - Share Inter Process Communication for the network 164
 - Starting the computer browser 164
 - Enabling file and printer sharing in the Windows firewall 165

Appendix 167

- Troubleshooting 167
- Deactivating HTTP proxy and configuring a pop-up blocker 173
 - Deactivating the HTTP proxy 173
 - Configuring the pop-up blocker 173
- Specifications 174
- Guarantee Certificate United Kingdom 177
- Guarantee certificate Ireland 177
- Open Source Software used in the product 179

Glossary 180

Index 195

For your safety

→ Please read the safety instructions carefully before putting into service.

Safety precautions

General safety instructions

- ◆ If you give the Gigaset SX686 WiMAX to someone else, make sure you also give them its documentation.
- ◆ The Gigaset SX686 WiMAX must only be used as described in these installation instructions.

Safety instructions for connection

- ◆ Only use the mains adapter supplied, as indicated on the underside of the Gigaset SX686 WiMAX.

Safety precautions for the Gigaset SX686 WiMAX

- ◆ The operation of medical appliances may be affected. Be aware of the technical conditions in your particular environment, e.g. doctor's surgery.
- ◆ The Gigaset SX686 WiMAX and the antenna can interfere with the functioning of medical devices such as pacemakers. Keep at least 20 cm between the devices and the pacemaker. For more information, consult your doctor.
- ◆ The device may cause an unpleasant humming noise in hearing aids.
- ◆ Do not use the devices in environments with a potential explosion hazard, e.g. car paint shops, or in a humid environment (bathroom etc.).
- ◆ The Ethernet function (LAN socket, **LAN**) and the FXS function (analogue phone port, **Phone**) are designed exclusively for connection **inside** a building.

Cleaning and care

Wipe the Gigaset SX686 WiMAX with a **damp** cloth (do not use solvent) or an antistatic cloth.

Never use a dry cloth. This can cause static.

Trademarks

Gigaset Communications GmbH is a trademark licensee of Siemens AG.

Microsoft, Windows Vista, Windows XP, Windows 2000 and Internet Explorer are registered trademarks of Microsoft Corporation.

Mozilla Firefox is a registered trademark of the Mozilla Organisation.


Information on Specific Absorption Rate (SAR)

This device meets the limits for protecting the health of the public from the effects of exposure to electromagnetic fields when it is operated in connection with the designated antenna(s) like described in the user manual.

Your device is a radio transmitter and receiver. It is designed and manufactured not to exceed the limits for exposure to emission from electromagnetic fields recommended by international guidelines from the International Commission on Non-Ionizing Radiation Protection (ICNIRP). These limits are part of comprehensive guidelines for the protection of the public and establish permitted levels of exposure to electromagnetic radiation for the population. The guidelines were confirmed by independent scientific organisations through periodic and thorough evaluation of scientific studies. The limits include a substantial safety margin designed to assure the safety of all persons, regardless of age and health.

The exposure limit employs a unit of measurement known as the Specific Absorption Rate, or SAR. The SAR limit stated in the international guidelines is 2.0 W/kg. Tests for SAR are conducted in all frequency bands with the device transmitting at its highest power level with minimum possible distance to the body. The actual SAR level of the device during operation with the designated antenna(s) is below the maximum value and is additionally decreased by a distance to the device. This is because the device is designed to operate at multiple power levels so as to use only the power required to enable seamless network connection.

Information about the optional outdoor antenna

	<p>Only one of the antennas listed on Seite 28 must be used.</p> <p>The outdoor antenna must be installed and put into service by a qualified electrician.</p> <p>➔ Only commence the outdoor work once you have taken all the necessary steps to make the location safe.</p> <p>Be sure to observe the safety instructions.</p>
---	--

Wall duct:

To connect the Gigaset SX686 WiMAX to the outdoor antenna, the antenna cable must be fed through the wall to the outside of the building. It must be possible to make a suitable wall or window duct at or near the location of the Gigaset SX686 WiMAX.

Setting up the antenna mast:

There should not be any obstructions (walls, trees etc.) in front of the antenna.

The best results will be obtained if the outdoor antenna is in sight of the WiMAX base station (cf. Fig. 1).

If a line of sight is not possible, you can reflect the radio waves off neighbouring buildings. To do this, direct the antenna at the building it is to reflect off and not at the base station (cf. Fig. 2).

Fig. 1

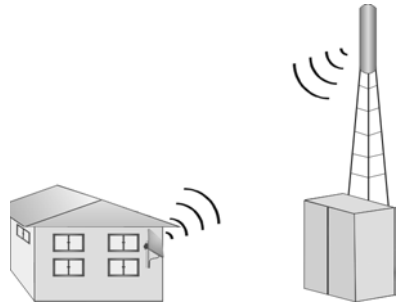


Fig. 2



The antenna mast must be structurally secure. Check how secure the various attachments are.

The antenna mast must be within reach of the cable. Ideally, the antenna cable should be protected outside (from frost, sun, unauthorised and mechanical influences etc.).

In particular, make sure the antenna mast has sufficient load capacity. If you are mounting the mast on the roof, make sure the roof is fully sealed again afterwards.

For your safety

Lightning protection

The antenna mast should be positioned near a lightning conductor. A suitable lightning conductor must be installed where necessary.

The outdoor antenna is not designed to be struck directly by lightning and must be protected accordingly. The antenna must therefore be mounted in areas that are protected against lightning (Lightning Protection Zone 0B). The corresponding separation distance (IEC 62305) must be complied with.

Earthing and lightning protection work may only be carried out by electricians specifically qualified for such work.

The appropriate earthing clamps must be used to create an equipotential bonding between a cable shield and an equipotential bonding bar that complies with regulations.

Please observe the standard DIN VDE 0855-300 and find out more on the Internet at http://www.dehn.de/www_DE/PAGES_D/service/down/blitzplaner.html (German)

Or

<http://www.dehn-usa.com/dehn-Application-Guides-pubcid1.html> (English)

Antenna cable and antenna connection:

It must be possible to connect the outdoor antenna to the Gigaset SX686 WiMAX by means of an antenna cable.

Please note that the antenna connection must be protected from the impact of rain and other weather effects.

Use cable clamps to attach the cable to the mast. Please note that the cable must be long enough to turn the antenna at a later stage.

Antenna alignment:

When aligning the antenna, we recommend asking a second person to run the basic setup wizard on the PC and to check the reception quality on the screen; see Chapter „Basic Setup Wizard“ auf Seite 46.

After installation:

Tighten all screw connections to the torques listed in the installation instructions.

Secure the antenna cable with cable clamps and cable ties. The cable must be protected from exposure to pressure and tension.

The Gigaset SX686 WiMAX

The Gigaset SX686 WiMAX gateway is a powerful but simple communications device for connecting your PC or local area network (LAN) to the Internet via WiMAX.



WiMAX stands for "**W**orldwide **I**nteroperability for **M**icrowave **A**ccess", a modern wireless network technology that enables fast Internet connection even in remote areas. With WiMAX technology you are no longer dependent on a DSL infrastructure in your home or place of work. Instead, you connect your PC or network wirelessly to radio stations operated in your region by your provider. As a result, WiMAX gives you fast, economical broadband Internet access, even in places that are not connected to the DSL cable network.

The WiMAX standard IEEE 802.16 generally defines WiMAX technology. Your Gigaset SX686 WiMAX already meets the latest IEEE 802.16e-2005 standard, a mobile WiMAX standard that offers many extra possibilities.

The Gigaset SX686 WiMAX

The Gigaset SX686 WiMAX 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 SX686 WiMAX is a convenient and simple solution.

You can build a local network ([LAN](#)) by connecting up to four PCs to your Gigaset SX686 WiMAX via cable. Additionally you can connect PCs wirelessly and create a wireless local area network ([WLAN](#)). For network security, wireless transmission can be encrypted using the WPA/WPA2 standard or 64/128-bit WEP.

There are two variants for operating the Gigaset SX686 WiMAX in a wireless network:

- With integrated WLAN antenna, if you operate WiMAX within the 3.5 GHz frequency band.
- With a connector for an external WLAN antenna, if you operate WiMAX within the 2.6 GHz frequency band. In this case the frequencies of the WiMAX and the WLAN adjoin. You can therefore use the supplied external WLAN antenna which should be positioned as far as possible from your device.

The Gigaset SX686 WiMAX 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 SX686 WiMAX provides the new WPS function for wireless connection of PCs or notebooks. You can activate this function via the user interface. If the other clients in your wireless network such as the Gigaset PC Card 300 also support WPS, you can connect with a simple click.

The Gigaset SX686 WiMAX has an extensive range of functions but remains simple to use. It can be configured and operational within a few minutes.

Do your part for the environment (ECO)

Thanks to a switch-mode power supply unit, all of our broadband products offer significantly reduced power consumption - for more energy-efficient use. Each device also lets you variably reduce WLAN transmission power based on the size of your home or office network via the user interface, which helps make a cleaner environment for everyone. You can even turn the WLAN off completely when you're not using it. Some of our broadband products also offer you the convenience of switching the WLAN on or off with a handy button directly on the device itself - or have a timer do it for you. It's our goal to ensure a sustainable economic process by using an environmentally friendly production and management system - which makes it easy for us to meet the strict ISO 14001 standards for international environmental management.



Note:

This user guide is based on software release 7.0.

Product overview

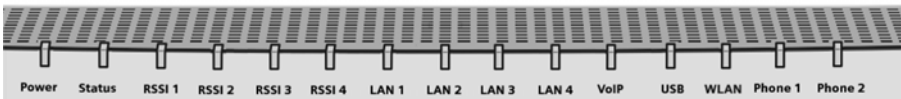
The device

Gigaset SX686 WiMAX with an external WLAN antenna connector



Gigaset SX686 WiMAX with an internal WLAN antenna

LEDs



The Gigaset SX686 WiMAX

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

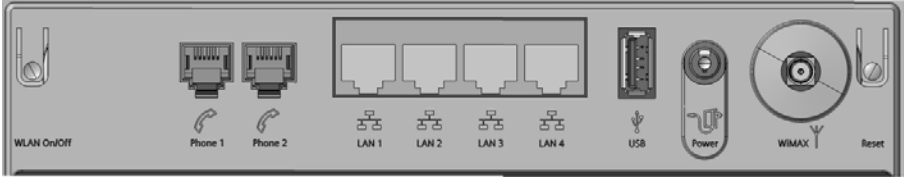
LED	State	Status
Power	On (green)	The Gigaset SX686 WiMAX is connected to the mains.
	Off	The Gigaset SX686 WiMAX is disconnected from the mains or the power supply has failed.
Status	On (green)	The Gigaset SX686 WiMAX is registered with a WiMAX network and ready for use. A connection to the Internet has been established.
	Off	The Gigaset SX686 WiMAX is not registered with a WiMAX network; it is not possible to establish an Internet connection.
	Flashes (green)	The Gigaset SX686 WiMAX is establishing a connection with a WiMAX network.
	Lights up red	Alarm: The Gigaset SX686 WiMAX is not ready. Possible cause: device is overheating or faulty (see page 143).
RSSI1 – RSSI 4	0 to 4 LEDs light up green	The LEDs on the Gigaset SX686 WiMAX help you to position the antenna more easily. The LEDs indicate the signal strength; the more LEDs that light up, the better the signal reception.
	All 4 LEDs flash green	The Gigaset SX686 WiMAX is being reset to the factory settings; see "Restoring factory settings" on page 134.
Line	On	One of the connected phones' receivers has been lifted for a call (fixed network telephony).
	Off	There is currently no fixed network connection.
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 activated, no data transmission at present.
	Flashing	The Gigaset SX686 WiMAX is sending or receiving data on the radio interface.
	Off	The radio interface is deactivated.
WLAN	During WPS registration	
	On (300 sec)	WPS registration was successful.
	Flashing slowly	WPS registration is in progress.
	Flashing quickly	WPS registration was not successful.
	Flashing quickly with interruption	More than one client tried to register.

LED	State	Status
VoIP	On	At least one VoIP account is set up, registered with the provider and assigned to one of the phone ports.
	Flashing	A call is currently being made via the Internet.
	Off	There is currently no connection for Internet telephony or no VoIP port has been configured.
USB	On	A device is connected to the Gigaset SX686 WiMAX via the USB port.
	Flashing	The device connected to the USB port is active.
	Off	There is no device connected.
Phone 1/ Phone 2	On	The receiver of the phone connected to the port has been lifted.
	Flashing	The phone is ringing and a call is being received or a call is being conducted.
	Off	The port is successfully configured. The attached phone is in on hook condition.

The Gigaset SX686 WiMAX

Ports and operating elements

Gigaset SX686 WiMAX with its own WLAN antenna



Gigaset SX686 WiMAX with an external WLAN antenna connector



The Gigaset SX686 WiMAX has the following ports and operating elements.

Element	Description
WLAN On/Off	WLAN on/off switch for activating and deactivating the wireless LAN. All the WLAN settings remain when switched off and become active if WLAN is switched on again.
WLAN	Port for an external WLAN desktop antenna (depending on the device variant).
Phone1/2	Sockets for connecting two phones, fax or answering machine
LAN1 – LAN4 (yellow)	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).
USB (blue)	USB port for printer or USB memory.
Power	Socket for the mains adapter supplied Warning: Using the wrong power supply unit may damage the Gigaset SX686 WiMAX.
Line (green)	Socket for connecting the phone line to the telephone port on the splitter
WiMAX	Port for an external WiMAX antenna (optional)
Reset	Reboot function: Press and hold 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 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.

Features and applications

The Gigaset SX686 WiMAX's wide range of features makes it ideal for a large number of applications.

Depending on your device, some of the features may differ from the description in this instruction manual.

◆ Internet access

The Gigaset SX686 WiMAX supports shared Internet access for up to 252 users via the integrated [WiMAX](#) modem. This means several users in your network can surf the Internet at the same time, all using the same Internet account. With your Gigaset SX686 WiMAX, you can make use of everything the Internet has to offer:

– Downloads

Even large files download quickly to your PC.

Complex Website designs are no longer characterised by the time they take to download – you can enjoy flash animation and high-resolution graphics immediately after clicking on a link.

– Audio

Play back audio files straight from the Internet.

Listen to the radio via the Internet in superb digital quality.

– Video

View short or longer films you find on the Internet without tedious waiting times.

Watch television via the Internet (IPTV).

Use "Video on Demand" and order films that are transmitted to you via the Internet.

– Real time

Take part in video conferences and feel as if you are sitting in the same room as the people you are talking to.

Speak to and see your chat partners.

– VoIP

Benefit from the economical telephone rates for Internet telephony (Voice over IP, VoIP). Your PC does not even need to be switched on.

◆ Setting up a local area network

The Gigaset SX686 WiMAX 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 54 Mbps. The Gigaset SX686 WiMAX complies with [IEEE 802.11g](#) standard and can work with all products that satisfy Standard IEEE 802.11b or 802.11g.

The Gigaset SX686 WiMAX

- Using the Gigaset SX686 WiMAX 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 SX686 WiMAX and make them available to all users in your network.

The Gigaset SX686 WiMAX supports **DHCP** for dynamic IP configuration of the local area network, and **DNS** for domain name mapping.

◆ Connecting phones and Internet telephony

The Gigaset SX686 WiMAX permits

- Internet telephony via the WiMAX 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 via the fixed network (if a fixed network phone is connected).

◆ Security functions

The Gigaset SX686 WiMAX 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 SX686 WiMAX for their Internet connections, which makes them 'invisible' on the Internet. The Gigaset SX686 WiMAX only allows access from the Internet if this has been requested from within the local area network.
With the firewall, the Gigaset SX686 WiMAX also offers comprehensive protection against hacker attacks.
- Service filtering
The Gigaset SX686 WiMAX can filter Internet access. Here you determine which PCs may access which Internet services.
- Access control and encryption for the local wireless network
You can use various encryption methods and authentication methods (WEP, WPA/WPA2-PSK, WPA/WPA2, MAC access control) to prevent unauthorised access to your wireless LAN or to make data illegible to unauthorised parties.

◆ Offering your own services on the Internet

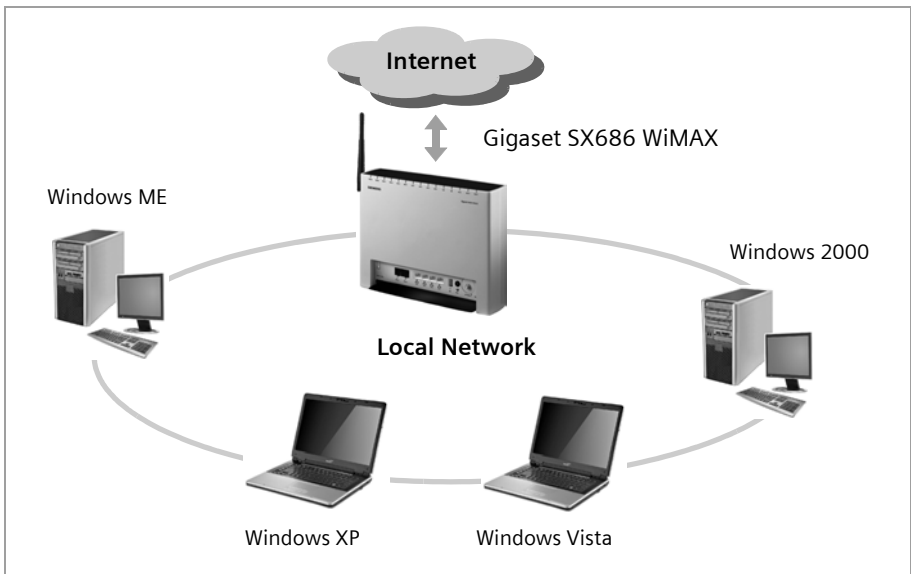
- If you want to offer your own services on the Internet, you can set up the Gigaset SX686 WiMAX as a virtual server without permitting further access to the local area network.
- **DMZ** (Exposed Host)
This allows you to release a PC in your local area network for unlimited access from the Internet. Note that in this case your local area network will no longer be adequately protected against Internet attacks.

◆ **Providing an HTTP or FTP server via USB interface**

- You can easily establish an FTP or an HTTP server for Internet access with the Gigaset SX686 WiMAX.
- You can connect a USB hub to the USB port on your Gigaset SX686 WiMAX and thereby at the same time provide a printer and a storage medium for all clients in your local area network.

Local area networks with Gigaset products

You can use the Gigaset SX686 WiMAX 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.



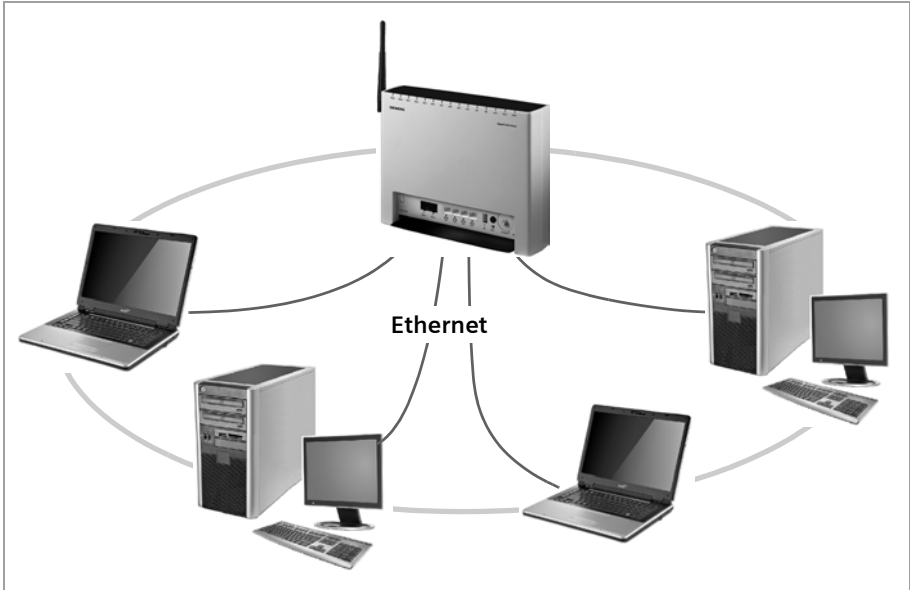
There are various ways in which you can set up the network using a Gigaset SX686 WiMAX.

- ◆ Set up a wired local area network (**Ethernet**) and allow the connected PCs access to the Internet (page 20).
- ◆ Set up a wireless local area network (**WLAN**) and allow the connected PCs access to the Internet (page 21).
- ◆ Set up a local area network comprising wireless and wired network components (page 23).

Wired local area network (Ethernet)

In a wired local area network, PCs communicate with one another via an Ethernet cable. When the Gigaset SX686 WiMAX 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 SX686 WiMAX are connected using an Ethernet cable (CAT5). There is one supplied. You can obtain additional Ethernet cables from your retailer.

The Gigaset SX686 WiMAX 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 SX686 WiMAX. 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 SX686 WiMAX 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 SX686 WiMAX.

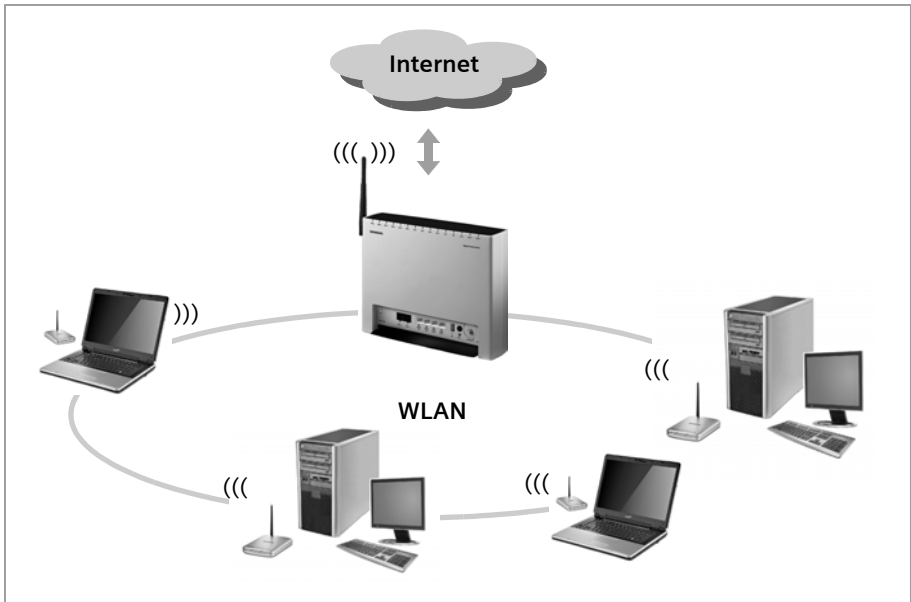
Ad-hoc mode

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.

The Gigaset SX686 WiMAX

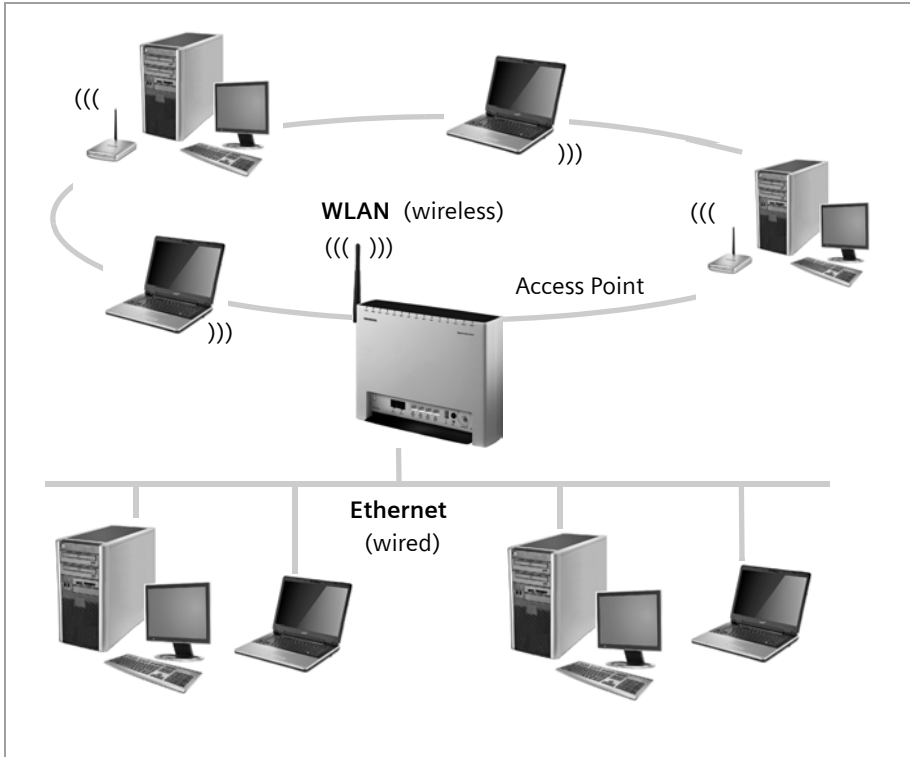
Linking wireless networks with the Internet

The Gigaset SX686 WiMAX has a WiMAX 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 WiMAX 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 SX686 WiMAX has four Ethernet interfaces (LAN ports). Up to four PCs can be connected directly to these LAN ports.

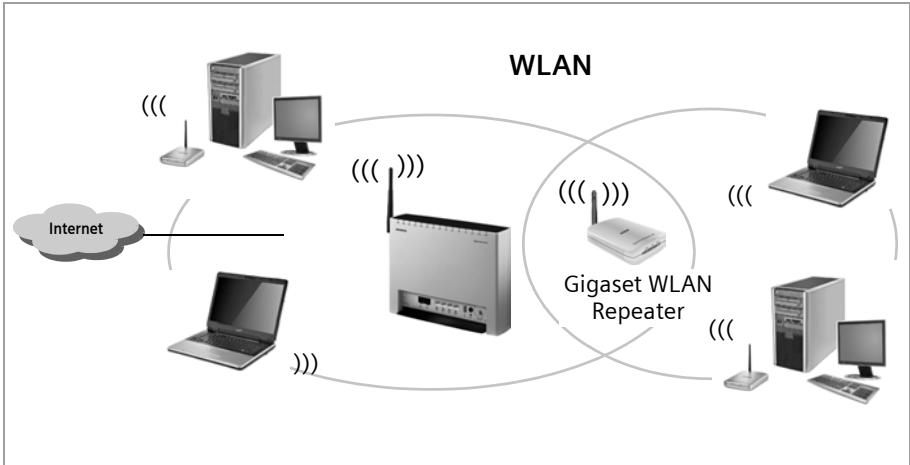
All PCs can access the Internet via the Gigaset SX686 WiMAX.

Please remember:

You can also connect an Ethernet router or switch 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 SX686 WiMAX.

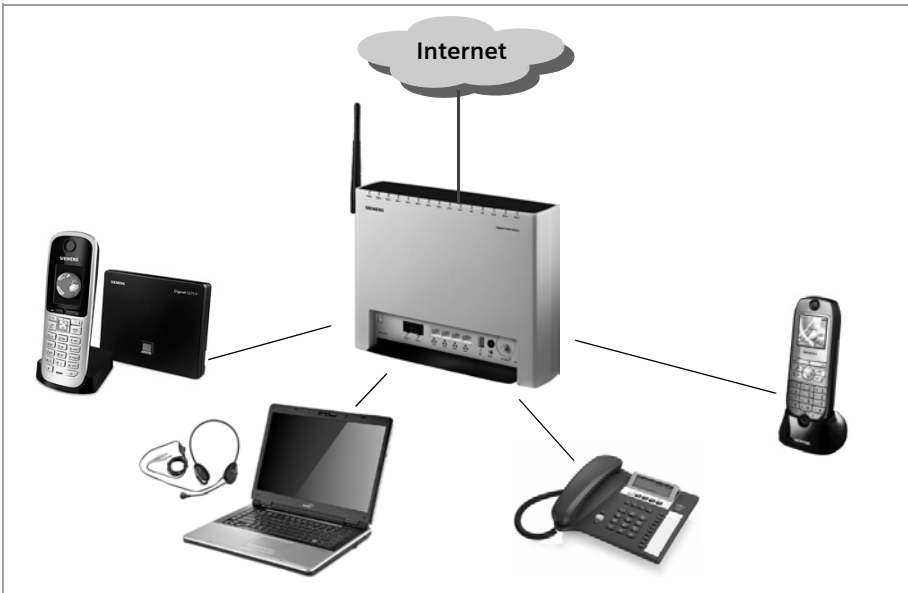


PCs to be connected in a wireless local area network via a repeater must be equipped with an integrated wireless network adapter or you have to connect an external wireless network adapter (e.g. a USB adapter).

Internet telephony and connecting analogue phones

The Gigaset SX686 WiMAX allows a combination of analogue fixed network telephony and [Internet telephony \(VoIP\)](#) over WiMAX 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 SX686 WiMAX gives you 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 SX686 WiMAX.

The PABX of the Gigaset SX686 WiMAX allows you to connect SIP phones and PCs with SIP clients (software for Internet telephony) as well as wireless SIP phones (WLAN handsets) 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.

Setting up a wireless network via WPS

Wi-Fi Protected Setup (WPS) makes it easier to establish and encrypt a wireless network. You no longer need to configure and synchronise the individual components of your wireless network manually.

A wireless network is assigned a name (SSID) and requires the encryption of data traffic to protect against the risk of unauthorised access. The access point requires authentication with an SSID and - if encryption is activated - a key to allow a WLAN adapter to access services.

WPS uses the encryption methods WPA-PSK or WPA2-PSK. Devices with WPS automatically synchronise their SSID and WPA encryption key (pre-shared key).

WPS is not possible in networks that use WEP encryption or WPA2/WPA authentication. WPS may be used without encryption.

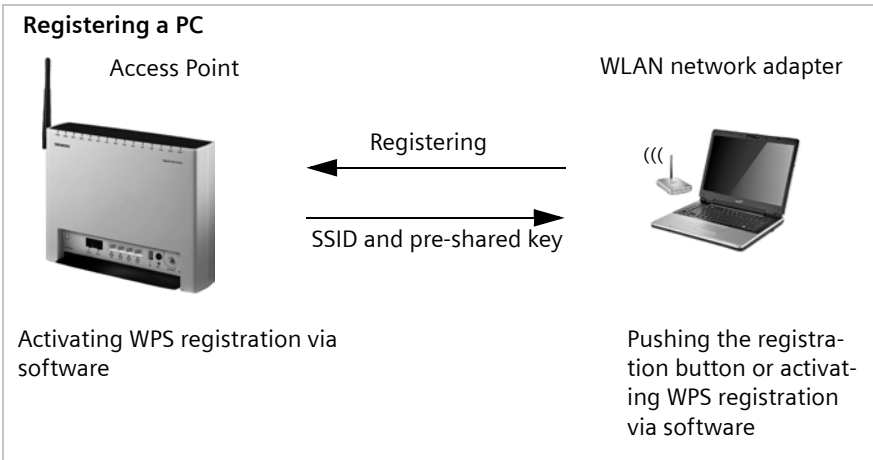
Clients without WPS can be connected manually.

WPS provides two possibilities for registration:

◆ Via registration button

The Gigaset SX686 WiMAX provides the registration button function via the user interface (see page 93).

Once the registration button has been activated, the device allows the registration of a WLAN client (repeater or wireless network adapter) during a two-minute interval.



If a client activates WPS registration within the two-minute interval, the security data is exchanged and a connection is established. Only **one** client may synchronise during the two-minute interval. After the successful synchronization the registration is closed.

If the SSID and the pre-shared key have been already set on delivery or have been configured before manually, these security data are used for registration. If this is

not the case, the first time the WPS registration is started, the device automatically creates a SSID and a pre-shared key.

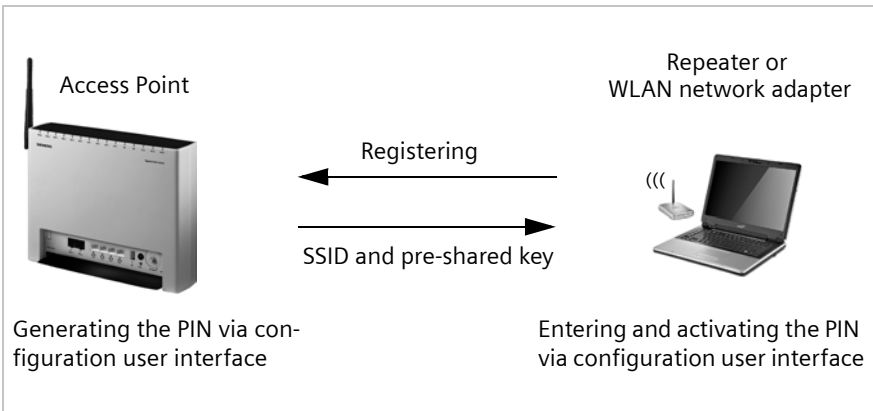
The automatically or manually created security data is valid for all further WPS registration processes. If you change this security data again manually or after a factory reset the clients have to be registered again.

◆ Via Personal Identification Number (PIN)

The PIN offers improved security for registration. No other device (e.g. in an adjacent room) can log in unnoticed. A PIN is used for registration which must be identical on both devices. If a client logs in with this PIN, the security data is synchronised. Usually the PIN of the access point is used. For security reasons a new PIN can be created.

It is also possible to create the PIN on one of the clients.

Further information you will find in chapter "Starting WPS registration and configuring WPS" on page 93.



WLAN adapters without WPS can also be set up manually, i.e. the SSID and key must be entered manually. How you can find out which SSID and which pre-shared key is set, you can read in chapter "Configuring wireless connections" on page 91.

Installing the Gigaset SX686 WiMAX

System requirements

You require the following components to operate your Gigaset SX686 WiMAX:

- ◆ A PC with
 - an 802.11g or 802.11b compatible wireless [Network adapter](#)

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.

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 SX686 WiMAX.

Note:


We recommend you use the Windows Vista or Windows XP operating system on the PCs you want to connect to the Gigaset SX686 WiMAX as only then are all system requirements for using the device fulfilled.

- ◆ To access the Internet you require
 - the access data for your WiMAX [Internet service provider](#).
- ◆ For Internet telephony you also require
 - the access data for your VoIP service provider and
 - a phone for connecting to the Gigaset SX686 WiMAX or a PC with a SIP client or a VoIP telephone.

If you use the separate WiMAX outdoor antenna (optional, not included in the scope of delivery):

The Gigaset SX686 WiMAX can only be used with the device's integrated antenna or with one of the following outdoor antennas.

3,5 GHz	18 dBi	WiMAX	Antenna Outdoor	C39453-Z5-C504	A5B00076092365
3,5 GHz	9 dBi	WiMAX	Antenna Outdoor	C39453-Z5-C505	A5B00076093200
2,6 GHz	9 dBi	WiMAX	Antenna Outdoor	C39453-Z5-C506	A5B00076093231
2,6 GHz	15 dBi	WiMAX	Antenna Outdoor	C39453-Z5-C507	A5B00076093596

	<p>3.5 GHz versions should be used for the European Economic Area. The following requirements apply: All the external antennas used for this product must undergo a conformity assessment procedure. The 3.5 GHz antennas listed here meet the European requirements and guarantee the functionality of the complete system. During the conformity assessment procedure it was ensured that the SAR limits set down in directive 99/519/EC are observed. Verification was performed using EN 50385.</p> <p>The outdoor antenna must be installed and put into service by a qualified electrician. The notes in the enclosed installation instructions must be followed</p>
---	--

This user guide assumes that installation of the outdoor antenna has been completed.

Choosing your location

The Gigaset SX686 WiMAX 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:

- ◆ Choose a location that enables you to simply set up the following connections without any further work.
 - Connect the Ethernet cable for connection to a PC or network.
 - Connect the power lead to the mains socket.
- ◆ Stand the Gigaset SX686 WiMAX upright on an even, non-slip surface.
- ◆ Lay the cables in such a way that nobody can tread on or trip over them.
- ◆ Position the Gigaset SX686 WiMAX so that you can see the LEDs.
- ◆ Do not cover the openings in the Gigaset SX686 WiMAX housing to ensure the heat can circulate; otherwise, the duty cycle of the device will be reduced or the Gigaset SX686 WiMAX switched off to avoid overheating.
- ◆ Do not operate the Gigaset SX686 WiMAX under the influence of direct heat sources (e.g. directly in the sun).
- ◆ Do not position the device in the immediate vicinity of stereo equipment, TV sets, microwave ovens or the like. This may cause interference.
- ◆ Position the Gigaset SX686 WiMAX respective the external desktop antenna so that it is as near to the centre of your wireless network as possible. The general rule is: The higher you place the WLAN antenna, the better the performance. Make sure that the place where you position the antenna offers optimum reception throughout the house, apartment or office.

Please remember:

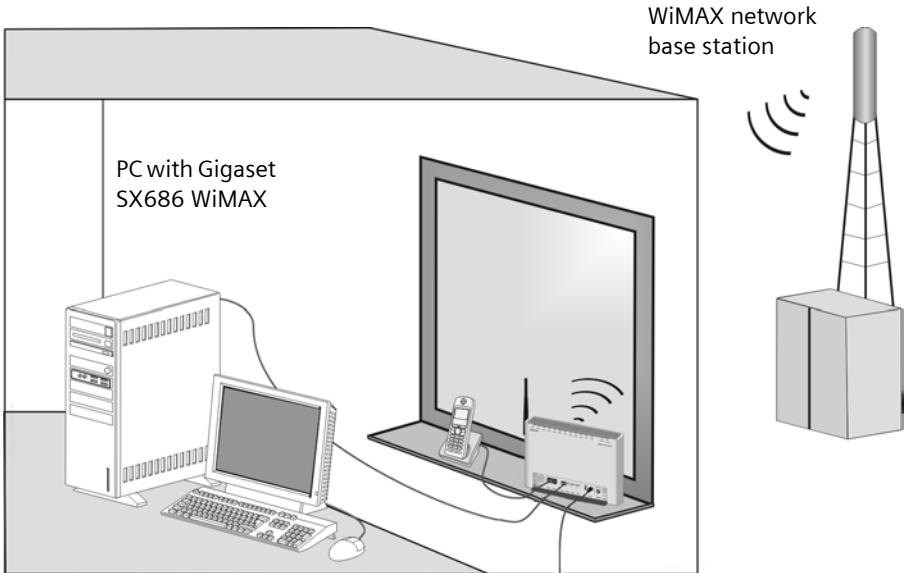
Network connections (LAN) via cables and telephone lines may only be set up with the Gigaset SX686 WiMAX within enclosed rooms.

Installing the Gigaset SX686 WiMAX

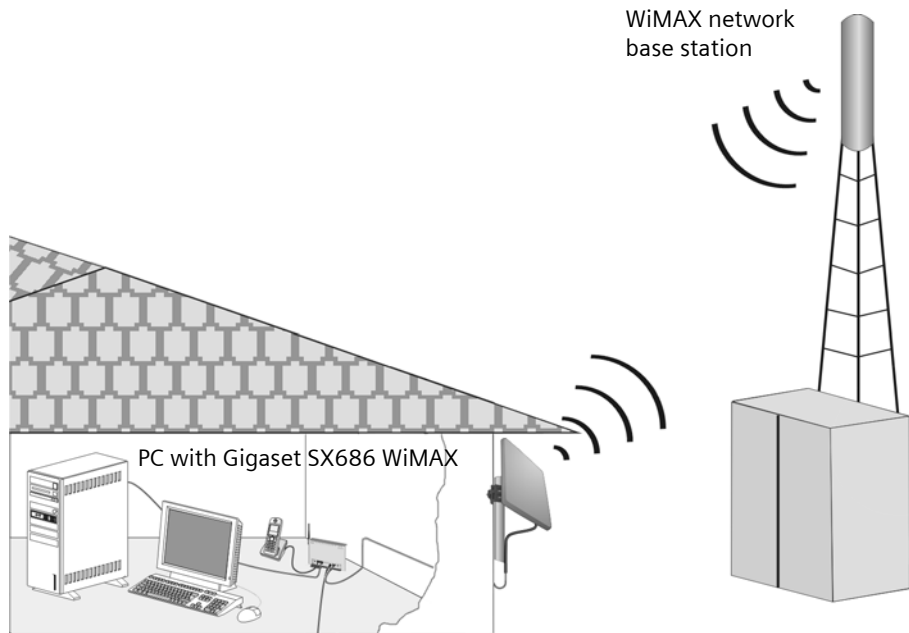
If you use the WiMAX antenna integrated into the Gigaset SX686 WiMAX:

- ◆ Position the Gigaset SX686 WiMAX directly in a window, so that the side with the LEDs and connectors is pointing into the room, towards you. Wherever possible, position the Gigaset SX686 WiMAX on one of the upper storeys. Note that obstructions, particularly doors and wall coverings containing metal can affect data transmission.
- ◆ Position the Gigaset SX686 WiMAX as far away as possible from metallic objects and coated foils.

Gigaset SX686 WiMAX with integrated antenna



Gigaset SX686 WiMAX with outdoor antenna



i

When used with the antenna integrated into the device or the outdoor antenna, the Gigaset SX686 WiMAX complies with the regulations on limiting the effect of electromagnetic fields on the general population.

Connecting and activating the Gigaset SX686 WiMAX

Installation overview

1. If you use the outdoor antenna, have it installed by a radio and television technician. Connect the antenna cable from outside to the Gigaset SX686 WiMAX.
2. Make sure that an Ethernet network card or a wireless [Network adapter](#) is installed in the PCs you want to connect to the Gigaset SX686 WiMAX. The installation is described in the user guides for these products.
3. Then make the necessary connections (PCs, phones) on the Gigaset SX686 WiMAX and activate the device.
4. Before the PCs can communicate with the Gigaset SX686 WiMAX and with each other in a local network, you may have to adapt your network settings (page 39). Configure these network settings on **one** PC first so that it can establish a connection to the Gigaset SX686 WiMAX. You can then use this PC to configure the device. To find out how to do this, refer to the section entitled "Configuring the local area network" on the CD-ROM.
5. With a wireless connection, you establish the link from the PC's wireless network adapter to the Gigaset SX686 WiMAX. This is described in the user guide for the network adapter. If the wireless network adapter provides WPS, you can establish the connection with a simple click (see page 37).
6. Then configure the Gigaset SX686 WiMAX to activate the device's Internet access (refer to the section entitled "Basic Setup Wizard" on page 46). To do this you will need the access data for your Internet service provider.

For experienced users

The default settings of the Gigaset SX686 WiMAX for LAN and WLAN configuration are:

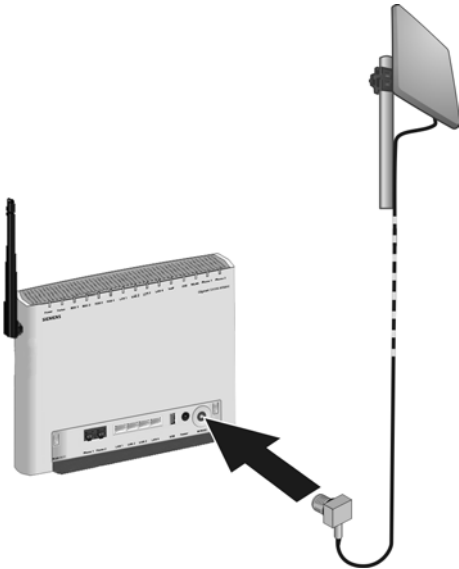
- IP address: 192.168.2.1
- Subnet mask: 255.255.255.0
- SSID: The SSID is shown on the device label.
Default SSID, e.g. ConnectionPoint,
or individual preset: SX686-XXXXXX, where XXXXXX stands for a string consisting of 0-9 and A-F.
- WLAN encryption: WPA-PSK SX686-XXXXXX
- Radio channel: 6

Caution: The Gigaset SX686 WiMAX is delivered with a preset individual encryption (WPA2-PSK/ WPA-PSK with pre-shared key). You will find this data at the label on the bottom of the device.

- ◆ If you want to connect more PCs to the Gigaset SX686 WiMAX, configure their network settings and set up the local area network accordingly (refer to the section entitled "Configuring the local area network" on the CD-ROM).

- ◆ If you want to use the Gigaset SX686 WiMAX for Internet telephony, you must configure your VoIP provider's registration data (refer to the section entitled "Setting up Internet telephony (VoIP)" on page 105).
- ◆ If you wish to use other functions of the Gigaset SX686 WiMAX, for example the comprehensive security features, use the Security Setup (page 59) or the Advanced Setup (page 69).

Connecting the outdoor antenna



- ➔ Plug the connector of the antenna cable into the **WiMAX** connector on your Gigaset SX686 WiMAX and screw tightly.

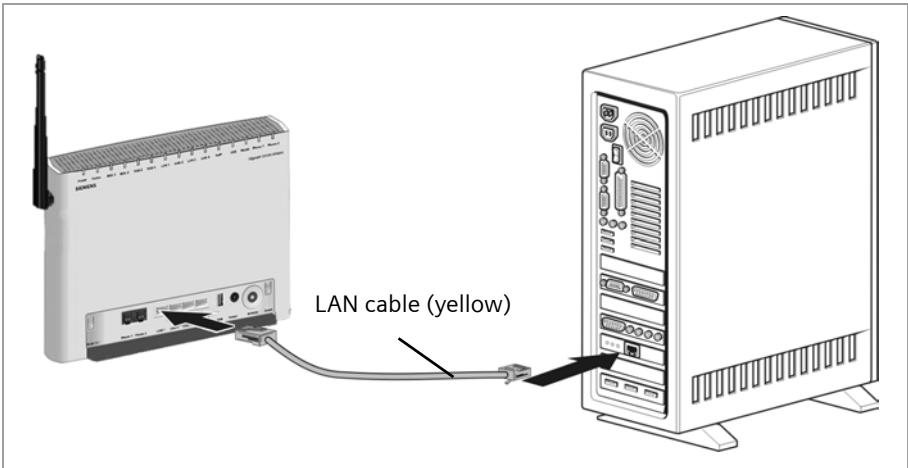
To remove the antenna cable plug, unscrew it from the antenna connector and pull the plug out.

Connecting a PC wired

You can connect wired or wireless PCs to your Gigaset SX686 WiMAX to create a local area network (LAN). Wireless connection is possible after connecting the Gigaset SX686 WiMAX to the power supply (see page 36).

First connect just **one** PC to the Gigaset SX686 WiMAX, wired connection is recommended. You can then carry out the general configuration. (If you wish to connect more PCs, please turn to page 40.)

- ➔ Connect one of the LAN ports (**LAN1 – LAN4, yellow**) on the Gigaset SX686 WiMAX to the Ethernet network card in your PC. To do this, use the LAN cable supplied (CAT5, **yellow**).



Connecting a telephone, fax machine or answer machine

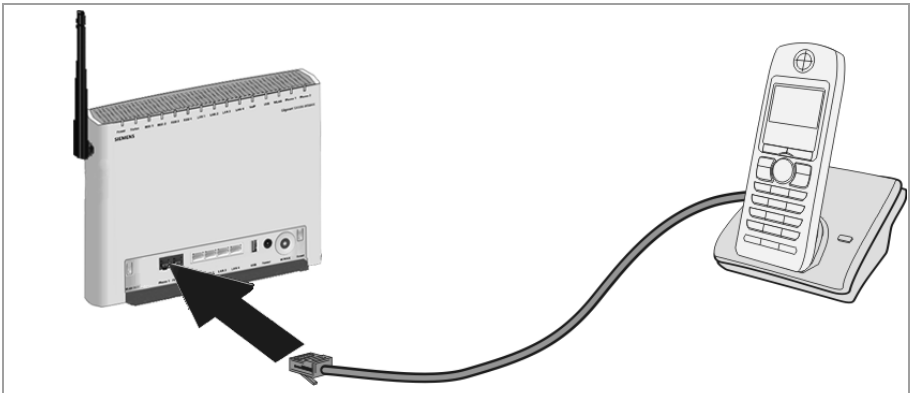
You can connect an analogue terminal, such as a telephone with cord, cordless telephone, fax machine or answer machine, and operate them via the Internet in future (Internet telephony/VoIP).

Note

Depending on the connection plug on your analogue terminal, you may require an additional adapter (TAE socket on the RJ11 plug).

Connect the Gigaset SX686 WiMAX with the analogue phone as follows:

- ➔ Insert the plug of the telephone into the **Phone 1** or **Phone 2** port on the Gigaset SX686 WiMAX.



If your analogue terminal has a TAE plug, first connect this to the adapter (connect a telephone to the F-coded socket, a fax machine or answer machine to the N-coded socket). Then connect the adapter plug to one of the **Phone** connections on the Gigaset SX686 WiMAX.

- ➔ If necessary connect the telephone, fax machine or answer machine to the mains power supply.

Note:

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

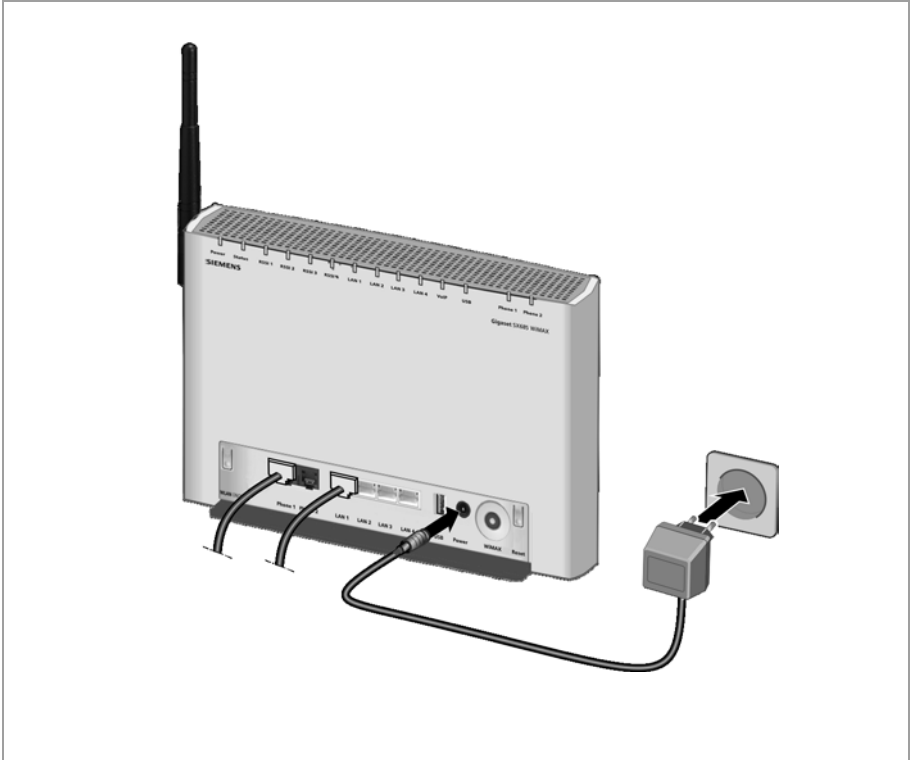
Connecting to the mains power supply

Please remember:

Only use the mains adapter supplied with the device (12V DC 2A).

- ➔ Connect the mains adapter cable to the **Power** socket on the Gigaset SX686 WiMAX.
- ➔ Plug the mains adapter into a mains socket.

The Gigaset SX686 WiMAX is now switched on and ready for operation.



The system starts up and performs a self-test. After the self-test, the Gigaset SX686 WiMAX continually attempts to register with a WiMAX network. Registration may be successful immediately. If not, registration will take place when the Gigaset SX686 WiMAX is being configured. You can check whether your device is already registered with a WiMAX network via the **Status** LED (see page 14).

Connecting PCs wirelessly

Wireless via WPS

If you are using WPS (see page 26), you can easily make a wireless connection to other WLAN devices.

- ➔ Activate the WPS registration via the corresponding function in the user interface to start WPS registration (see page 57).
- ➔ During the two-minute interval, activate WPS registration of the wireless network adapter on the PC. The client receives the security data for the Gigaset SX686 WiMAX (SSID and pre-shared key) and is thereby registered.

WLAN LED display during WPS registration:

On (300 sec)	WPS registration was successful.
Flashing slowly	WPS registration is in progress.
Flashing quickly	WPS registration was not successful.
Flashing quickly with interruption	More than one client tried to register.

Only one client may register during an individual registration phase. If the device indicates by means of the WLAN LED that more than one client has tried to register, there is no client registered. You can start WPS registration again after a short time.

If the LED indicates a successful WPS registration, the desired client, however, has no connection to the Gigaset SX686 WiMAX and has not been registered successfully, an external device may have connected to your WLAN. In this case, you should modify the WPA-PSK key as quickly as possible (see page 63) or perform a factory reset (see page 16) and perform WPS registration for the clients using a PIN (see page 57).

For additional WPS registration options see chapter "WPS Registration" on page 57.

For the wireless connection of additional PCs without WPS function see page 40.

Wireless without WPS

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 54 or the Gigaset USB Adapter 54.

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

- ➔ You should therefore enter the SSID for the Gigaset SX686 WiMAX in your network adapter configuration. You will find the default SSID for the Gigaset SX686 WiMAX at the label on the bottom of the device (e.g. ConnectionPoint or SX686-XXXXXX, where XXXXXX is an individual string consisting of 0-9 and A-F).

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

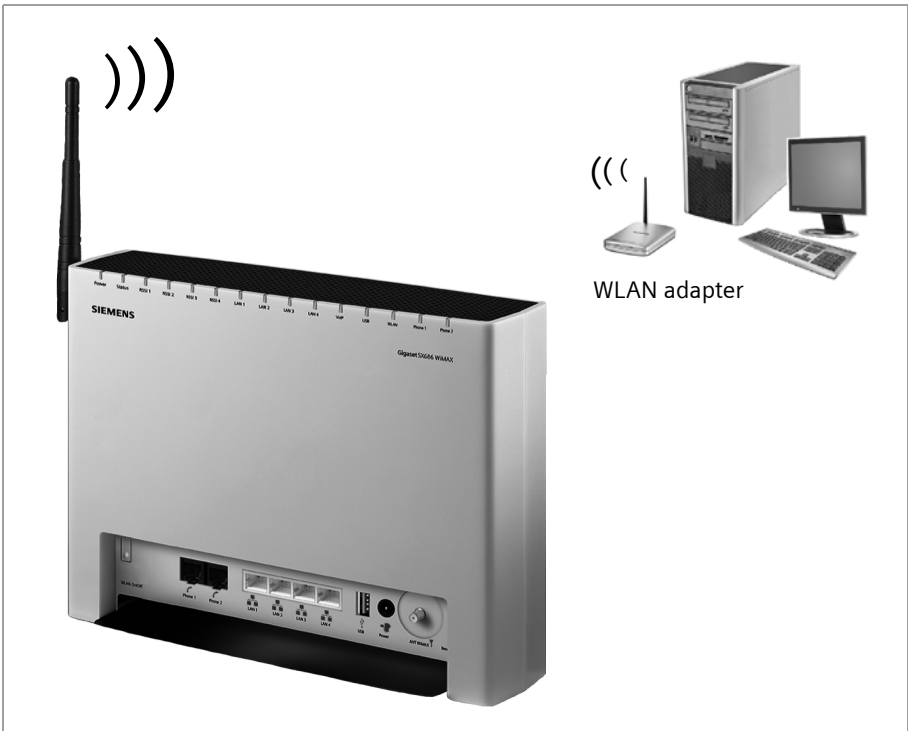
Installing the Gigaset SX686 WiMAX

The Gigaset SX686 WiMAX is delivered with preset individual encryption (WPA2-PSK/ WPA-PSK with pre-shared Key). You will find this key at the label on the bottom of the device.

→ Choose the encryption method WPA2-PSK/ WPA-PSK in the configuration settings of your network adapter and enter the pre-shared key of you Gigaset SX686 WiMAX.

If one of your network adapters do not provide this encryption method, you must change the encryption method at the Gigaset SX686 WiMAX (see page 94) and then configure the encryption appropriately for all network adapters. The settings at the Gigaset SX686 WiMAX should be performed only with a wired connected PC

If the correct SSID and encryption has been entered in your PC's wireless network adapter, the wireless link will be established automatically.



Checking the operating state

Your Gigaset SX686 WiMAX is now ready for use. The LED displays on the front panel of the Gigaset SX686 WiMAX provide information about the operating state (see page 13).

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

- ◆ The **Power** LED on the front lights up green.
- ◆ If registration with a WiMAX network has already been successful, the **Status** LED lights up green. The **RSSI 1 - RSSI 4** LEDs indicate the signal strength.
If the **Status** LED does not light up, register your Gigaset SX686 WiMAX during configuration.
- ◆ The **WLAN** LED lights up to indicate that the Gigaset SX686 WiMAX 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 SX686 WiMAX. 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 167).

Network configuration of the PCs

In order to communicate via the Gigaset SX686 WiMAX, the **network configuration** may have to be set up on the connected PCs.

With

- ◆ **Windows Vista** or
- ◆ **Windows XP** or
- ◆ **Windows 2000** and
- ◆ **Mac OS X**

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 SX686 WiMAX (page 41).

If you want to connect additional PCs to the Gigaset SX686 WiMAX, 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 SX686 WiMAX. 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 and encryption of all wireless network components (Gigaset SX686 WiMAX and network adapters) is **identical**.

You will find the default SSID at the label on the bottom of the device.

If you have connected a PC via WPS, you will find the created SSID in the **Advanced Settings** of the user interface (see page 91). You can see the preset pre-shared key at the label on the bottom of the device or also via the user interface in the **Advanced Settings** menu (see page 91). You use this information to manually configure PCs without WPS.

PCs with WPS can be connected wirelessly via WPS (see page 37 and page 93).

- ➔ If necessary, set up the network for each newly connected PC (page 39).
- ➔ Reboot the additional PCs.

Wired

- ➔ Connect the network cards of each additional PC to a free LAN port (**LAN1 – LAN4**) on the Gigaset SX686 WiMAX using an Ethernet cable.
- ➔ Make sure that the corresponding LAN LED on the front of your Gigaset SX686 WiMAX flashes.
- ➔ If necessary, set up the network for each newly connected PC (page 39).
- ➔ Reboot the additional PCs.

The user interface

You have connected a PC to the Gigaset SX686 WiMAX and possibly made the settings in the local area network. You can now configure the Gigaset SX686 WiMAX using this PC via the user interface. 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.

If you use Window Vista or Windows XP Service Pack 2, you will need to configure the popup blocker.

You will find additional information on these two points on "Deactivating HTTP proxy and configuring a pop-up blocker" on page 173.

If you use a firewall, it must allow connection to the Gigaset SX686 WiMAX. For details, refer to the user guide for your firewall. If necessary, deactivate the firewall while you configure your Gigaset SX686 WiMAX.

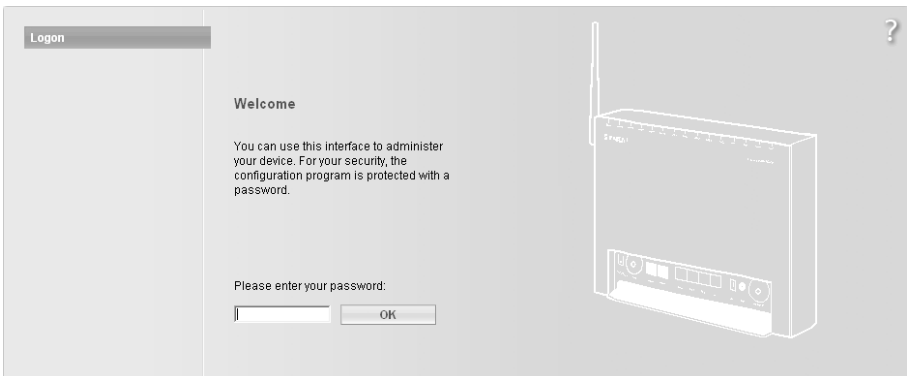
Starting the user interface

To access the user interface of the Gigaset SX686 WiMAX:

- ➔ Start your Internet browser.
- ➔ Enter the IP address of the Gigaset SX686 WiMAX in the browser's address field:

http://sx686 or **http://192.168.2.1**

The login screen appears:



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

- ➔ Enter the password.

The user interface

→ Click **OK**.

Note:

For security reasons you should change this password at a later stage (page 60).

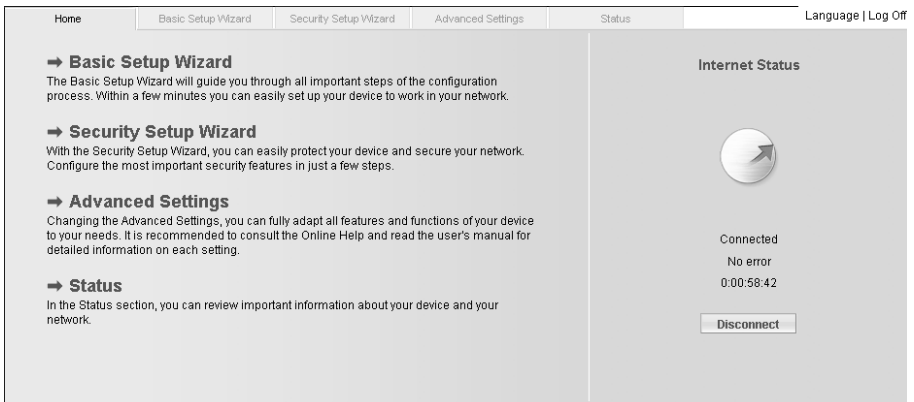
A screen with security information will appear. You can skip this when configuring the device for the first time. If you carry out all the general and security settings using the wizard as described below, your device and network will be fully protected. If not, the next time you log on you will be informed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

→ Click **OK**.

The start screen is displayed.

The start screen

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



Start screen functions

You can start the following actions on the start screen:

- ◆ Select the language for the user interface (page 44).
- ◆ When you have established a connection to the WiMAX network and configured an Internet connection for the first time, you can 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 44). The start screen shows the status and also the button **Connect** or **Disconnect**.
- ◆ Open the **Status** menu to obtain status information about the Gigaset SX686 WiMAX (page 136).
- ◆ Call up the wizard for the basic configuration (**Basic Setup Wizard** see page 46),
- ◆ Call up the **Security Setup Wizard** (page 59).
- ◆ Open the **Advanced Settings** menu for additional configuration options (page 69).

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.

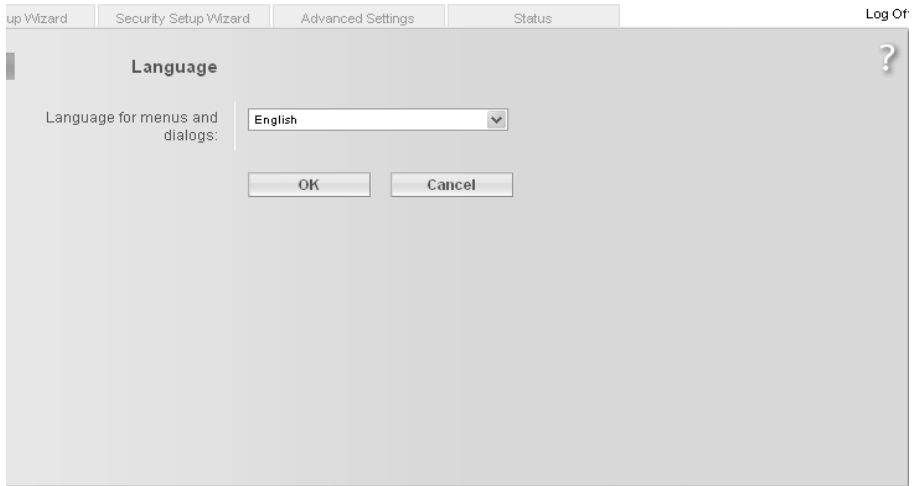
The configuration program comprises the following functions:

- Basic Setup Wizard** Use this wizard to make the settings required for connecting to the Internet. You align your WiMAX antenna to obtain optimum reception and establish the connection to the WiMAX network, configure your Internet account, select your region and configure Internet telephony. Additionally, you can perform a WPS registration. This is described from page 46.
- Security Setup Wizard** This wizard allows you to take security precautions against unauthorised access to the Gigaset SX686 WiMAX and the local network. You can assign a password and set up encryption for wireless traffic. This is described from page 59. 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 Internet telephony, back up and restore the configuration data, set up the Gigaset SX686 WiMAX as a virtual server for the network, configure a Web server, a file server or a print server and perform other functions as required. These configuration steps are optional and can be carried out at a later stage. This is described from page 69.
- Status** You can view information about the configuration and status of the Gigaset SX686 WiMAX in the Status menu. This is described from page 136.
- Language** You also have the opportunity to specify the language for the user interface (page 44).

Selecting a language

The user interface can be presented in various languages.

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



- ➔ 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 54 and page 72), 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.

To establish or end an Internet connection manually:

- ➔ Open the start screen of the Gigaset SX686 WiMAX as described on page 41.
 - 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 require the connection.

Elements in 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.
- ◆ *Cancel* returns you to the start screen. This button is not available for the initial configuration of the device.

Buttons in the *Advanced Settings* menu

OK Transfers the settings you have made to the Gigaset SX686 WiMAX configuration.

Cancel Deletes all the entries on a screen since the last time you clicked **OK**.

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 guides you step by step through the general configuration of the Gigaset SX686 WiMAX. This includes

- ◆ choosing and aligning the WiMAX antenna as well as connection establishment and fine tuning to obtain optimum reception,
- ◆ the settings for your region,
- ◆ setting up your Internet access,
- ◆ setting up your VoIP account and
- ◆ registering a WLAN client via WPS.

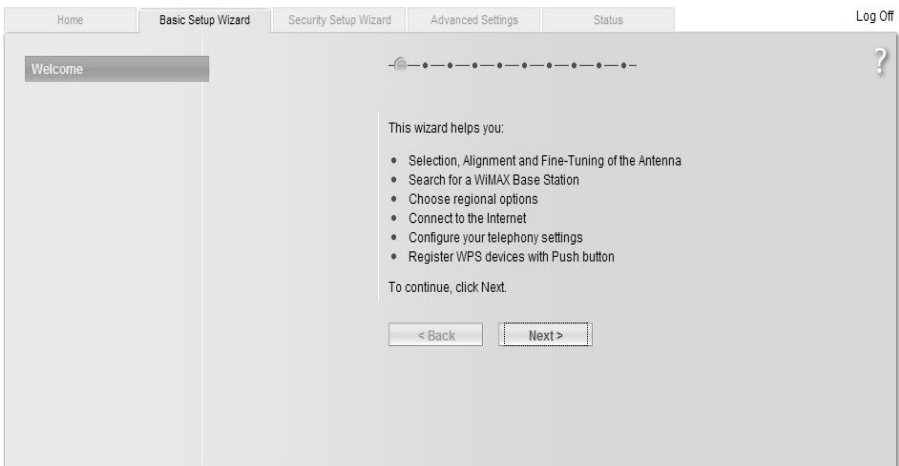
Connection to the [Internet](#) is established via the Gigaset SX686 WiMAX for all PCs connected to it. You need your [Internet service provider's](#) access data for the configuration. Please have this data to hand.

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 SX686 WiMAX during configuration. Before passing the device on to somebody else or having your dealer replace it, you should always reset the configuration of your device to its factory settings (page 134). Otherwise, unauthorised persons may use your Internet access at your expense.

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



➔ Click **Next >**.

Choosing the antenna

On this screen you choose if you want to operate your Gigaset SX686 WiMAX with an internal or external antenna.

The screenshot shows the 'Basic Setup Wizard' interface. At the top, there are navigation tabs: 'Home', 'Basic Setup Wizard' (selected), 'Security Setup Wizard', 'Advanced Settings', and 'Status'. A 'Log Off' link is in the top right corner. The main content area is titled 'Usage of the Antenna' and contains the following text: 'Please select whether there is an external antenna connected to the device or not.' Below this text are two radio button options: 'Gigaset without an external antenna' (which is selected) and 'Gigaset with an external antenna'. At the bottom of the form are two buttons: '< Back' and 'Next >'. A progress indicator at the top shows a series of dots, with the first dot being filled, indicating the current step in the wizard.

- ➔ Choose ***Gigaset without an external antenna*** if you are using the antenna integrated in the Gigaset SX686 WiMAX.
- ➔ Choose ***Gigaset with an external antenna*** if you received the outdoor antenna together with your Gigaset SX686 WiMAX. The outdoor antenna must already have been installed and connected by a qualified electrician.
- ➔ Click ***Next >***.

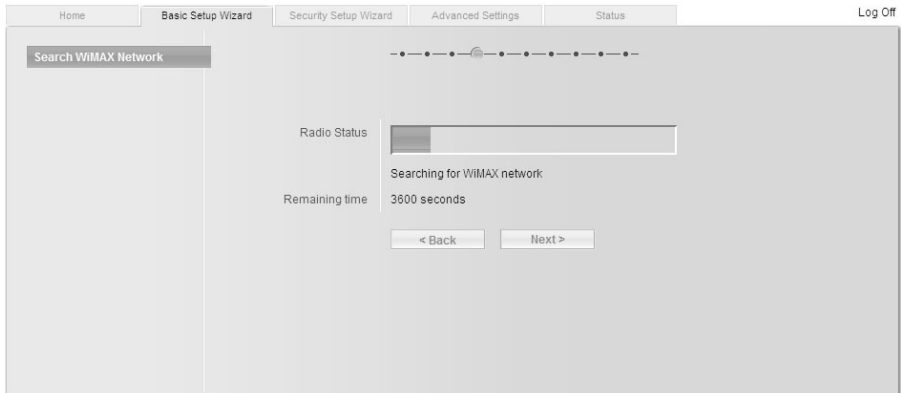
Aligning the antenna



- ➔ If you are using the antenna integrated in the Gigaset SX686 WiMAX, align it towards the window. Your Gigaset SX686 WiMAX is already standing by the window with the cable connections turned inwards and is connected.
- ➔ If you are using the outdoor antenna, align the antenna later.
- ➔ Click **Next >**.

Searching a WiMAX network

The frequency scan begins automatically.



The frequency scan begins automatically. A progress bar indicates how far the scan has progressed. In addition, you will see in the **Remaining time** area roughly how much time is still needed for the complete scan. Depending on how your Gigaset SX686 WiMAX has been preconfigured by your provider, the scan can last several minutes before the first radio connection is established.

Note

During the scan, the Gigaset SX686 WiMAX or antenna must not be moved; this is the only way to guarantee a complete scan with the current antenna alignment.

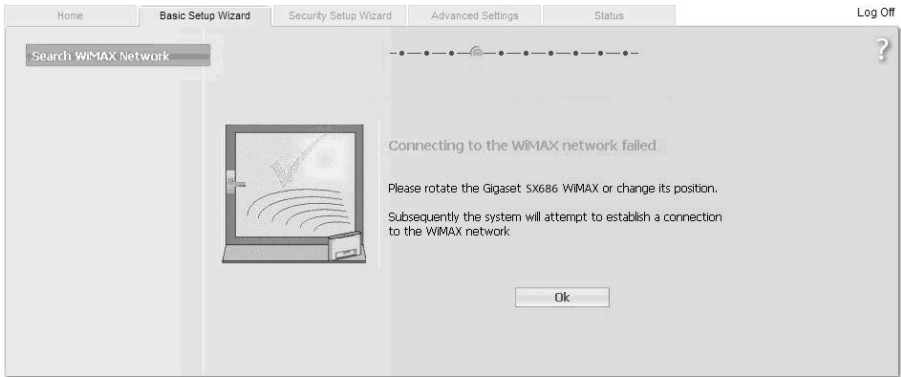
As soon as a radio connection has been established with a WiMAX network, the scan will end. The progress bar is fully filled in and the display in the **Remaining time** area jumps to **0 seconds**.

- ➔ When a connection to a WiMAX network has been established, click on **Next >** to make fine adjustments to the antenna.
- ➔ Read on in Chapter "Antenna fine tuning" on page 52.

If the scan has not been successful:

The following screen is displayed.

Basic Setup Wizard



Both the integrated antenna and the outdoor antenna are directional antennae; this means that they must at least be pointing roughly in the direction of a WiMAX network base station in order to establish a radio connection.

If the scan was unsuccessful, align the antenna differently:

If you are using the antenna integrated in the Gigaset SX686 WiMAX:

➔ Turn your Gigaset SX686 WiMAX by approx. 60°.

Correct:



Incorrect:



➔ Click on **OK** to restart the scan.

Note

You must not move the Gigaset SX686 WiMAX during the scan. You should therefore always place the Gigaset SX686 WiMAX upright and on a level surface directly by the window.

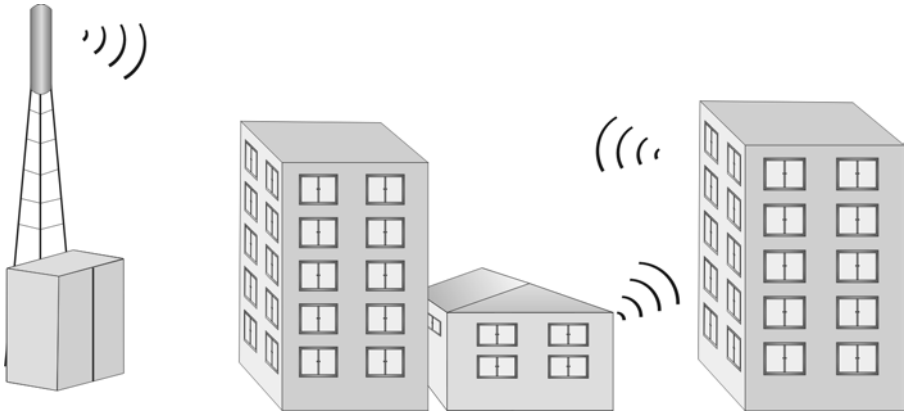
If the scan has still not been successful with the alignment changed:

➔ Place the Gigaset SX686 WiMAX by a window that faces a different direction.

- ➔ If necessary, repeat the scan with all possible locations and alignments.
- ➔ If necessary, ask your provider for the location of the nearest WiMAX network base station and select a location for your Gigaset SX686 WiMAX that points towards this base station.

The best results will be obtained if the Gigaset SX686 WiMAX is in sight of a WiMAX network base station.

If a line of sight is not possible, you can reflect the radio waves off neighbouring buildings. To do this, direct the Gigaset SX686 WiMAX at the building it is reflecting off and not at the WiMAX network base station.



If you are using the outdoor antenna:

- ➔ The qualified electrician turns the antenna through 20° in the vertical axis. Then the scan is repeated by clicking on the **OK** button.
- ➔ If necessary, the scan should be repeated with all possible antenna alignments.

Antenna fine tuning

Once you have established a wireless connection to a WiMAX network, align your Gigaset SX686 WiMAX or antenna precisely using the connection wizard.

Note

Take extra care to align the Gigaset SX686 WiMAX or outdoor antenna precisely. The better the connection quality, the faster your Internet connection will be in the future.

To obtain precise alignment of the Gigaset SX686 WiMAX or antenna, turn it a little at a time. If you use the antenna integrated in the Gigaset SX686 WiMAX, you can also move the device a little at a time to optimise the reception quality.



The quality of the radio connection is represented graphically by a signal strength bar. The longer the bar is, the better the radio connection. Try to obtain the best possible radio connection setting.

- ➔ If you are using the antenna integrated in the Gigaset SX686 WiMAX: Memorise the current location and alignment of your Gigaset SX686 WiMAX, so that you can restore it if the connection is broken.
- ➔ Turn or move the Gigaset SX686 WiMAX or turn the antenna a little at a time and note the signal strength display. Use this to move the antenna to the position with the best signal strength.

You can also determine the quality of the connection by how many of the 4 LEDs indicating signal strength light up on the device (**RSSI 1 – RSSI 4**). The more LEDs that light up, the better the connection quality.

If you have turned your Gigaset SX686 WiMAX or the antenna too far, the connection might break. You should then return to the alignment that provided a connection and repeat the procedure for establishing a connection to the WiMAX network. Then make any fine adjustments step by step.

When your Gigaset SX686 WiMAX or outdoor antenna is optimally aligned:

- ➔ Click **Next >**.
- ➔ Make sure that in future your Gigaset SX686 WiMAX or outdoor antenna is always in the set position.

Regional Options

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

- ➔ 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 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 70) menu.

The screenshot shows the 'Basic Setup Wizard' interface. At the top, there are navigation tabs: 'Home', 'Basic Setup Wizard' (selected), 'Security Setup Wizard', 'Advanced Settings', and 'Status'. A 'Log Off' link is in the top right corner. Below the tabs is a progress indicator with a question mark icon. The main content area is titled 'Internet Connection' and contains the following fields and options:

- Service provider:** A dropdown menu with 'Other' selected.
- Protocol:** A dropdown menu with 'Dynamic IP' selected.
- MTU:** A text input field containing '1500'.
- PPPoE pass-through:** Radio buttons for 'On' and 'Off', with 'Off' selected.
- UPnP Connection:** Radio buttons for 'On' and 'Off', with 'Off' selected.
- Test Settings:** A button.
- < Back** and **Next >** buttons.

- ➔ 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.
- ➔ Choose the **Protocol** which is used for your Internet connection.
- ➔ Leave the default settings for further parameters 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 service provider correctly.

PPPoE pass-through

PPPoE pass-through allows you to use an additional Internet connection (through another service provider) on one PC.

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

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. Further information about this can be found on page 74.

➔ Activate **UPnP** if you wish to use this function.

Test settings

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

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

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

➔ 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.

The screenshot shows the 'Telephony' configuration page in the Basic Setup Wizard. The page is divided into several sections:

- VoIP account:** Radio buttons for 'On' (selected) and 'Off'.
- Service provider:** A dropdown menu with 'Other' selected.
- User name:** An empty text input field.
- Displayed name:** An empty text input field.
- Authorization user name:** An empty text input field.
- Password:** An empty text input field.
- Confirm password:** An empty text input field.
- SIP domain:** An empty text input field.
- SIP realm:** An empty text input field.
- SIP listen port:** A text input field containing '5060'.
- Proxy server address:** An empty text input field.
- Proxy server port:** A text input field containing '5060'.
- Registrar server address:** An empty text input field.
- Registrar server port:** A text input field containing '5060'.
- Voice codecs:** A section with 'Selected codecs' and 'Available codecs'. The 'Selected codecs' list includes: 6.729a (*), 6.729 (*), 6.723-14300 (*), 6.726-32000 (*), 6.726-40000 (*), 6.711ALaw(*), and 6.711MuLaw(*). The 'Available codecs' list includes: 6.726-16000 (*), 6.726-24000 (*), 6.728a (*), 6.728, 6.723-14300 (*), 6.722, and 6.722.1.
- Out-of-band DTMF:** Radio buttons for 'Off' (selected), 'RFC2833', and 'SIP-Info'. A 'Clear' button is located below these options.

At the bottom of the page, there are '< Back' and 'Next >' buttons.

- ➔ Select the option **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** and **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 >**.

WPS Registration

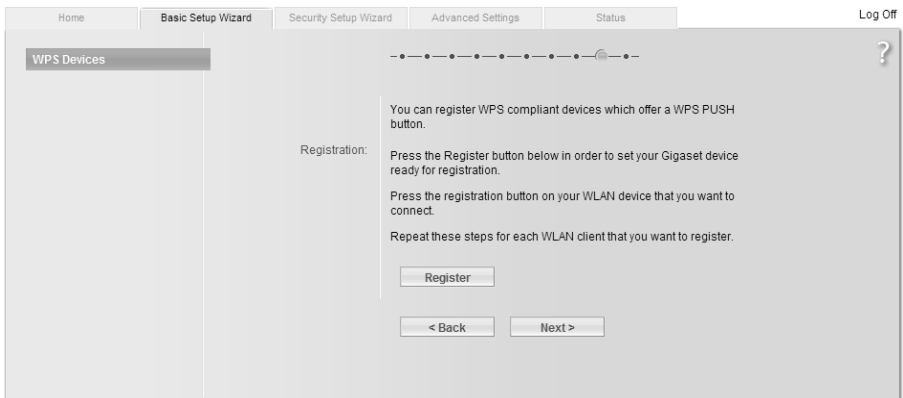
Wi-Fi Protected Setup (WPS) makes it easier to establish a wireless network. Devices equipped with WPS can create and synchronise an SSID and a WPA key (pre-shared key) automatically. These security data can be created in different ways:

- They are generated automatically on initial WPS registration.
- They have been previously configured manually.
- The device has been delivered with preset security data.

All you need to do to establish a secure wireless connection is

- ◆ for devices with hardware button – to press the registration (or Scan) button on the access point and on the client or
- ◆ for devices without hardware button – to activate the WPS registration in the user interface of the access point and the client.

For further information, see "Setting up a wireless network via WPS" on page 26.



➔ Click **Register** to start WPS registration.

Once WPS registration is activated, the device searches for a WPS client within range. Any WPS client within range that activates the WPS function during the two-minute interval receives the Gigaset SX686 WiMAX security data (SSID and pre-shared key) and is thereby registered.

The registration progress is shown in the window.

You can repeat these steps for each WLAN client to be registered.

Only one client may register during the two-minute interval. If two clients try to register at the same time, the registration will be broken down and an error message appears.

➔ To go to the next step, click **Next >**

Summary

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



- ➔ 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 SX686 WiMAX 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 SX686 WiMAX 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 options for improving your network security. You can:

- ◆ Assign a password for configuring the Gigaset SX686 WiMAX (page 60),
- ◆ Change the SSID for your wireless network (page 61),
- ◆ Set up the [Encryption](#) for the wireless network (page 62),
- ◆ Limit access to the wireless network to certain PCs (page 66).

The user interface of the Gigaset SX686 WiMAX 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 again, click **< Back**.

When using WPS please note the following:

Your Gigaset SX686 WiMAX is equipped with [WPS](#) (Wi-Fi Protected Setup). You can use it to set the security of your wireless network easily with one click only (see page 26).

If no manual configuration of security data has been performed before, with the WPS registration the SSID and pre-shared key (WPA2-PSK/WPA-PSK) are used which are shown on the device label.

You can also inspect the SSID and the pre-shared key used in the **Security Setup Wizard** or in the **Advanced Settings**, see page 61 and page 91 or page 62 and page 95.

- ➔ 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.



- ➔ 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 SX686 WiMAX is protected with the **admin** password. To prevent unauthorised changes to the configuration, you should change the password at regular intervals.

Setup Wizard | Security Setup Wizard | Advanced Settings | Status | Log Off

Progress: [Step 1 of 4]

Please set a new password for your device in order to prevent unauthorized access to the configuration program.

Current password:

New password:

Confirm new password:

< Back | Next > | Cancel

- ➔ 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 may contain up to 20 characters. Note case sensitivity. Avoid proper names and all too obvious words. Use a combination of letters, digits and special characters.

Note:

If you ever forget your password you will have to return the Gigaset SX686 WiMAX to its factory settings (page 134). 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 >**

Changing the SSID

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

The Gigaset SX686 WiMAX is delivered with a preset SSID. You will find it at the label on the bottom of the device. This can be a default SSID, e.g. ConnectionPoint, or a SSID which is individually set for each device in the format SX686-XXXXXX, where XXXXXX is a string consisting of 0-9 and A-F, e.g. SX686-EB691A.

For security reasons you can change this SSID and deactivate SSID broadcast. If this option is enabled, your wireless network will be visible for other wireless network users. In this case, unauthorised persons could use the SSID to gain access to your network.

If you have performed a successful WPS registration before a manual configuration of security data, this screen shows the generated SSID. Make a note of this SSID. You will need it to manually configure the wireless network adapters that do not support WPS.

➔ If you are using WPS registration, click on **Next >**.

➔ Enter a character string of your choice in the **SSID** field. The SSID is case-sensitive. It can contain up to 32 characters. Use a combination of letters, digits and special 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 for further wireless connections to the Gigaset SX686 WiMAX.

➔ Click **Next >**.

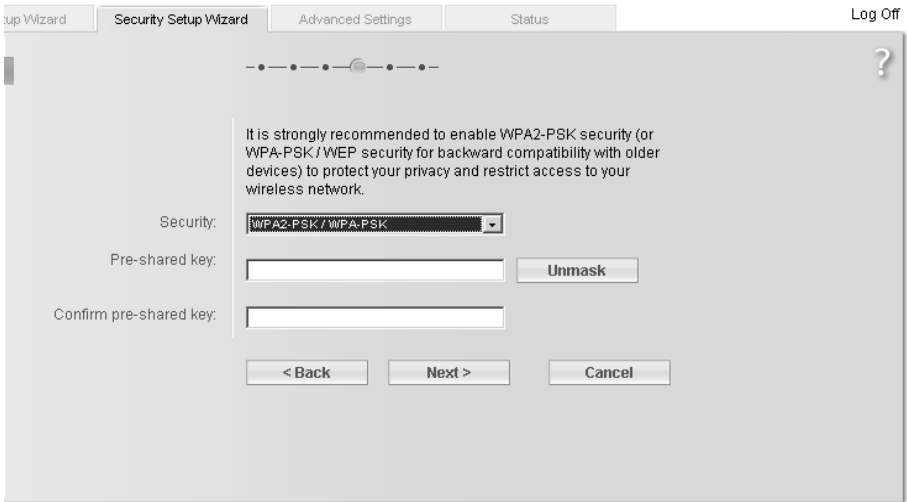
Setting up security functions for the wireless network

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 SX686 WiMAX makes use of effective encryption methods to prevent unauthorised eavesdropping as far as possible.

The Gigaset SX686 WiMAX is delivered with preset individual encryption (WPA2-PSK/WPA-PSK with pre-shared key). You will find this key at the label on the bottom of the device.

If all components of your wireless network provide this encryption method there is no need of any settings in this screen. If not, or if you want to change the preset key (e. g. if unauthorised persons may have access to your device), you can configure the encryption for your wireless network in the next step.



You can use the following security mechanisms:

- ◆ WPA2-PSK, WPA-PSK or WPA2-PSK/WPA-PSK (page 63)
- ◆ WEP encryption (Wired Equivalent Privacy, see page 64)

You will find further options for setting up data encryption and authentication in the **Advanced Settings** menu (page 94).

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 Integrity 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. Information about this can be found in the operating manual for your network adapter.

This screen shows the preset encryption settings.

➔ If you do not want to change the encryption settings, click on **Next >**.

If you want to change the pre-shared key:

- ➔ Select **WPA2-PSK** if WPA2 is supported by all components in the wireless network.
- ➔ Select **WPA-PSK** only if WPA is supported by all components in the wireless network.
- ➔ Select **WPA2-PSK / WPA-PSK** if only some components in the wireless network support WPA.

- ➔ Enter a key of your choice in the **Pre-shared key** field (min. 8 to max. 63 characters or hexadecimal characters [0-9, A-F]) and confirm it by repeating the entry. You must set up the same pre-shared key for all wirelessly connected PCs. Use a combination of letters, digits and special characters.

Security Setup Wizard

- ➔ By clicking the **Unmask** button, a message showing the pre-shared key is output in readable characters.
- ➔ 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 63), we recommend that you activate [WEP Encryption](#).

WEP encryption and WPS registration cannot be used together in a wireless network.

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 SX686 WiMAX and all your wireless network adapters.

The screenshot shows the 'Security Setup Wizard' window with the following elements:

- Navigation tabs: 'Setup Wizard', 'Security Setup Wizard' (active), 'Advanced Settings', 'Status'. A 'Log Off' link is in the top right.
- Progress indicator: A series of dots with the second dot highlighted.
- Help icon: A question mark '?' in the top right corner.
- Text: 'It is strongly recommended to enable WPA2-PSK security (or WPA-PSK / WEP security for backward compatibility with older devices) to protect your privacy and restrict access to your wireless network.'
- Fields:
 - Security: WEP (dropdown)
 - Key length: 64 bits (dropdown)
 - Input type: Key (dropdown)
 - Key type: HEX (dropdown)
 - Key: [Empty text box]
 - Confirm key: [Empty text box]
- Buttons: '< Back', 'Next >', 'Cancel'.

- ➔ 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**, **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

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

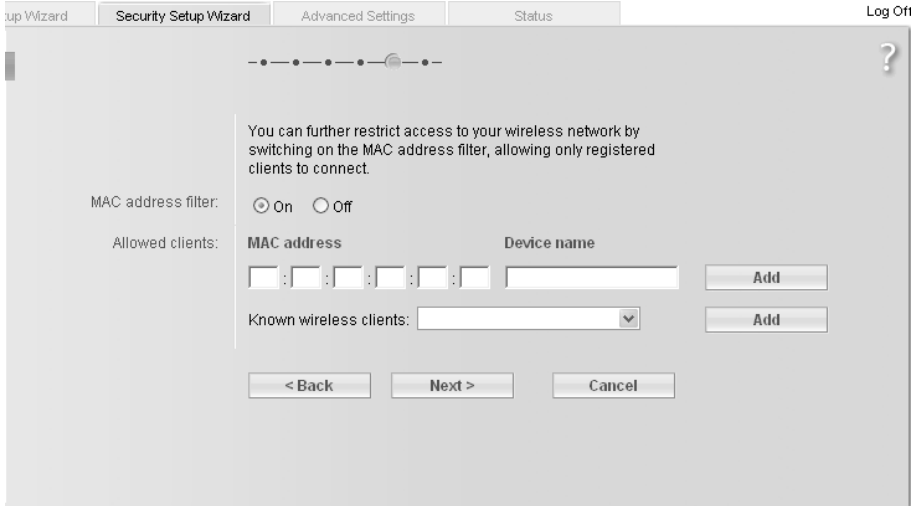
Note:

- ◆ 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.
- ◆ You have to 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 SX686 WiMAX wireless network.

➔ To go to the next step, click **Next >**

Access control within the wireless network

In this step you can specify which PCs will have wireless access to the Gigaset SX686 WiMAX and hence to the LAN. 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.



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 SX686 WiMAX to the list. Otherwise, you will have no access to the user interface and will receive an appropriate error message.

WPS registration is only possible for PCs in the list if you have activated MAC access control.

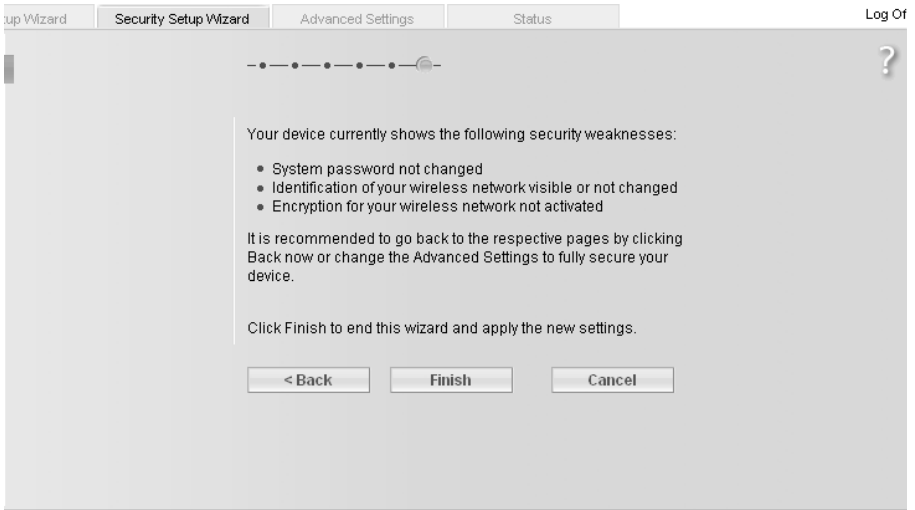
If you have inadvertently denied all PCs access to the Gigaset SX686 WiMAX, you have two options:

- ◆ You can completely reset the Gigaset SX686 WiMAX (page 16).
- ◆ You can connect a PC to the Gigaset SX686 WiMAX 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.



➔ Click **Finish** to end the wizard.

The settings will now be activated on the Gigaset SX686 WiMAX.

Note:

If you have changed the encryption setting, 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 SX686 WiMAX.

Configuring Advanced Settings

In the **Advanced Settings** menu, you can configure all the options for the Gigaset SX686 WiMAX. 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	<p>This menu comprises all the setting options relating to the Internet. In particular, you can do the following:</p> <ul style="list-style-type: none"> ◆ Check and change the configuration for Internet access (page 72) or specify a preferred DNS server (page 75), ◆ Configure the firewall, i.e. a number of security and special functions (page 76), ◆ Make the NAT settings required to provide your own services on the Internet (page 80), ◆ Set up dynamic DNS for a fixed Internet address on the device (page 85), ◆ Set up routing for your Internet connection services (page 87).
Local Network	You can change the Private IP address of the Gigaset SX686 WiMAX here and make settings on the DHCP server (page 88).
Wireless Network	You can configure the options for wireless communication (SSID and encryption) here and restrict access to the Gigaset SX686 WiMAX (page 91).
Telephony	You can make the settings for Internet telephony (VoIP) here and configure your extensions (page 105).
USB	You can make the settings here for operating an external data carrier, a Web server, a file server or a print server on the USB port (page 116).
Administration	You can make or change various system settings here, for example change the password (page 131) or set the time (page 130). In addition, you can also back up the data on the Gigaset SX686 WiMAX (page 133).

Internet

If you have configured the Gigaset SX686 WiMAX 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:

Internet	Activate/deactivate the Internet connection and edit the virtual connection parameters (for further information see below),
Internet Connection	Check and edit the Internet connection of the Gigaset SX686 WiMAX (for further information see below),
DNS Servers	Make DNS server settings (page 75),
Firewall	Protect the network against unauthorised external access (see page 76),
Address Translation (NAT)	Provide your own services on the Internet (NAT, see page 80),
Dynamic DNS	Set up dynamic DNS (page 85),
Routing	Set up routing for your Internet connection services (page 87).

Internet selection

On this screen you can activate or deactivate the Internet connection for the Gigaset SX686 WiMAX and you can set up a number of connection services.

➔ In the **Advanced Settings** menu, select: **Internet**

The screenshot shows the 'Internet' configuration window. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. A 'Log Off' button is in the top right. The main area is titled 'Internet' and contains the following elements:

- 'Internet:' with radio buttons for 'On' (selected) and 'Off'.
- 'Configure multiple connection services:' with radio buttons for 'On' (selected) and 'Off'.
- 'Connection services:' section with a table:

VLAN tag	Priority	Comment
3	7 (highest)	wan0
4	7 (highest)	wan1
- An 'Add' button to the right of the table.
- 'OK' and 'Cancel' buttons at the bottom.

➔ Select the appropriate option to activate or deactivate the Internet function of the Gigaset SX686 WiMAX.

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 87).

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

➔ In the **VLAN tag** field enter a number to be used as VLAN tag for the connection service. Your Gigaset SX686 WiMAX supports VLANs (Virtual Local Area Network) according to the IEEE 802.1 Q standard. The VLAN tag thereby indicates in all incoming and outgoing data packets the VLAN (connection service) to which the data packet belongs. Value range: 0 - 4096.

➔ From the **Priority** option menu, select a priority level (0-7) for the connection service. You can, for example, assign a higher priority to a connection service which is used for voice transmission (VoIP) than to a connection service which is used for Internet surfing. You thus increase the voice quality of your Internet telephony.

➔ Enter a description of the connection service in the text field

➔ Click on **Add** to set up the connection service.

➔ To remove a connection service from the list, click on **Delete**.

➔ 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 service provider makes available to you. False information can lead to problems with your Internet connection.

- ➔ If you want to configure or modify settings for the Internet connection, select from the **Advanced Settings** menu: **Internet – Internet Connection**

The screenshot shows the 'Internet Connection' configuration window. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. The 'Advanced Settings' tab is selected. The window title is 'Internet Connection' with a help icon. The 'Connection service selected to edit' is '3 (wan0)'. The 'Service provider' is 'Other'. The 'Protocol' is 'PPPoE'. There are input fields for 'User name', 'Password', and 'Confirm password'. The 'Access concentrator name' is empty. The 'MTU' is '1492'. '24h reconnection' is 'Off'. The 'VLAN tag' is '3'. The 'Connection mode' is 'Always on'. 'PPPoE pass-through' is 'Off'. There is a section for 'UPnP Connection' with 'UPnP' set to 'Off'. At the bottom are 'Test Settings', 'OK', and 'Cancel' buttons.

All settings apply for the displayed connection service that you selected for editing on the **Advanced Settings – Internet** (page 71) screen.

- ➔ Select your **Service provider**. Depending on the country you selected when making the basic settings (page 53), 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**, **Password**.

Only if you have selected **PPPoE** as the protocol and if you want to set up a number of connection services with this protocol:

- ➔ Enter the name of the connection given to you by your service provider in the **Access concentrator name** field.
- ➔ Apply the default settings for the other parameters 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.

- ➔ Your Internet service provider may disconnect and reconnect your Internet connection daily. In this case enable **24h reconnection** and choose the period of time in which the reconnection should be performed from the **Reconnection time** option menu.
- ➔ In the **VLAN tag** field, enter a number to be used as VLAN tag for the connection service. Your Gigaset SX686 WiMAX supports VLANs (Virtual Local Area Network) according to the IEEE 802.1 Q standard. The VLAN tag thereby indicates in all incoming and outgoing data packets the VLAN (connection service) to which the data packet belongs. Value range: 0 - 4096.
- ➔ 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 SX686 WiMAX 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 SX686 WiMAX.
- ◆ 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** and **Connect manually** options.
- 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.

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** menu, select: **Internet – Internet Connection**

Configuring Advanced Settings

➔ Select **On** to activate **PPPoE pass-through** and 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 operating system Windows ME, Windows XP or Windows Vista must run on the PC. Check, if the UPnP function has been installed on the PCs operating system. Maybe you have to install the UPnP components retroactively. Please consult the operating instructions of your PC.

As soon as you have installed UPnP on a PC operating system 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 83), thereby facilitating communication via the Internet.

The task bar on the PC on which UPnP is installed contains an icon for the Gigaset SX686 WiMAX. Click this icon to open the user interface. On Windows XP system, this icon is also shown under network connections.

➔ In the **Advanced Settings** menu, select: **Internet – 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.

Test settings

➔ 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.

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

➔ 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 service 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** menu, select: **Internet – Internet Connection – DNS Servers**

The screenshot shows a window titled "DNS Servers" with a question mark icon in the top right corner. The window has a tabbed interface at the top with "Advanced Settings" selected. Below the title bar, there is a section labeled "Use custom DNS servers:" with two radio buttons: "On" (selected) and "Off". Underneath, there are two rows of input fields for IP addresses. The first row is labeled "Preferred DNS server:" and the second row is labeled "Alternate DNS server:". Each row has four input boxes separated by dots. At the bottom of the window, there are two buttons: "OK" and "Cancel".

All settings apply for the displayed connection service that you selected for editing on the **Advanced Settings – Internet** (page 71) 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.

Firewall

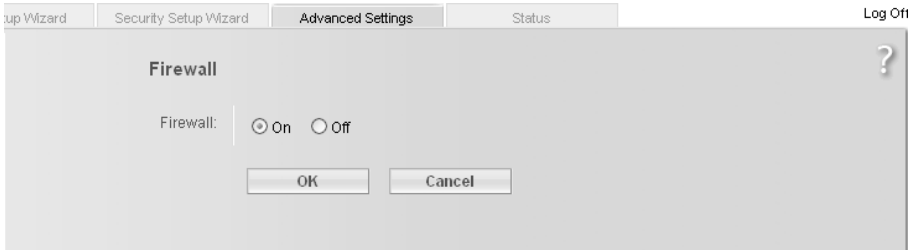
The firewall functions of the Gigaset SX686 WiMAX include various security functions for the local network.

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 78).

The firewall functions for the Gigaset SX686 WiMAX are activated and configured in the factory. If you want to deactivate the firewall, carry out the following steps:

➔ In the **Advanced Settings** menu, select: **Internet – Firewall**



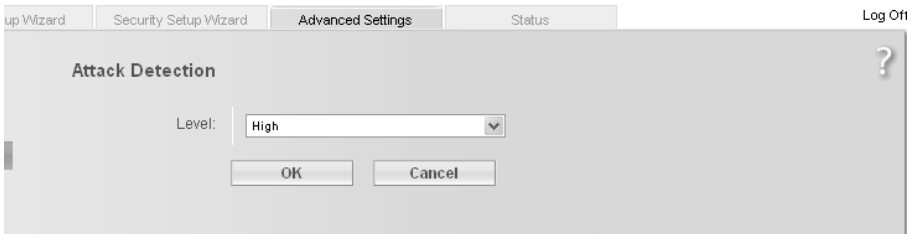
- ➔ Click the required option.
- ➔ Click **OK** to apply the settings.

Attack Detection

If the firewall functions of the Gigaset SX686 WiMAX are activated, the device monitors and limits access to incoming data traffic via the WiMAX connection with a function called "Stateful Packet Inspection" (SPI). This allows the Gigaset SX686 WiMAX 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 change the standard firewall settings.

➔ In the **Advanced Settings** menu, select: **Internet – Firewall – Attack Detection**



➔ 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.

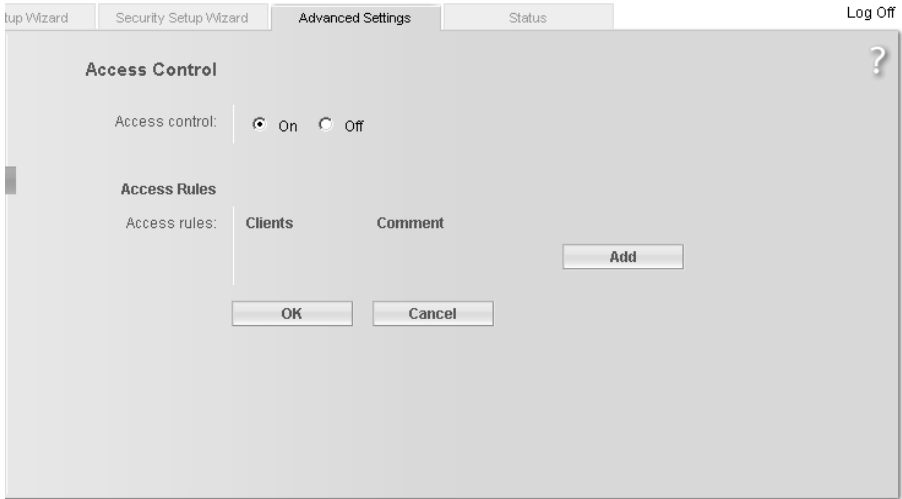
➔ Click **OK** to apply the settings.

Configuring Advanced Settings

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** menu, select: **Internet – Firewall – Access Control**



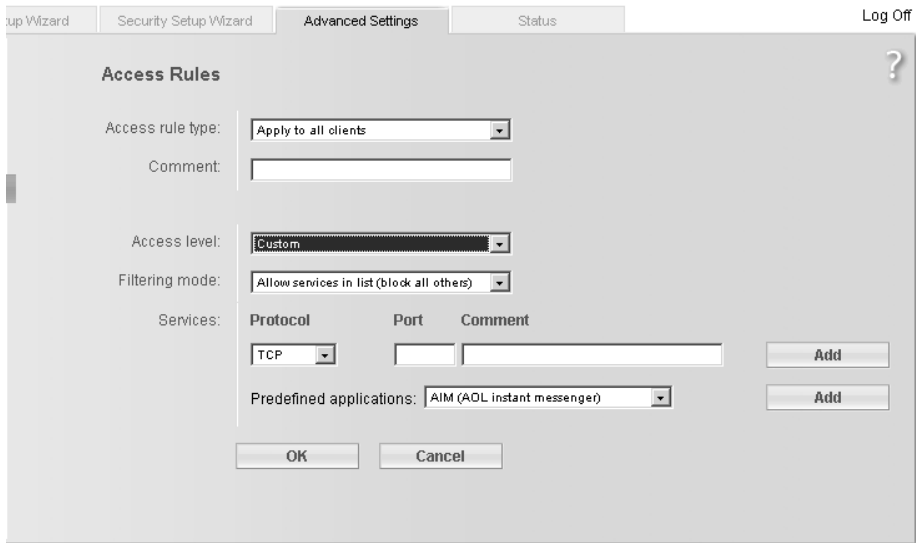
➔ Activate the **Access Control** function by selecting **On**.

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

Access Rules

You can limit access to the Internet for all clients, or only for certain clients in the network, thereby allowing or blocking access to services.

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



- ➔ 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:** Sie wählen die PCs aus, auf die die Regel angewendet werden soll, indem Sie einen IP-Adressbereich eingeben.
 - **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** or **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.
 - 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 SX686 WiMAX 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 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 work 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.

Port triggering is a special variant of port forwarding. Unlike port forwarding, the Gigaset SX686 WiMAX forwards the data from the port block to the PC which has previously sent data to the Internet via a certain port (trigger port). This means that approval for the data transfer is not tied to one specific PC in the network, rather to the port numbers of the required Internet service.

Where configuration is concerned, this means:

- ◆ You have to define a so-called trigger port for the application and also the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port.
- ◆ The router checks all outgoing data for the port number and protocol. If it identifies a match of port and protocol for a defined trigger port, then it will open the assigned public ports and notes the IP address of the PC that sent the data. If data comes back from the Internet via one of these public ports, the router allows it through and directs it to the appropriate PC. A trigger event always comes from a PC within the local network. If a trigger port is addressed from outside, the router simply ignores it.

Note:

- ◆ An application that is configured for port triggering can only be run by one user in the local network at a time.
- ◆ As long as the public ports are open, they can be used by unauthorised persons to gain access to a PC in the local network.

When the Gigaset SX686 WiMAX 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 SX686 WiMAX to carry out the following tasks:

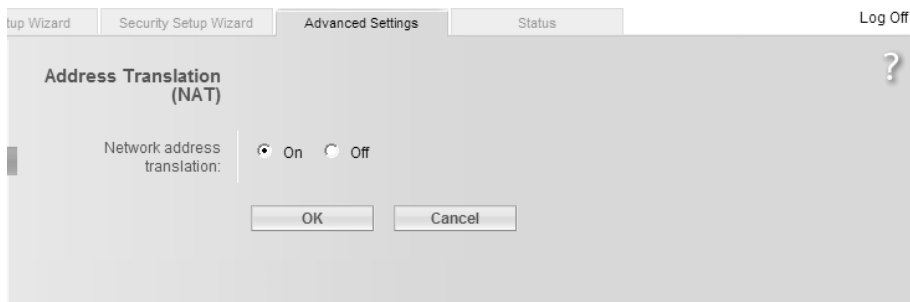
- ◆ Set up the Gigaset SX686 WiMAX as a virtual server by configuring Port Forwarding (page 83),
- ◆ Open the firewall for a selected PC (page 84).

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 SX686 WiMAX, you must select **Never expires** (page 89) as the setting in the **Local Network** menu entry for the **Lease time** or assign static IP addresses for the PCs.

By default the NAT function is activated. You should only deactivate the NAT function if you want to configure you own firewall in you local network.

➔ In the **Advanced Settings** menu, select: **Internet – Address Translation (NAT)**



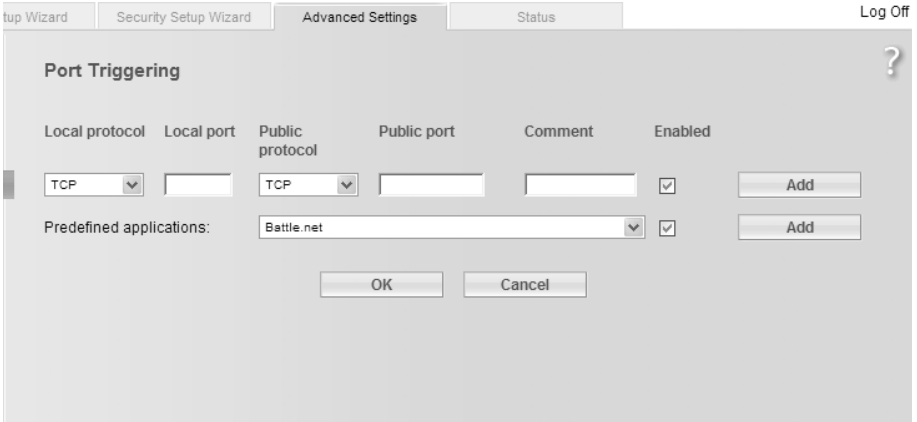
- ➔ Select the required option.
- ➔ Click **OK** to apply the settings.

Port Triggering

If you configure port triggering for a certain application, you must identify a trigger port and the protocol (TCP or UDP) this port uses. You can then assign the public ports that must be opened for the application and this trigger port.

You can select known Internet services for this purpose or assign ports or blocks of ports manually.

- ➔ In the **Advanced Settings** menu, select: **Internet – Address Translation (NAT) – Port Triggering**



- ➔ Select the required application from the **Predefined applications** list.
- ➔ Click the **Add** button. The data for the required service is entered on the screen.
- ➔ Select the check box in the **Enabled** column.

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

- ➔ **Local protocol:** Select the protocol that is to be monitored for outgoing traffic.
- ➔ **Local port:** Enter the port that is to be monitored for outgoing traffic.
- ➔ **Public protocol:** Select the protocol that is to be allowed for incoming data traffic.
- ➔ **Public port:** Enter the port that is to be opened for incoming traffic.

You can enter a single port number, several individual 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 to help you identify different entries.
- ➔ Select the check box in the **Enabled** column.
- ➔ Click the **Delete** button to delete an entry. Click the **Add** button to add a new entry.
- ➔ Apply the settings by clicking **OK**.

Port Forwarding

If you configure Port Forwarding, the Gigaset SX686 WiMAX 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 SX686 WiMAX 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.

➔ In the **Advanced Settings** menu, select: **Internet – Address Translation (NAT) – Port Forwarding**

Protocol	Public port	Local port	Local IP address	Comment	Enabled
TCP					<input checked="" type="checkbox"/>
Predefined applications: FTP				FTP	<input checked="" type="checkbox"/>

- ➔ Select the required application from the **Predefined applications** list.
- ➔ Enter the IP address of the PC that provides the service in the **Local IP address** field.
- ➔ **Comment:** Enter a description that makes it easy to identify different entries.
- ➔ 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(s) of the service you are providing.

Configuring Advanced Settings

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**).

➔ In the **Local port** field, enter the internal port number(s) to which service requests are to be forwarded.

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.

- ➔ Enter the IP address of the PC that provides the service in the **Local IP address** field.
- ➔ **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 a selected PC (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 Port Forwarding on page 83).

- ➔ In the **Advanced Settings** menu, select: **Internet – Address Translation (NAT) – Exposed Host**

The screenshot shows a web-based configuration interface for a router. The main window is titled 'Exposed Host' and is part of the 'Advanced Settings' section. It features a 'Local IP address' field with four separate input boxes for each octet, a 'Comment' text field, an 'Enabled' checkbox, and an 'Add' button. Below these fields are 'OK' and 'Cancel' buttons. The interface also includes a 'Log Off' link in the top right corner and a question mark icon in the top right of the window's title bar.

- ➔ 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.
 - You can add more than one PC to the list, but you can only activate one of them.
- ➔ Click the **Delete** button to delete the entry from the list.
- ➔ Apply the settings by clicking **OK**.

Dynamic DNS

Any service you provide on the Internet can be accessed via 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 SX686 WiMAX an individual fixed domain name on the Internet even if it does not have a static IP address.

Various Internet service 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.

Configuring Advanced Settings

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.

➔ In the **Advanced Settings** menu, select: **Internet – Dynamic DNS**

The screenshot shows the 'Dynamic DNS' configuration window within the 'Advanced Settings' menu. The window has a title bar with 'Dynamic DNS' and a help icon. Below the title bar, there are four tabs: 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings' (which is selected), and 'Status'. In the top right corner of the window, there is a 'Log Off' link. The main content area contains the following fields and controls:

- Dynamic DNS:** A radio button group with 'On' selected and 'Off' unselected.
- Service provider:** A dropdown menu with 'DynDNS.org' selected.
- Domain name:** An empty text input field.
- User name:** An empty text input field.
- Password:** An empty text input field.
- At the bottom, there are two buttons: 'OK' and 'Cancel'.

- ➔ Activate the **Dynamic DNS** function.
- ➔ 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.

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 71), 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, these define criteria for determining which data traffic is assigned to which connection service.

➔ In the **Advanced Settings** menu, select: **Internet – Routing**

The screenshot shows the 'Routing' configuration window. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. The 'Advanced Settings' tab is selected. The window title is 'Routing'. On the left, there is a sidebar with a search icon and a question mark icon. The main area contains the following settings:

- Policy-based routing:** On Off
- Policy type:** Specify interface (dropdown menu)
- Routes:**

Interface	Connection service
(all other interfaces)	None (dropdown menu)
LAN1 (dropdown menu)	3 (wan0) (dropdown menu)

At the bottom right, there is an 'Add' button. At the bottom center, there are 'OK' and 'Cancel' buttons.

- ➔ 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**, **Specify IP address range** or **Specify MAC address** to specify routes for clients depending on your IP address or MAC address. If you choose **Specify MAC address**, you can select PCs from the list of known clients.
- ➔ Click **Delete** 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.

LAN configuration

You can use the LAN configuration to define an [IP address](#) for the Gigaset SX686 WiMAX and configure the DHCP server.

➔ In the **Advanced Settings** menu, select: **Local Network**

The screenshot shows the 'Local Network' configuration window. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. A 'Log Off' link is in the top right corner. The window title is 'Local Network' with a help icon. The configuration is divided into several sections:

- IP address:** 192 . 168 . 2 . 1
- Subnet mask:** 255 . 255 . 255 . 0
- DHCP Server:**
 - DHCP server: On Off
 - Lease time: 30 minutes (dropdown menu)
 - First issued IP address: 192 . 168 . 2 . 17
 - Last issued IP address: 192 . 168 . 2 . 253
 - Default gateway: 192 . 168 . 2 . 1
 - Preferred DNS server: [] . [] . [] . []
 - Alternate DNS server: [] . [] . [] . []
 - Domain name: dummy.porta.siemens.net
- Clients:** A table with columns for MAC address and IP address. The IP address column shows 192 . 168 . 2 . []. There is an 'Add' button to the right.

At the bottom, there are 'OK' and 'Cancel' buttons.

Defining the private IP address for the Gigaset SX686 WiMAX

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 SX686 WiMAX. 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 SX686 WiMAX can be reached from outside is assigned by the Internet service provider. The [Subnet mask](#) for the local network administered by the Gigaset SX686 WiMAX is 255.255.255.0.

➔ If you want to assign a different IP address to the Gigaset SX686 WiMAX, enter your chosen IP address in the boxes next to **IP address**.

Please note which subnet mask is set when assigning the IP address. The preset subnet mask defines the first three parts of the IP address which must be identical for all network components (including routers).

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.

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

The **Subnet mask** specifies how many address parts of the IP address must be identical for all network components (including routers).

Notes:

New settings can only be made after the Gigaset SX686 WiMAX 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 SX686 WiMAX has a **DHCP server** for which the factory setting is active. Consequently, the IP addresses of the PCs are automatically assigned by the Gigaset SX686 WiMAX.

Note:

- ◆ If the DHCP server for the Gigaset SX686 WiMAX is activated, you can configure the network setting on the PC so that the option **Obtain an IP address automatically** is set up. For further information, refer to the section entitled "Configuring the local area network" on the CD-ROM.
- ◆ 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 least time indicates how long the client may use the allocated IP configuration.

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 SX686 WiMAX should use to automatically assign IP addresses to the PCs. Define the **First issued IP address** and the **Last issued IP address**.

➔ If you want to define a different **Default gateway** in your local area network instead of the Gigaset SX686 WiMAX, enter the IP address of this default gateways in the relevant boxes.

Configuring Advanced Settings

Entering the 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 must administer this information for each server or for each LAN with an Internet connection.

Your Internet service provider will usually provide you with a [DNS server](#) that makes this assignment when an Internet connection is set up. If necessary, you can manually define the DNS server to be used for the Internet connections.

- ➔ Enter the IP addresses for your preferred DNS servers (***Preferred DNS server*** and ***Alternate DNS server***).
- ➔ 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*** of the PC to which you want to assign a static IP address.
- ➔ Enter the ***IP address*** you wish to assign to the PC.
- ➔ 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 you have implemented wireless PC communication via the Gigaset SX686 WiMAX, you should improve the security of your wireless network via the **Advanced Settings – Wireless Network** menu. You can carry out the following functions:

- Wireless Network** Activate the wireless module of the Gigaset SX686 WiMAX and specify basic settings for your wireless network, for example **SSID**, **Transmission mode** or **Sending power**.
- WPS Registration** Start WPS registration and configure WPS (see page 93).
- Encryption & Authentication** Set up **Encryption** for wireless transmissions (page 94).
- Allowed Clients** Restrict access to the LAN of the Gigaset SX686 WiMAX (page 101).
- Repeater (WDS)** Activate the repeater function (Wireless Distribution System, **WDS**) and define repeaters to increase the range of your WLAN (see page 103).

➔ In the **Advanced Settings** menu, select: **Wireless Network**

The screenshot shows the 'Wireless Network' configuration window. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. A 'Log Off' button is in the top right corner. The window title is 'Wireless Network' with a help icon. The settings are as follows:

- Wireless network: On Off
- Channel: 6 (dropdown menu)
- SSID: ConnectionPoint (text field)
- SSID broadcast: On Off
- Transmission mode: IEEE 802.11b/g (mixed) (dropdown menu)
- Sending power: 100 % (dropdown menu)

At the bottom, there are 'OK' and 'Cancel' buttons.

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

Devices can only log in wirelessly if the WLAN module of the Gigaset SX686 WiMAX is activated.

You can now make the settings for the wireless network.

Configuring Advanced Settings

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 Gigaset SX686 WiMAX is delivered with a preset SSID. You will find it at the label on the bottom of the device. This can be a default SSID, e.g. ConnectionPoint, or a SSID which is individually set for each device in the format SX686-XXXXXX, where XXXXXX is a string consisting of 0-9 and A-F, e.g. SX686-EB691A.

For security reasons you can change this SSID and deactivate SSID broadcast (for information see below).

Note:

If a WPS registration (see page 57) was performed before manual configuration, the generated SSID is displayed in this screen. You should not change this SSID here manually. Otherwise, the registered clients will no longer have access to your wireless network.

Enter a character string of your choice. The SSID is case-sensitive. It can contain up to 32 characters. Use a combination of letters, digits and special 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 SX686 WiMAX will send the SSID in all data transfers and the SSID of the Gigaset SX686 WiMAX 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 SX686 WiMAX will not be displayed. This increases protection against unauthorised access to your wireless network. Make a note of the SSID. You will need it to log on to the PC.

To protect your wireless network, you should also enable encryption of data transmissions (page 94).

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

Transmission mode

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.

➔ Click **OK** to apply the settings.

Starting WPS registration and configuring WPS

Wi-Fi Protected Setup (WPS) makes it easier to establish a wireless network. Devices equipped with WPS can synchronise the SSID and the WPA key (pre-shared key).

The most simple method to establish a secure wireless connection is click once in the user interface of the Gigaset SX686 WiMAX and do the same with the client. For further information, see "Setting up a wireless network via WPS" on page 26.

The configuration program of the Gigaset SX686 WiMAX provides beside the **Push Button** method for WPS registration for more security the registrations mode via PIN.

➔ In the **Advanced Settings** menu select: **Wireless Network – WPS Registration**

The screenshot shows the 'WPS Registration' dialog box within the 'Advanced Settings' menu. The dialog has a title bar with 'up Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status' tabs, and a 'Log Off' button in the top right corner. The main content area is titled 'WPS Registration' and contains a 'Registration Mode:' dropdown menu with 'Enter partner device PIN' selected. Below this is a 'PIN:' text input field. A message below the input field reads: 'Enter the PIN of the WLAN partner device and click OK to start the WPS registration.' At the bottom of the dialog are 'OK' and 'Cancel' buttons. A question mark icon is visible in the top right corner of the dialog area.

➔ Choose the desired **Registration Mode**:

– **Push Button**

Click **OK** to start the WPS registration.

Configuring Advanced Settings

Once WPS registration is activated, the device searches for a WPS client within range. Any WPS client within range that activates the WPS function during the two-minute interval receives the Gigaset SX686 WiMAX security data (SSID and pre-shared key) and is thereby registered.

The registration progress is shown in the window.

You can also follow the registration process via the LED display (see page 37).

If more than one client tries to register within the two minutes, an error message is displayed. You may retry the WPS registration after a short time.

If an external client succeeds in registering, the LED (see page 37) displays a successful WPS registration. The desired client in your network, however, has no connection to the Gigaset SX686 WiMAX and displays a registration failure. In this case you should change the pre-shared key (WPA2-PSK/WPA-PSK) as soon as possible and then perform WPS registration via PIN (see below).

– **Send own PIN**

An automatically generated PIN is shown.

If you want to create a new PIN, click **Generate PIN**.

Click **OK** to activate your settings.

Enter the generated PIN on all WLAN partner devices that are to establish a connection.

– **Enter partner device PIN**

You would use this option if you have created a PIN at the desired client. Enter the PIN of the WLAN partner device and click **OK** to activate your settings.

Note:

If you have activated access control via the MAC address filter, you have to include the clients in the MAC address list before registering via WPS (see page 101).

Setting encryption

Note:

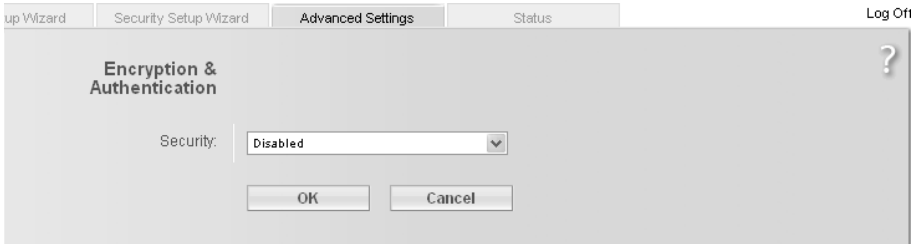
The Gigaset SX686 WiMAX is delivered with preset individual encryption (WPA2-PSK/WPA-PSK with pre-shared key). You should change this settings only, if not all components of your wireless network provide this encryption method or if you want to change the preset key for security reasons, or if you want to use the WDS repeater function.

If you change the preset key after having registered PCs at the Gigaset SX686 WiMAX via WPS or manually, you must register all PCs again manually or via WPS.

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 also supports the use of an authentication server.

➔ In the **Advanced Settings** menu select: **Wireless Network – Encryption & Authentication**



The following security mechanisms are currently available:

- ◆ WPA2-PSK, WPA-PSK and WPA2-PSK/WPA-PSK (page 95)
- ◆ WPA2 and WPA2/WPA with authentication server (page 96)
- ◆ WEP encryption (Wired Equivalent Privacy, see page 98)

Note:

If you want to use the repeater function of your Gigaset SX686 WiMAX (page 103) you can only use WEP encryption.

WPA2-PSK and WPA2-PSK / WPA-PSK

Note:

This screen allows you to display the pre-shared key. You can change the encryption here. In this case, you also have to configure all wireless network adapters manually or perform WPS registration once again.

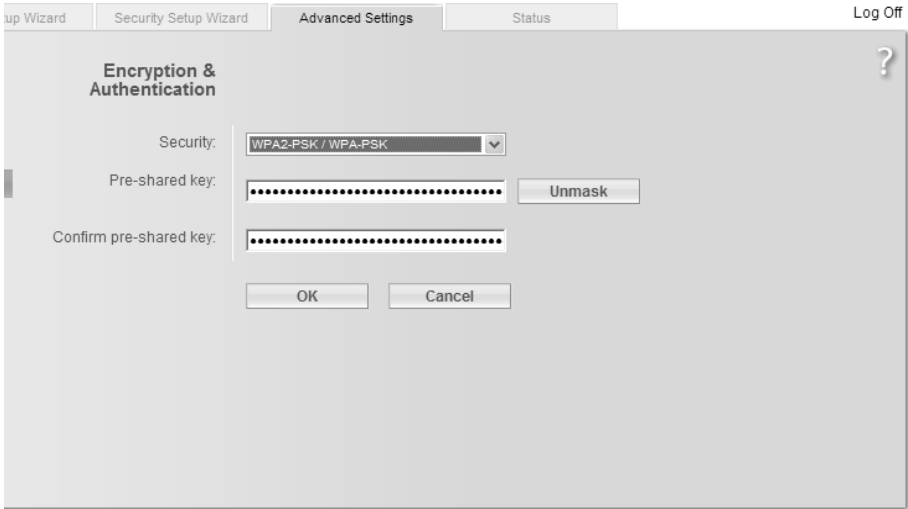
WPA with a pre-shared key (WPA-PSK)

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 **WPA-PSK**. Select **WPA2-PSK / WPA-PSK** if both methods are used in your network. Your device then automatically defines the best possible way to protect your data for each client. The entries described below are identical for both options.

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

Configuring Advanced Settings



- ➔ Enter a key in the **Pre-shared key** field (up to 32 characters) and confirm it by entering it again. Use a combination of letters, digits and special characters.
- ➔ By clicking the **Unmask** button, a message showing the pre-shared key is output in readable characters.
- ➔ 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.

Setup Wizard Security Setup Wizard **Advanced Settings** Status Log Off

Encryption & Authentication ?

Security:

RADIUS server IP address:

RADIUS server port:

RADIUS server secret key:

- ➔ 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.

Configuring Advanced 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.

Note:

You cannot use WEP together with WPS.

➔ Choose the **WEP** option in the **Security** field.

The screenshot shows a configuration window titled "Encryption & Authentication". At the top, there are tabs for "Setup Wizard", "Security Setup Wizard", "Advanced Settings", and "Status". The "Advanced Settings" tab is active. The window contains the following fields:

- Security: WEP (dropdown)
- Authentication type: Open (dropdown)
- Key length: 64 bits (dropdown)
- Input type: Key (dropdown)
- Key type: ASCII (dropdown)
- Key 1: [text input]
- Confirm key 1: [text input]
- Key 2: [text input]
- Confirm key 2: [text input]
- Key 3: [text input]
- Confirm key 3: [text input]
- Key 4: [text input]
- Confirm key 4: [text input]
- Default key: Key 1 (dropdown)

At the bottom, there are "OK" and "Cancel" buttons. A question mark icon is visible in the top right corner of the window.

➔ Select the **Authentication type**:

- Select **Shared** to require that each client log 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 SX686 WiMAX 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**.

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.
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**, **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_SX76x

- ➔ 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**.

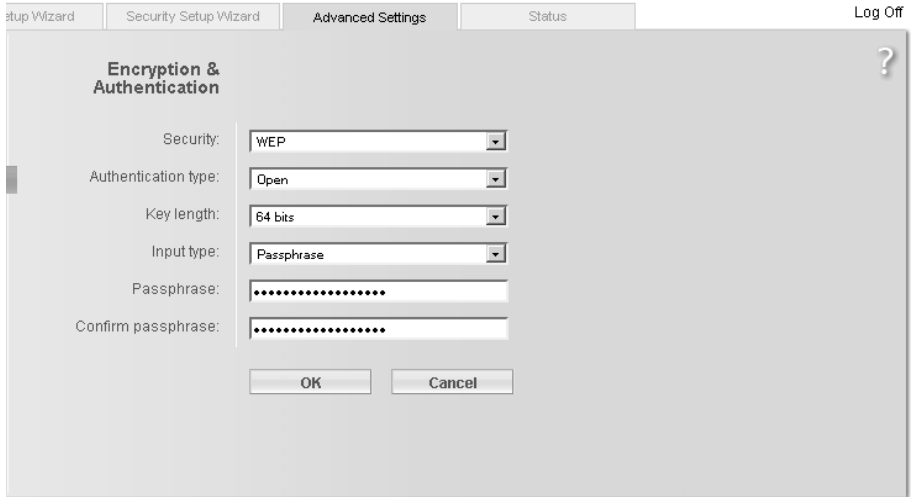
Note:

- ◆ It is very **important** that you make a note of the key(s) that have been entered. 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 SX686 WiMAX.

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

Configuring Advanced Settings

Generating a key by means of a Passphrase



- ➔ Enter a **Passphrase** (up to 32 characters) and confirm it by entering it again. The key is generated automatically.
- ➔ 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 SX686 WiMAX and hence to your LAN and WLAN.

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 address** of the PC network adapters.

➔ In the **Advanced Settings** menu, select: **Wireless Network – Allowed Clients**

The screenshot shows the 'Allowed Clients' configuration window. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. The 'Advanced Settings' tab is selected. The window title is 'Allowed Clients' with a help icon (?). The 'MAC address filter' is set to 'On'. Below this is a table with two columns: 'MAC address' and 'Device name'. There are 'Add' buttons for each row. At the bottom, there is a 'Known wireless clients' dropdown menu with an 'Add' button, and 'OK' and 'Cancel' buttons.

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

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.

Note: Only following deletion is the entry transferred to the list of known MAC addresses.

➔ 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**.

Configuring Advanced Settings

Note:

If you activate MAC access control, you must at least add the PC on which you are configuring the Gigaset SX686 WiMAX to the list. Otherwise, you will have no access to the user interface and will receive an appropriate error message.

If you have inadvertently denied all PCs access to the Gigaset SX686 WiMAX, you have two options:

- ◆ You can completely reset the Gigaset SX686 WiMAX (page 16).
- ◆ You can connect a PC to the Gigaset SX686 WiMAX 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.

Repeater function (WDS)

WDS (Wireless Distribution System) allows you to extend the range of your wireless network using a repeater. A repeater located at the outer range of a wireless network ensures that data is forwarded between WLAN clients in this wireless network and clients within its own wireless range. Repeaters and access points thereby form a common wireless network within which all clients can be moved about freely. Clients automatically set up a connection to the next access point / repeater (roaming). For security purposes you must determine which access points / repeaters are to form a common wireless network.

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

Note:

WDS can only be used with WEP encryption or without encryption. If you use WPA-PSK encryption (default) you have to change the encryption of your wireless network. For information refer to the section "Setting encryption" on page 94.

➔ In the **Advanced Settings** menu, select: **Wireless Network – Repeater (WDS)**

➔ To activate WDS select the **On** option next to **Wireless distribution system**.

The environment is scanned for wireless networks in range. If the search has been completed successfully the networks are displayed.

up Wizard Security Setup Wizard **Advanced Settings** Status Log Off

Repeater (WDS) ?

Wireless distribution system: On Off

Accessible WLAN stations

Nr	SSID	MAC Address	ChannelType	Active
1		00:1A:4F:02:D9:5C	6 11g	<input checked="" type="checkbox"/>
2		00:13:49:9A:C0:0C	6 11g	<input type="checkbox"/>

Refresh

OK Cancel

All repeaters/access points in range are displayed with the following information:

- **SSID**
- **MAC address**
- **Channel**

Configuring Advanced Settings

- **Type** (11b or 11g)

The **Signal strength** of the connection to the repeater, if one exists, is shown as a percentage. You can use this data to determine the best possible location for your repeater. You can register a maximum of three repeaters to extend your WLAN.

➔ Select the **Active** check box to register a repeater to your wireless network.

Note:

The registered but currently unavailable repeaters are presented only by their MAC addresses.

➔ Click **Refresh** to update the display.

➔ Click **OK** to apply the settings.

Note:

- ◆ WDS can only be used with WEP encryption or without encryption. You may have to change the encryption of your wireless network, if applicable.
- ◆ The encryption settings on the repeater have to correspond to the settings on your Gigaset SX686 WiMAX.
- ◆ The Gigaset SX686 WiMAX and the repeaters must use the same channel.

Further information can be found in the user manual for the repeater.

Setting up Internet telephony (VoIP)

The Gigaset SX686 WiMAX allows you to make telephone calls via the Internet using an analogue telephone and also 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 have to enter this data along with other configuration settings under Advanced Settings in the **Telephony – VoIP** menu.

You can connect a base station for handsets or fax machines to the two telephone ports of the Gigaset SX686 WiMAX analogue phone. In addition, you can set up additional extensions for Internet and fixed network calls using **SIP clients** (as VoIP phones, WLAN handsets or in wired or wireless mode on PCs).

The menu comprises the following functions:

VoIP	Enter the basic data from your service provider here (page 106).
Extensions	Set up the functions for internal extensions here (page 109).
Dialing Plans	Specify numbers here that are to be dialled only via the fixed network or only via the Internet. You can also enter a call-by-call provider for the fixed network (page 113).
	Define an area code (page 113).
Quick Dial	Specify speed dial numbers or names here for phone numbers you use frequently (see page 115)

Note:

If you do not specify any of your own dialling plans, 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 plans will not apply in this case (page 113).
- ◆ Check these dialling plans (page 113) 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 54). 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 service provider.

VoIP settings

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

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

The screenshot shows the 'VoIP' configuration window. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. A 'Log Off' link is in the top right corner. The window title is 'VoIP' with a help icon. The 'VoIP' section has a radio button for 'On' (selected) and 'Off'. Below it is a 'Connection service' dropdown menu with 'wan0' selected. The 'VoIP accounts' section has a table with columns 'Access Code', 'User name', and 'SIP domain', and an 'Add' button. The 'Voice Quality' section includes: 'Maximum upstream bandwidth' set to '50000 kbps'; 'Voice activity detection' with 'On' selected; 'Echo canceller delay' set to 'Disabled'; and 'Fixed gain control (input/output)' set to '24 / 24'. 'OK' and 'Cancel' buttons are at the bottom.

- Select **On** if you wish to use Internet telephony (default setting).
- If you have defined more than one **Connection service** (see page 71), choose from the list the **Connection service**, for which you want configure a VoIP account.
- 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** (page 108).
- To delete a VoIP account click the **Delete** button.
The account is deleted immediately and irrevocably when you confirm the action.
- If you want to configure additional **VoIP accounts**, click **Add** (page 108).
- You can generally accept the default settings for **Voice Quality**:
 - **Maximum upstream bandwidth**: The upstream transmission rate (bandwidth) varies depending on the provider and WiMAX tariff and is normally much lower than the transmission rate for downstream data traffic. If there is upstream data

traffic at the same time over the WiMAX line, the voice quality may not be optimum.

To ensure optimum voice quality, you can use the **Maximum upstream bandwidth** option to define the bandwidth, which is to be used as a maximum for your VoIP connection. The bandwidth is set automatically by default.

You can change these values if necessary, but you have to find out first how high your upstream transmission rate is. Most providers supply tools for administering your WiMAX connection, which should tell you this information. Otherwise, you will find plenty of Web sites on the Internet that provide such tools.

Enter a value for **Maximum upstream bandwidth**, which is 90 percent of your available bandwidth.

- **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 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):** To adjust the volume for call input (hear) or output (speak), simply enter a different value.

The value range is -24 to +24.

The higher the value, the higher the volume.

-24	quiet
0	normal
24	loud

The value range which can be used depends on your device. If you enter a wrong value, a message with the valid value range will be displayed.

Configuring Advanced Settings

Setting up or modifying a VoIP account

Setup Wizard | Security Setup Wizard | **Advanced Settings** | Status | Log Off

VoIP

VoIP account: On Off

Service provider:

User name:

Displayed name:

Authorization user name:

Password:

Confirm password:

SIP domain:

SIP realm:

SIP listen port:

Proxy server address:

Proxy server port:

Registrar server address:

Registrar server port:

Voice codecs:

Selected codecs	Available codecs
G.729e (*)	G.726-16000 (*)
G.729 (*)	G.726-24000 (*)
G.723.1-6300 (*)	G.729e (*)
G.726-32000 (*)	G.728
G.726-40000 (*)	G.723.1-6300 (*)
G.711ALaw (*)	G.722
G.711MuLaw (*)	G.722.1

Out-of-band DTMF: Off RFC2833 SIP-Info

Clear

OK Cancel

- ➔ To set up a new account, select **On**.
- ➔ In the **Service provider** menu, select the **Other** option or otherwise select one of the 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 SX686 WiMAX 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 connected to your Gigaset SX686 WiMAX via the Phone 1 and Phone 2 ports, 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 use the two telephone ports of the Gigaset SX686 WiMAX, 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 SX686 WiMAX, or PCs with a SIP client, which are connected to the Gigaset SX686 WiMAX.

Configuring Advanced Settings

➔ In the **Advanced Settings** menu, select: **Telephony – Extensions**

Phone connectors:

Connector	Extension number	User name	Phone number	
Phone 1	*1	Phone 1	Fixed line	<input type="button" value="Edit"/>
Phone 2	*2	Phone 2	Fixed line	<input type="button" value="Edit"/>

SIP Proxy Server

IP address: 192.168.2.1

Port:

SIP client accounts:

User name	Extension number	Phone number		
	*3	Fixed line	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
	*4	Fixed line	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
	*5	Fixed line	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
	*6	Fixed line	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Phone connectors

The two telephone ports Phone 1 and Phone 2 of the Gigaset SX686 WiMAX have the internal phone number ***1** or ***2**.

➔ Click **Edit** to adapt the settings for an entry (page 111).

SIP Proxy Server

In addition to the telephones connected to your Gigaset SX686 WiMAX, 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 (see below).
- ➔ Click **Delete** to delete an entry.

Configuring extensions

The screenshot shows a configuration window titled "Extensions" within the "Advanced Settings" tab. The window contains the following fields and options:

- Extension:** Phone 1
- Extension number:** *1
- User name:** Phone 1
- Phone number:** Fixed line (dropdown menu) (incoming/outgoing)
- Receive calls for all numbers:** On Off
- Divert calls:** Disabled (dropdown menu)
- Call waiting:** On Off
- Call pickup:** On Off
- Hide own number for outgoing calls (CLIR):** On Off

Buttons for "OK" and "Cancel" are located at the bottom of the dialog.

The Extension shows either the selected port of the Gigaset SX686 WiMAX (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) for this extension or choose the entry **Fixed line**.

The list of numbers for Internet telephony is the one you set up in the **VoIP** menu (page 106). All outgoing calls are directed by default via this phone number. Incoming calls for the selected phone number are signalled.

Configuring Advanced Settings

- ➔ 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 extension selected in the **Divert calls to** field.
 - **When busy**: A call for the extension is forwarded to the selected extension if the extension is busy.
 - **No reply**: A call for the extension is forwarded to the selected extension 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 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 Phone 1 and Phone 2 ports).

Note:

Many service providers either do not support this function at all or only unreliably. 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 your area code,
- ◆ Define for Internet telephony whether the area code should be automatically dialled,
- ◆ Specify whether certain phone numbers or prefixes are to be dialled via the Internet or the fixed network,
- ◆ Enter a call-by-call provider for the fixed network,
- ◆ Define dialling plans.

➔ In the **Advanced Settings** menu, select: **Telephony – Dialing Plans**

➔ Area code

Enter the **Area code** for your current location.

➔ Predial area code for local calls through VoIP

If you activate this function, the area code will be dialled automatically when you make a local call via a VoIP provider. This will save you having to enter the area code which was previously always necessary with VoIP.

➔ Wait for dial tone on fixed line

Only activate this function if it is necessary for the smooth functioning of your Gigaset SX686 WiMAX within the telephone network.

➔ If you wish to make all fixed network calls via a call-by-call provider, activate the **Preselection** function.

➔ Enter the provider's number in the **Preselection number** field.

➔ Choose whether you want to use dialling plans.

Configuring Advanced Settings

- ➔ In the **Phone number** field, enter an individual number or also the first digits of phone numbers (e. g. 0800 or a specific area code) for which the dialling plan is to apply.
- ➔ In the **Connection type** selection field, you can specify the VoIP account to be used to dial the entered number.
- ➔ You can enter a description for the dialling plan in the **Comment** field.
- ➔ Click **Delete** to delete the dialling plan. You can add a new dialling plan by clicking the **Add** button.
You can define up to a maximum of 20 dialling plans.
- ➔ Click **OK** to apply the settings.

Notes:

- ◆ Dialling plans may already be predefined for certain emergency phone numbers depending on the country. These can be changed as required.
- ◆ If you do not specify any dialling plans, 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 plans will not apply in this case.

Quick dial

Quick dial numbers or **Vanity** (phonewords) enable you to dial frequently used phone numbers quickly and easily.

The quick dial number is a two-digit number (01 to 20). A vanity number is a combination of letters you can enter instead of a phone number. You can specify a quick dial number and/or a vanity number for a phone number.

Activate quick dial numbers with the keys *7 quick dial number #, and vanity numbers with the key combination *8 Vanity #.

➔ In the **Advanced Settings** menu, select: **Telephony – Quick Dial**

The screenshot shows the 'Quick Dial' configuration window. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. The 'Advanced Settings' tab is selected. In the top right corner, there is a 'Log Off' link. The main window title is 'Quick Dial' with a help icon (?). Under 'Quick dial:', there are two radio buttons: 'On' (selected) and 'Off'. Below this, there are three input fields: 'Quick dial' (with a *7 prefix), 'Vanity' (with a *8 prefix), and 'Phone number / user name'. To the right of the 'Phone number / user name' field is an 'Add' button. At the bottom, there are 'OK' and 'Cancel' buttons.

- ➔ Click **On** to activate the **Quick Dial** option.
- ➔ Enter the quick dial number in the **Quick Dial** field and/or a name or combination of letters in the **Vanity** field.
- ➔ Enter the phone number in the **Phone number / user name** field.
- ➔ Click **Add** to save the entry.
More empty lines will then be added.
- ➔ Click **OK** to confirm the settings.

USB

The USB port of your Gigaset SX686 WiMAX can be used to set up a

File Server to share a USB mass storage device (page 117)

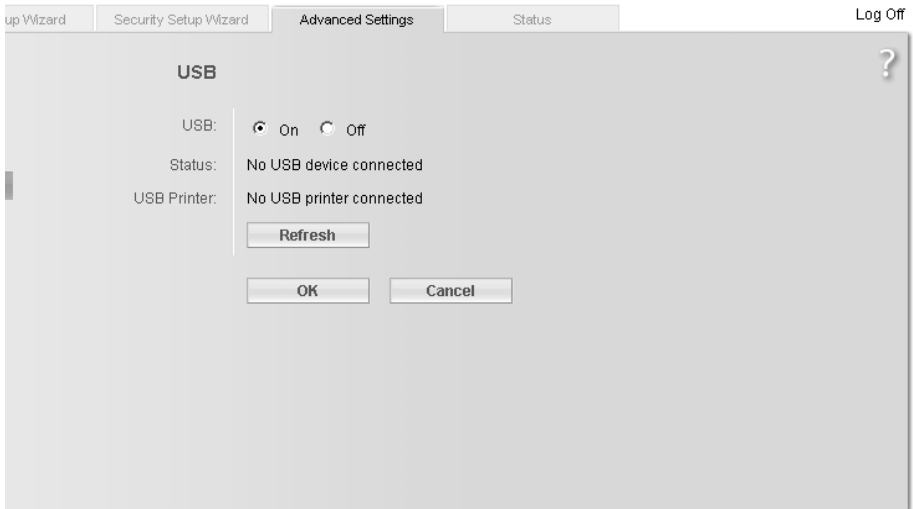
Print Server to share a printer (page 123)

Web Server to provide a Web server (page 123)

Notes:

- ◆ If you connect a USB hub to the USB port of the Gigaset SX686 WiMAX, you can connect and use a USB memory and a USB printer at the same time.
- ◆ If connecting a device without its own power supply directly to the USB port, please note that the power consumption must not exceed 500 mA.
- ◆ The Gigaset SX686 WiMAX supports USB V 2.0. Devices that support USB V 1.1 may also be connected.

➔ Go to the **Advanced Settings** menu and select: **USB**



➔ Select the **On** option for **USB**.

➔ Click **OK** to activate the USB port.

If a USB device is connected, its **Status** is displayed. If a USB mass storage device is connected, the partitions are displayed.

➔ Click **Refresh** to display the current status.

Safely Remove Hardware

- ➔ Click this button and wait until any connected USB storage device are fully deactivated before disconnecting them from your device.
- ➔ Click **OK** to save the changes.

File Server

The devices integrated file server allows you to manage folders and files on a connected USB mass storage device (for example a USB flash drive or external USB drive) and make them available to all users in the local network and on the Internet.

Connect a USB data carrier to the Gigaset SX686 WiMAX via the USB port.

- ➔ In the **Advanced Settings** menu, select: **USB – File Server**

The screenshot shows the 'File Server' configuration window. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. The 'Advanced Settings' tab is selected. The window title is 'File Server' with a help icon. The 'File Server' section has two radio buttons: 'On' (selected) and 'Off'. Below this are three text input fields: 'Workgroupname:' with 'WORKGROUP', 'Description:' with 'CIFS Server', and 'Users:' with 'currently no users added' and an 'Add' button. The 'Shared Folders:' section has 'currently no shared folders added' and an 'Add' button. At the bottom are 'OK' and 'Cancel' buttons.

- ➔ Select the **On** option for the **File Server**.
- ➔ Enter the **Workgroup name** (**WORKGROUP** is the standard name for Windows) in which the file server is located. If you now search your network you will find the file server in the specified domain / workgroup in the network environment.
- ➔ You can enter a **Description** of the file server in the next field.
- ➔ Click **Add** to define **Users** who should have access to the File Server.
You have to define at least one use to define shares on the **File Server**.

Configuring Advanced Settings

The screenshot shows the 'Advanced Settings' tab of a configuration wizard. The window title is 'File Server'. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. In the top right corner, there is a 'Log Off' link and a question mark icon. The main area contains the following fields and buttons:

- User name:** A text input field.
- Password:** A password input field.
- Confirm password:** A password input field.
- OK** and **Cancel** buttons at the bottom.

➔ Enter a **User name**, a **Password**, and confirm it in the next line.

➔ Click **OK**.

The **File Server** start screen is shown again.

➔ Click **Add** to define **Shared Folders** for the **Users** defined above.

The screenshot shows the 'Advanced Settings' tab of the configuration wizard, now at the 'Share Properties' step. The window title is 'File Server'. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. In the top right corner, there is a 'Log Off' link and a question mark icon. The main area contains the following fields and buttons:

- Share name:** A text input field containing 'share1'.
- Directory:** A text input field containing 'usb0/dir_1' and a **Browse** button to its right.
- Comment:** A text input field containing 'myshare'.
- Access Rights:** A dropdown menu showing 'user1' and 'no access'.
- OK** and **Cancel** buttons at the bottom.

➔ Enter a name for the new file share.

➔ Choose the directory for the share via the **Browse** button.

➔ Enter a comment in the next line.

➔ Click **OK**.

Now the users you have defined are displayed.

- ➔ Choose the **Access Rights** for each user: **no access**, **read-write access**, or **read-only access**.
- ➔ Click **OK**.

The **File Server** start screen is shown again.

The screenshot shows the 'File Server' configuration window. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. A 'Log Off' link is located in the top right corner. The main title is 'File Server'. Below the title, there are radio buttons for 'On' (selected) and 'Off'. The 'Workgroupname' field contains 'WORKGROUP' and the 'Description' field contains 'CIFS Server'. Under the 'Users' section, there is a list with 'user1' and an 'Add' button. To the right of 'user1' are 'Edit' and 'Delete' buttons. Under the 'Shared Folders' section, there is a list with 'share1' and an 'Add' button. To the right of 'share1' are 'Edit' and 'Delete' buttons. At the bottom are 'OK' and 'Cancel' buttons.

- ➔ You can edit or delete a user by clicking the **Edit** or **Delete** button.
- ➔ You can edit or delete a file share by clicking the **Edit** or **Delete** button.
- ➔ Click **OK** to save your settings.

Configuring Advanced Settings

Web Server

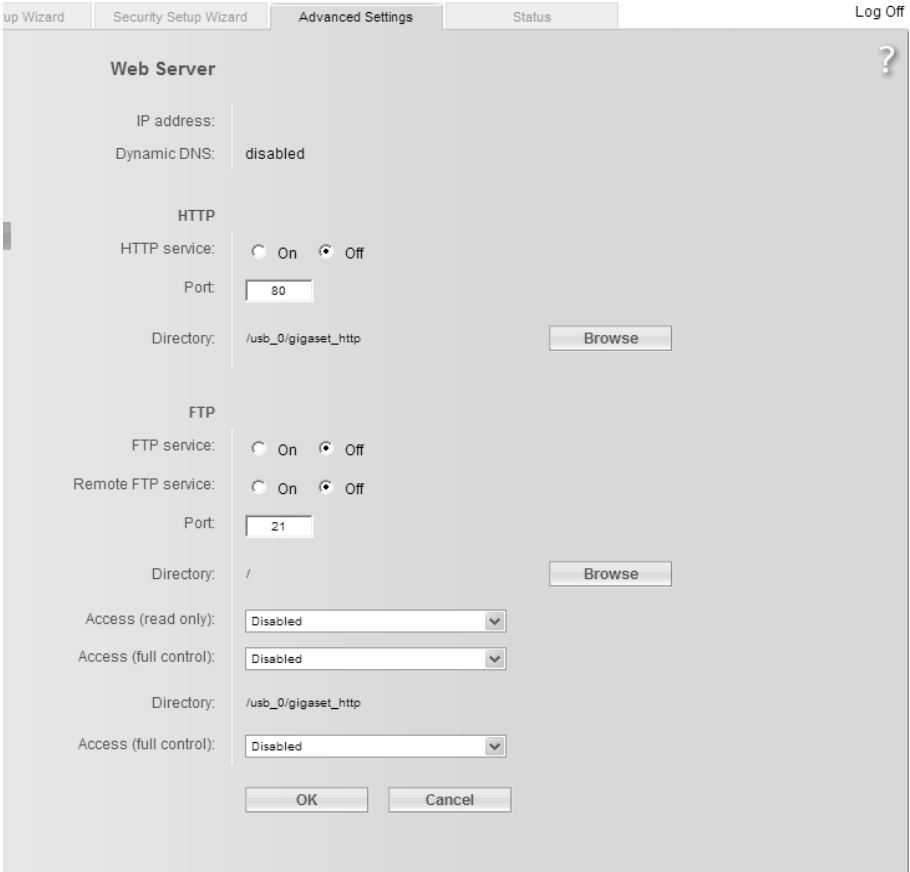
Your devices integrated Web server allows you to publish data stored on a connected USB mass storage device (for example a USB flash drive or external USB drive) on the Internet.

Internet users can access your Web server by entering the public IP address in their Internet browser. As Internet providers often change this each time someone dials in, it is also worth using dynamic DNS (see page 85).

➔ Connect the USB mass storage device containing the data to be published to the USB port.

You can check the status of the connection to the USB device on the **Advanced Settings – USB** screen.

➔ In the **Advanced Settings** menu, select: **USB – Web Server**



The **IP address** (see page 88) of the Gigaset SX686 WiMAX is displayed, as well as information as to whether **Dynamic DNS** (see page 85) is activated.

HTTP

HTTP (Hypertext Transfer Protocol) is the standard protocol for transferring data on the Internet. You can use this to publish your own homepage on the Internet, for example.

- ➔ Activate the HTTP service for your Web server.
- ➔ You can change the **Port** via which Internet users can access your data, to mask your data and protect it from unauthorised users, for example.
- ➔ Choose the **Directory** in which the data is stored on the USB mass storage device and which should be shared for Internet access using the **Browse** button. Please note that this will share the selected directory and all its subdirectories for Internet access.

The `/usb0/gigaset_http` path is shown by default. `usb_0` is the partition number on the USB device. After you have chosen a directory on the USB device, this will be shown.

Internet users can access the HTTP server as follows:

- ➔ Open the Internet browser and enter the full address:

```
http://public_IP_address:[port]/gigaset_http/directory/  
start_file
```

public_IP_address

IP address of the Gigaset SX686 WiMAX assigned by the Internet service provider. This address is shown on the **Status** page (see page 136).

If you use a dynamic DNS service (see page 75) enter the domain name given by your service provider instead of the IP address.

Port

The port 80 is used for the HTTP service by default. **Port** must only be specified if another port is used for the HTTP server.

gigaset_http

This is a fixed part of the path and has to be entered always.

directory

Enter the directory in which the HTTP server start file is located on the USB mass storage device. You have to enter the full directory path of the shared directory.

Example: If the Web server is located in the `/usb0/web-server/my_webpage` directory and the `/` directory is shared, you have to enter this full path. If the `/usb0/web-server/my_webpage` is shared, you can start the Web server without entering the path.

start_file

Enter the name of the HTTP server start file.

Configuring Advanced Settings

Example:

The public IP address of your Gigaset SX686 WiMAX is **159.134.4.16**. The data is stored in the **/usb_0/WebServer/my_webpage** directory and you have shared the **/usb_0/WebServer** directory. The start file is **index.htm**. You use the port number 51000.

A remote user has to enter the following:

http://159.134.4.16:51000/gigaset_http/my_webpage/index.htm

Or, when using a dynamic DNS service:

http://my.dyndns.com:51000/gigaset_http/my_webpage/index.htm

FTP

FTP (File Transfer Protocol) is a protocol for exchanging files on the Internet. You can use this to offer files for downloading or to receive files from other users, for example.

➔ Choose **On** for **FTP service** if you want to make data available in the local network.

PCs in the network access the USB mass storage device via FTP.

To do this, open the Internet browser and enter the following address:

ftp://192.168.2.1

If you have changed the IP address of the Gigaset SX686 WiMAX (see page 88), enter the new address instead of 192.168.2.1.

➔ Choose **On** for **Remote FTP service** if you also want to make data available on the Internet.

Internet users can access your USB mass storage device by entering the public IP address in the Internet browser. As Internet service providers often change this each time someone dials in, it is also worth using dynamic DNS (page 85).

➔ The **Port** field contains the port number via which local PCs and Internet users can access your data. You should not change the default port number without very good reason.

If you use a different port number, active FTP mode is no longer possible. FTP clients must then be converted to passive FTP mode.

➔ Choose the **Directory** in which the data is stored on the USB mass storage device using the **Browse** button.

You can allow general access for both FTP services, or only for selected users with a user name and password.

➔ For **Access (read only)**, select whether all users should be able to read your data in **Anonymous** mode or whether only one **Specified user** should be supported.

➔ Specify whether **Access (full control)** to your data should be **disabled** or whether a **Specified user** may read, edit and delete your data.

➔ Enter the name in the **Specified user** field. Define different user names for the different access type and directory.

- ➔ Enter the password for the user and confirm it by entering it again in the field below. The password is case-sensitive. Avoid using proper names and obvious terms. Instead, use upper case and lower case letters, numbers and special characters.
- ➔ Click **OK** to apply the changes.

Print Server

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

Notes:

- ◆ The Windows Vista, Windows XP or Windows 2000 operating system is a prerequisite for using the print server.
- ◆ Only printer functionality is supported in the case of multifunction devices (combination of printer, scanner or fax). You can obtain additional information by contacting the hotline or else on the Internet (address 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 in the screen. You can check the status of the connection to the USB device on the **Advanced Settings – USB** screen.

- ➔ In the **Advanced Settings** menu, select: **USB – Print Server**

The screenshot shows the 'Print Server' configuration window. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. A 'Log Off' link is in the top right corner. The window title is 'Print Server' with a help icon (?). The configuration options are: 'Print server:' with radio buttons for 'On' (selected) and 'Off'; 'IP address:' set to '192.168.2.1'; and 'Device:' set to 'USB Printer'. At the bottom, there are 'OK' and 'Cancel' buttons.

- ➔ Activate your devices integrated print server.

You can set up the connected printer on your PC by using the **IP address** of the Gigaset SX686 WiMAX shown here when configuring the printer.

- ➔ Click **OK** to accept the changes.

You will find information on setting up the printer connected to the Gigaset SX686 WiMAX in the section entitled "Using the USB port" on page 147.

Call guide

Your Gigaset SX686 WiMAX allows you to make calls via the Internet (VoIP) and your fixed line. A description of how to configure your Gigaset SX686 WiMAX for using the telephone functions is provided under "Telephony" on page 56 and "Setting up Internet telephony (VoIP)" on page 105.

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.

Please note:

With the exception of the first five key combinations, the key combinations specified in this chapter only apply for telephones on the **Phone1** and **Phone2** ports. The key combinations ***1 ...*6**, ******, ***99***, ***00** and ***01 to *06 phone number** can also be entered on a SIP client. Please refer to the operating manual for your SIP client for the other functions.

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 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* .
*00 Phone number	Switching from VoIP to fixed network for a call	To make a call on a VoIP extension via the fixed network, simply enter *00 .
*01 to *06 Phone number	Switching to a VoIP extension for a call	If you want to make a call on a VoIP or fixed network extension via a (different) VoIP extension, you can use this VoIP connection by entering *0 and the number of the desired extension (1 ... 6) (e.g. *04 for the fourth extension).

Key combination	Effect	Description
*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 SX686 WiMAX, apply both for external calls and for internal calls. The functions described below are dependent on the connected terminal in the case of VoIP extensions.

Please remember:

When using the signal button **R**, always wait until you hear a dialling tone before you enter the phone number for a consultation call or complete the key combination for the respective function.

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 call is rejected automatically after 120 seconds have elapsed.

Call guide

Key combination	Effect	Description
R1	Terminate one call and return to the waiting 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 external 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* , the desired internal phone number to which all calls are to be forwarded that are received on this extension, and then press the # key. Example: You want to set up call forwarding from your phone to a second internal phone number. Dial *21**2# .
#21#	Delete call forwarding	Use the key combination #21# to delete internal call forwarding, which you set up as described above.

Key combination	Effect	Description
61[number]#	Call forwarding to internal number if absent	Dial *61* , 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* , 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 line busy	Use the key combination #67# to delete internal and external 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 all calls	Use the key combination *26# to specify that all calls are to be rejected. This is only possible if call waiting is disabled.
#26#	Delete the reject calls setting	Use the key combination #26# to delete the reject all calls setting.

Notes:

- ◆ If you additionally enter ***#** in each case before the key combination shown in the table, the settings will be forwarded directly to the exchange and will be activated there.
- ◆ The phone numbers of waiting calls are not displayed even if the caller permits this.

Special functions

Key combination	Effect	Description
*52#	Enable WLAN function	This shortcut key allows the WLAN function of your Gigaset SX686 WiMAX to be enabled without you having to open the configuration program.
#52#	Disable WLAN function	This shortcut key allows the WLAN function of your Gigaset SX686 WiMAX to be disabled again.

Note:

This function is only available if **Phone-based Management** is enabled. For that purpose open the user interface **Advanced Settings – Administration – System Management** screen.

Confirmation tones

If you activate a service attribute, for example set up call forwarding, you will hear a positive confirmation tone if successful and a negative confirmation tone if unsuccessful.

Positive confirmation tone: Ascending tone sequence at 6-second intervals

Negative confirmation tone: Regular sequence of short low-frequency tones

Administration

The Gigaset SX686 WiMAX user interface includes several helpful functions for administration.

Regional Options	Enables regional settings (page 130)
System Password	Changes the system password (page 131)
System Management	Configures system management (page 132)
Save & Restore	Backs up and, if necessary, restores configuration data (page 133) or reset the Gigaset SX686 WiMAX to the factory settings (page 134)
Reboot	Reboots the device (page 134)
System Log	Configures settings for the system log (page 135)

Regional Options

For operating your Gigaset SX686 WiMAX, 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** menu, select: **Administration – Regional Options**

The screenshot shows the 'Regional Options' configuration screen. At the top, there are navigation tabs: 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings' (selected), and 'Status'. A 'Log Off' link is in the top right corner. The main content area is titled 'Regional Options' and contains the following settings:

- Country:** A dropdown menu set to 'Germany'.
- Automatically adjust clock for daylight saving changes:** Radio buttons for 'On' (selected) and 'Off'.
- Date format:** A dropdown menu set to 'dd.mm.yyyy'.
- Time format:** A dropdown menu set to 'hh:mm:ss'.
- Internet Time** section:
 - System time:** 01.01.0001, 01:27:47
 - Last synchronization with time server:** (unknown)
 - Use custom time servers:** Radio buttons for 'On' (selected) and 'Off'.
 - Preferred time server:** 0.pool.ntp.org
 - Alternate time server:** 1.pool.ntp.org

At the bottom of the screen are 'OK' and 'Cancel' buttons.

- ➔ 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 SX686 WiMAX 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** menu, select: **Administration – System Password**

The screenshot shows a configuration window titled "System Password" with a question mark icon in the top right. The window has a title bar with tabs for "up Wizard", "Security Setup Wizard", "Advanced Settings", and "Status". A "Log Off" button is located in the top right corner. The main content area contains the following fields and controls:

- Current password:** A text input field.
- New password:** A text input field.
- Confirm new password:** A text input field.
- Idle time before log off:** A field with a spinner set to "10" and the text "minutes".
- At the bottom, there are two buttons: "OK" and "Cancel".

After installation, the Gigaset SX686 WiMAX user interface is protected by the System Password **admin**. To prevent unauthorised changes being made to the configu-

Administration

ration, 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 SX686 WiMAX (page 16). This returns **all** your settings to the factory configuration. This means the system password is changed back to **admin**.

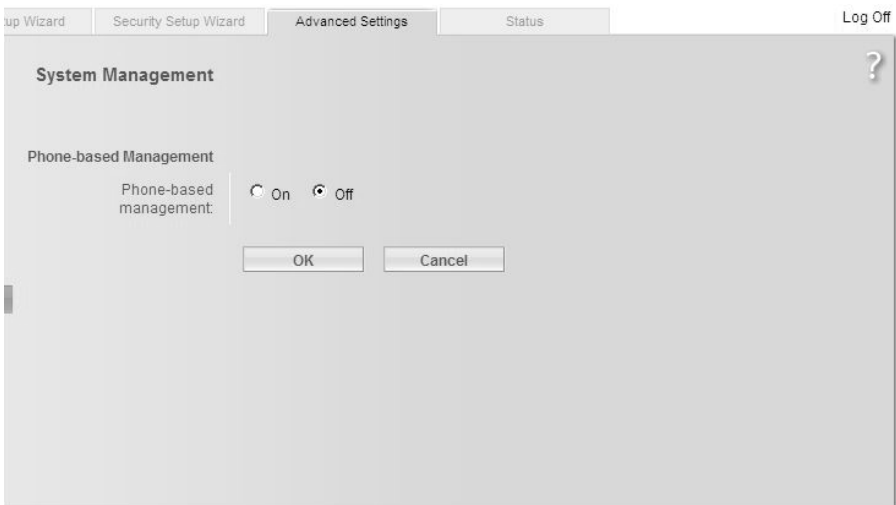
Idle time before log off:

- ➔ Enter the number of minutes after which the configuration program is to be ended if no further entry is made. The default is 10 minutes. If you enter 0, the program will never be ended automatically.
- ➔ Click **OK** to apply the settings.

System management

Your Gigaset SX686 WiMAX provides you with the option of switching the WLAN function of the device on and off via one of the connected phones. On this screen you can activate or deactivate this feature.

- ➔ In the **Advanced Settings** menu, select: **Administration – System Management**



Phone-based Management

➔ Click **On** to activate **Phone-based Management**.

You can activate or deactivate the WLAN function (page 128) via phone.

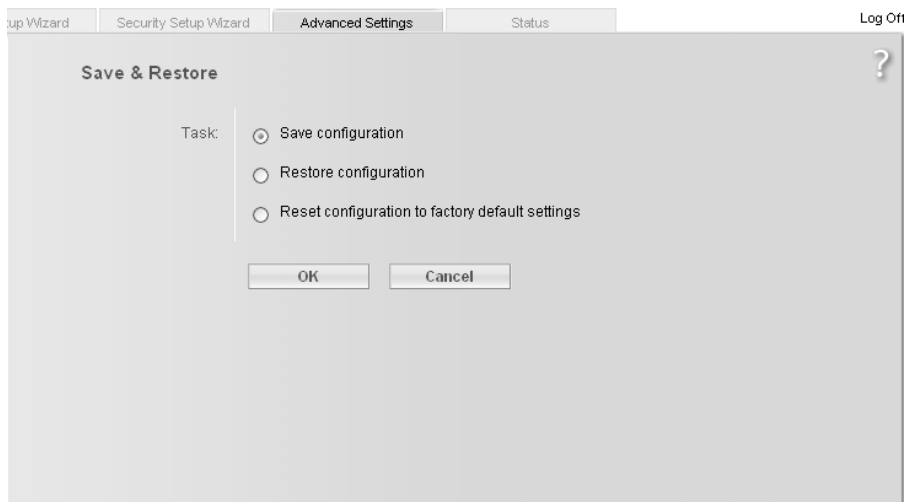
➔ Click **OK** to accept the settings.

Backing up and restoring a configuration

When the Gigaset SX686 WiMAX 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** menu, select: **Administration – Save & Restore**



Backing up configuration data

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

➔ Click **OK**.

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.
- ➔ Enter the path of the backup file that you want to use to restore the configuration or choose the file in the file system via the **Browse** button.
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 SX686 WiMAX 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 SX686 WiMAX is not operating properly, you can reboot it. It should then be ready for use again (page 16).

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 SX686 WiMAX.

Reboot

If the Gigaset SX686 WiMAX is not operating properly, you can reboot it. It should then be ready for use again.

- ➔ In the **Advanced Settings** menu, select: **Administration – Reboot**
- ➔ Click **OK** to reboot the device.

A window will appear prompting you to confirm the procedure.

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** menu, select: **Administration – System Log**

The screenshot shows the 'System Log' configuration window. It features a 'Log level' dropdown menu currently set to 'Warning'. Below it, the 'System log server' is set to 'On' via a radio button. The 'Server address type' is set to 'IP address'. The 'Server address' is entered as '127.0.0.1' and the 'Server port' is '514'. 'OK' and 'Cancel' buttons are at the bottom.

→ **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.
- **Warning** and **Informational** are intermediate levels.
- **Debugging:** Complete and detailed information on all device functions

Please remember:

Setting the log level **Debugging** can generate enormous load on the system and thus impair the data throughput of the device.

→ **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 type**
Choose if you want to enter the server address as IP address or domain name.
- **Server address**
Enter the IP address or the domain name 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 SX686 WiMAX is displayed in the **Status** menu of the Gigaset SX686 WiMAX. On the first screen you will find an overview of the status of the WiMAX connection, the Internet connection, the local and wireless network, the telephony, the USB interface and the device.

Detailed information is available on the following status screens:

- ◆ **Security**
- ◆ **Radio Status**
- ◆ **Internet**
- ◆ **Local Network**
- ◆ **Wireless Network**
- ◆ **Telephony**
- ◆ **Device**
- ◆ **Alarms**

To display a status screen:

- ➔ Select **Status** in 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.

WiMAX

- ◆ **Connection status**

The status of the connection to the WiMAX network (**Connected with base station** or **Disconnected**)

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.

◆ **Registration Button**

Shows if the registration button (Scan button) on the device's back panel is enabled or disabled.

Telephony

◆ **VoIP accounts**

Shows the number of VoIP accounts and the connection status.

USB

◆ **Status**

Status of the USB connection of the device. It can be enabled (**On**) or disabled (**Off**). Additionally, the occurrence of the following problems is displayed:

USB device not supported or not recognized.

USB device not supported (the device exceeds the power consumption limit).

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.

➔ In the **Status** menu, select **Security**:

◆ **System password not changed**

The configuration program of the device is not sufficiently protected against unauthorised access because you have not changed the system password since setting up the device. Information on how to avoid this security risk is given in the section "System Password" on page 131.

Status information

◆ **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 the section "Configuring wireless connections" on page 91.

◆ **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 the section "Setting encryption" on page 94.

◆ **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 the section "Permitted clients" on page 101.

◆ **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 the section "Firewall" on page 76.

◆ **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 the section "Setting up the NAT function" on page 80.

◆ **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 the section "Opening the firewall for a selected PC (Exposed Host)" on page 84.

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

Radio Status

Information about received and sent data as well as possible data transmission errors is displayed in the **Radio Status** submenu.

◆ **Received power level**

Range: from -30 dBm to -90 dBm

Readings above -30 dBm indicate possible traffic on the RF interface, and in this case all other measured values are invalid. Averaging is carried out according to the standard.

◆ **Transmitted power level**

Current transmission power.

◆ **Carrier to interference and noise ratio**

CINR = Carrier to Interference plus Noise Ratio. The CINR calculation is based on the value of the downlink measurement. Averaging is carried out according to the standard.

◆ **Current uplink channel center frequency**

Currently used uplink frequency. The reading changes frequently during the measurement.

◆ **Current downlink channel center frequency**

Currently used downlink frequency. The reading changes frequently during the measurement.

◆ **Current channel size**

Currently used bandwidth.

◆ **Radio port uplink current average throughput**

Average approximate uplink throughput in 1 second, moving average (5 samples).

◆ **Radio port downlink current average throughput**

Average approximate downlink throughput in 1 second, moving average (5 samples).

◆ **Current uplink modulation scheme**

Currently used uplink modulation type.

◆ **Current downlink modulation scheme**

Currently used downlink modulation type.

➔ 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.

➔ In the **Status** menu, select **Internet**:

◆ **Connection services**

You can select the **Connection service**, for which the following information is to be displayed.

This information is not displayed if you only set up one connection service.

◆ **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 72), you can **Connect** or **Disconnect** the connection to the Internet manually here.

◆ **Connection mode**

Shows the connection mode set for connecting to the Internet.

Status information

- ◆ **IP address**
Shows the current public IP address of the device.
 - ◆ **MAC address**
Shows the public MAC address of the device.
 - ◆ **Default gateway**
Shows the IP address of the assigned default gateway.
 - ◆ **Preferred DNS server**
Shows the IP address of the assigned DNS server.
 - ◆ **Alternate DNS server**
Shows the IP address of the alternate DNS server, if available.
 - ◆ **Downstream rate**
Shows the current transmission rate for incoming traffic.
 - ◆ **Upstream rate**
Shows the current transmission rate for outgoing traffic.
 - ◆ **PPPoE pass-through**
Shows the status of PPPoE pass-through for the WiMAX connection for establishing an Internet connection directly between a PC and the network.
 - ◆ **Address Translation (NAT)**
Shows the status of the NAT (Network Address Translation) for the Internet connection.
 - ◆ **Dynamic DNS**
Shows the status of the configuration for dynamic DNS. If dynamic DNS is set up, the name of the provider is shown.
- ➔ 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.

- ➔ In the **Status** menu, select **Local Network**:
- ◆ **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 to identify each client. Information is also provided about the **IP address** assigned to each client and about the **Lease time** for the IP address, i.e. the length of time before the current IP address becomes invalid and the client is 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.

➔ In the **Status** menu, select **Wireless Network**:

- ◆ **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.

- ◆ **Repeater (WDS)**

- **Status**

Shows the status of the WDS (Wireless Distribution System) in the wireless network for increasing the range.

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

Telephony

You will find information about the VoIP accounts and phone call statistics on the **Telephony** screen in the **Status** menu.

➔ In the **Status** menu select **Telephony**:

◆ **VoIP accounts**

Shows the number of VoIP accounts and the connection status.

◆ **SIP client accounts**

All WLAN handsets or other SIP clients currently set up as extensions 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.

Note:

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

Device

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

➔ In the **Status** menu, select **Device**:

◆ **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.

◆ **MAC version**

Indicates the internal version of the installed MAC layer. The MAC layer is part of the system software. During a software upgrade of the modem a new MAC layer might also be installed.

◆ **Bootcode version**

Shows the version of the bootcode currently installed on your device.

◆ **Configuration file version**

Shows which configuration file is loaded.

◆ **Calibration date**

Shows the date when the device was manufactured and calibrated.

◆ **Wireless driver version**

Shows the version of the WLAN driver currently installed on the device.

◆ **User interface version**

Shows the version of the user interface currently installed on the device.

◆ **Hardware version**

Shows your device's hardware version.

◆ **Serial number**

Shows your device's serial number.

◆ **Device Temperature**

Shows the current temperature inside the device in degrees Celsius (°C). This temperature should be below 75°C. In the event of overheating, the Gigaset SX686 WiMAX switches off.

◆ **System Log**

The system log contains important information about how the device functions and possible problems. You can adapt the scope of the system log to suit your requirements (see "System Log" on page 135).

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

Alarms

The Gigaset SX686 WiMAX provides two kinds of alarm information for the WiMAX network:

◆ **Functional Alarms**

Conditions such as insufficient link quality that is affecting throughput, failure to obtain network access or servers unavailable in the backbone are indicated in this group. These alarms together with their detailed description in the error log will pinpoint the fault. These conditions may result in "bad" Internet connections, lag or complete failure to access the Internet.

Transient Alarms, such as the **Overtemperature** condition, are a special kind of functional alarm indicating a non-durable condition.

◆ **Physical Alarms**

Physical alarms always indicate a failure that cannot be repaired at the end-user or admin site. The device has to be returned to the supplier service for repair or replacement.

A physical alarm is always indicated by a permanently lit red **Status** LED (see page 14).




Status information

Alarm display in the user interface

The alarm screens show the following information for each alarm:

Alarm indication describes the alarm.

State shows the current state of the alarm by means of a coloured symbol.

	Grey	Unknown
	Red	Active
	Green	Inactive

The symbols always show a snapshot of the situation at query time.

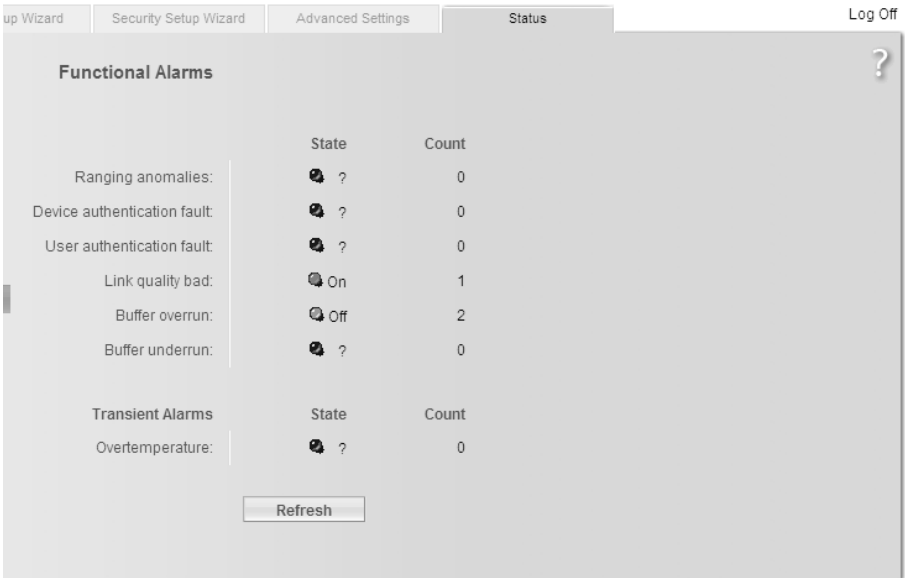
Count indicates how often the alarm has occurred since the last alarm reset.

Functional alarms: You can reset the value by powering off the device and restarting it.








Physical alarms: The alarm counters can only be set to zero by the service technician.

Functional Alarms

➔ In the **Status** menu, select **Alarms – Functional Alarms**:



The screenshot shows a web interface with a navigation bar at the top containing 'up Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. A 'Log Off' link is in the top right corner. The main content area is titled 'Functional Alarms' and contains a table of alarm data. A 'Refresh' button is located at the bottom of the table.

	State	Count
Ranging anomalies:	 ?	0
Device authentication fault:	 ?	0
User authentication fault:	 ?	0
Link quality bad:	 On	1
Buffer overrun:	 Off	2
Buffer underrun:	 ?	0
Transient Alarms		
Overtemperature:	 ?	0

Refresh

◆ **Ranging anomalies**

Communication to the base station is impaired as it is either too far away or the link quality is bad.

➔ Improve link. For helpful information please consult the sections "Aligning the antenna", "Searching a WiMAX network" and "Antenna fine tuning" from page 48.

◆ **Device authentication fault**

The device authentication failed. No operation is possible.

➔ Check the configuration and the service level agreement with your provider.

◆ **User authentication fault**

The user authentication failed. No operation is possible.

➔ Check the configuration and the service level agreement with your provider.

◆ **Link quality bad**

The Received Signal Strength Indication (RSSI) or Carrier to Noise Ratio (CNR) is below the configured threshold or the Packet Error Rate (PER) is above the specified threshold. This indicates that the link quality is below the expected quality.

➔ Improve link. For helpful information please consult the sections "Aligning the antenna", "Searching a WiMAX network" and "Antenna fine tuning" from page 48.

◆ **Buffer overrun**

Packets have been lost since all buffers were in use.

➔ Check your provider's service level agreement.

◆ **Buffer underrun**

Packets have been lost since no ready buffer was available.

➔ Check the service level agreement with your provider.

◆ **Overtemperature**

An overtemperature condition was detected. During overtemperature traffic is reduced in order to reduce power dissipation and heat.

➔ Wait until the device has cooled down and normal operation continues. Check if venting holes are blocked. Find better/cooler position for your device.

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

Physical Alarms

➔ In the **Status** menu, select **Alarms – Physical Alarms**:

◆ **RF PHY broken**

The RF chip for proper WiMAX communication is failing.

➔ Replace the device.

◆ **Auxiliary data broken**

Vital data for proper operation is missing. This information can only be stored by the supplier.

➔ Recalibrate the device.

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

The alarm counters can be set to zero only by the service technician activating a service reset.

Using the USB port

Your Gigaset SX686 WiMAX is equipped with a USB port that can be used, for example, to connect a printer for use as a network printer or a USB mass storage device for use as a file server. This chapter describes which settings you have to define on your computer to use these functions.

Note:

Depending on operating system variants and individual settings the procedures described may differ from your given facts. Follow the instructions of your operating system, if applicable.

Installing the printer port for network printers

The Windows Vista, Windows XP or Windows 2000 operating system is a prerequisite for connecting a printer under Windows.

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 multi-function 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 to which the printer is connected reduces the performance (resources) of this PC.

If you use the USB port on the Gigaset SX686 WiMAX 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 SX686 WiMAX and the printer itself must be switched on, of course).
- ◆ As it is connected to the USB printer port on your Gigaset SX686 WiMAX, 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.

Using the USB port

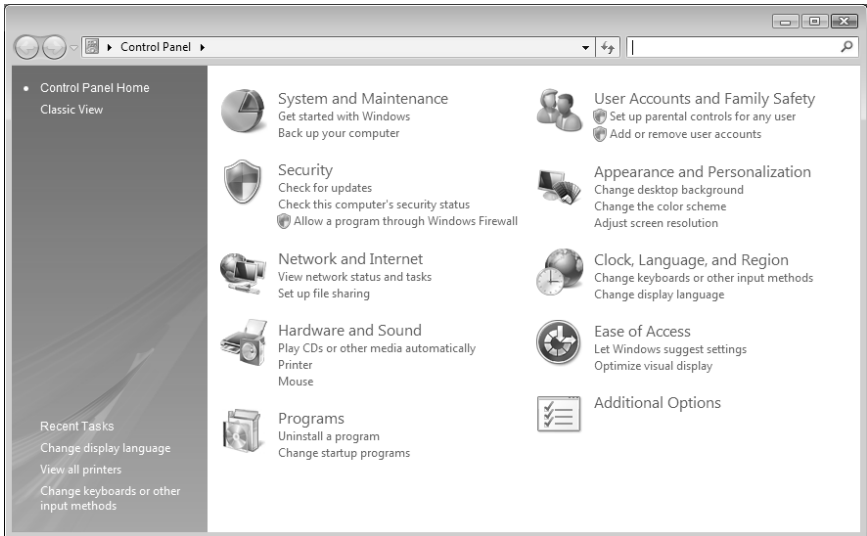
Note:

Before starting to set up the printer please make sure that a printer is connected to the USB port of the Gigaset SX686 WiMAX and that the printer has been identified. You can check this in the user interface via **Advanced Settings – USB – Print Server**.

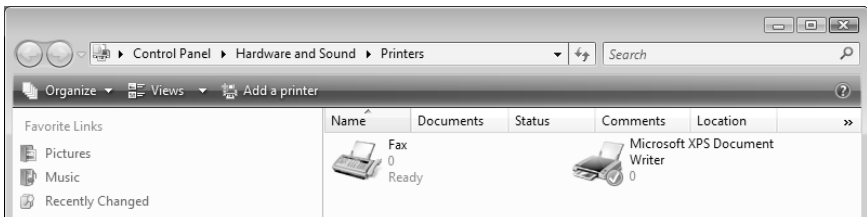
Installing a standard TCP/IP printer port under Windows Vista

You can use the standard TCP/IP port driver available with this operating system. Make sure that the Gigaset SX686 WiMAX is connected and is available in the network. A printer does not have to be connected to the USB port on your Gigaset SX686 WiMAX at this point.

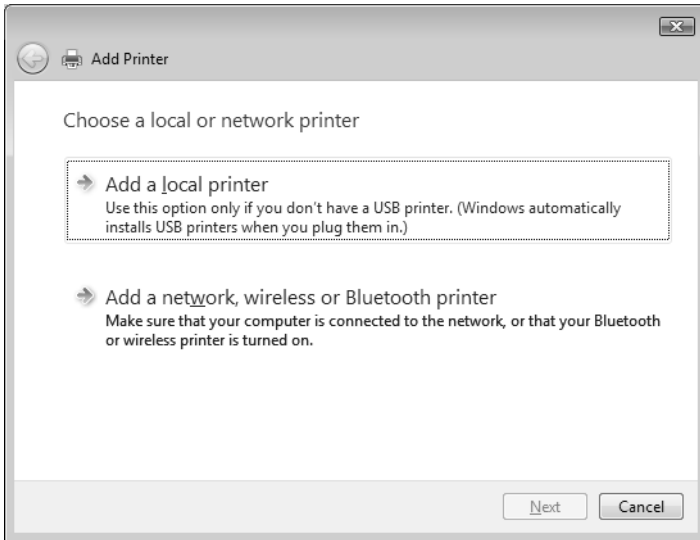
➔ Click **Start – Control Panel**.



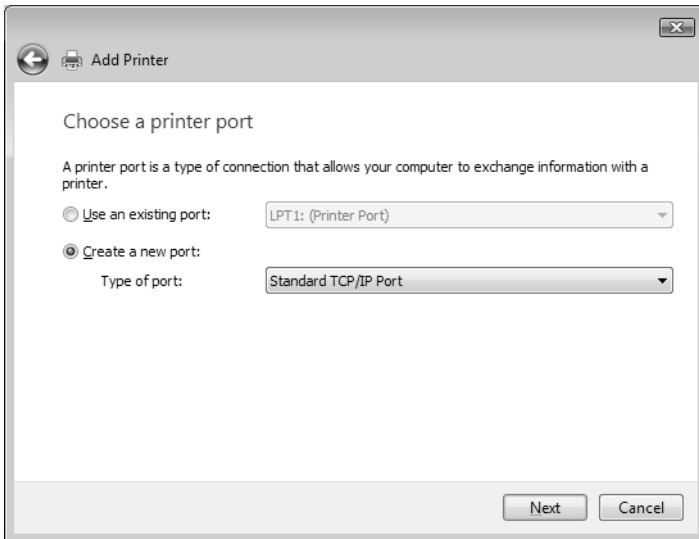
➔ In the window that opens, click **Hardware and Sound** followed by **Printer**.



➔ Click **Add a printer**.

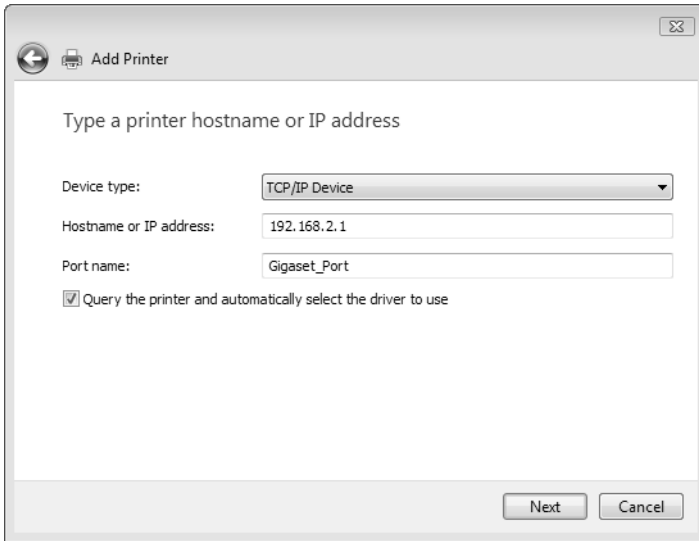


→ In the Add Printer Wizard, click the option **Add a local printer**.



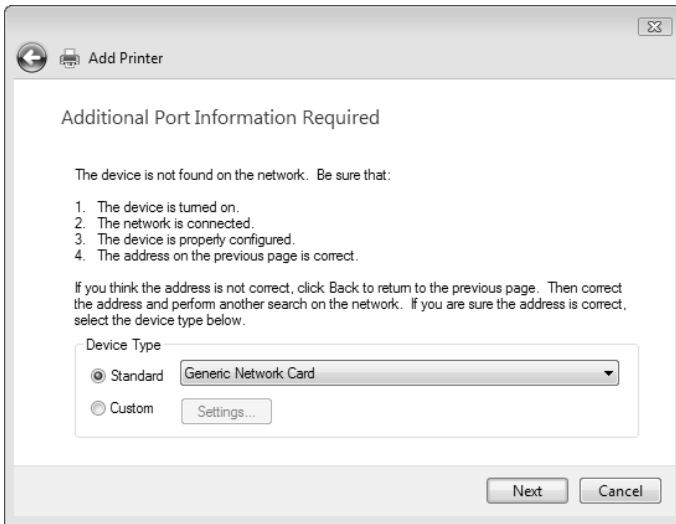
- Select the **Create a new port** option button.
- Then select **Standard TCP/IP Port** from the selection menu in the field **Type of Port**.
- Click **Next**.

Using the USB port

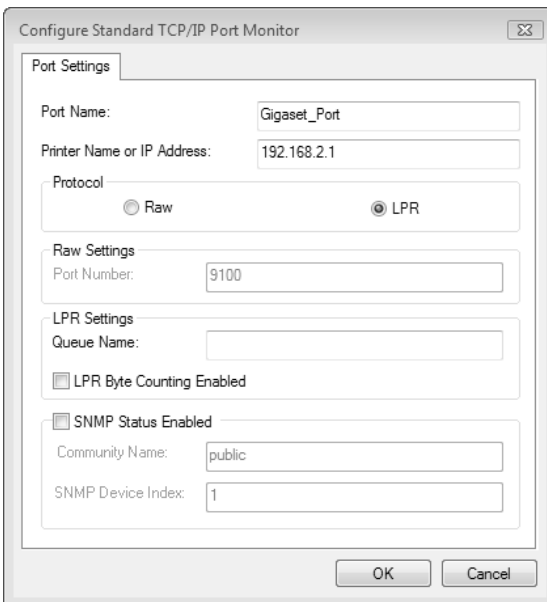


- ➔ Choose **TCPI/IP** as **Device type**.
- ➔ In the **Host Name or IP Address** input field, enter the IP address of the printer server (Gigaset SX686 WiMAX): e.g. 192.168.2.1.
This entry is transferred into the **Port Name** field. This name will later appear in the list of printer ports.
- ➔ To change the name, click in the **Port Name** field and enter a name. Name this port, for example, **Gigaset_Port**.
- ➔ Click **Next**.

As Windows Vista usually first looks for a network card when a printer port is installed, the **Additional Port Information Required** window is displayed.



➔ Select the **Custom** option and click on **Settings**.



➔ Select the **LPR** option box.

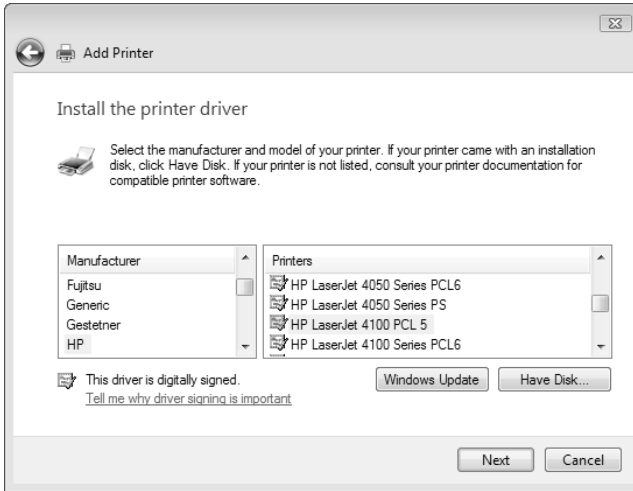
➔ For **Queue name** enter **lp0** (lower case: lima, papa, number 0).

➔ **LPR Byte Counting Enabled** should not be selected.

➔ Click on **OK** and then on **Next**.

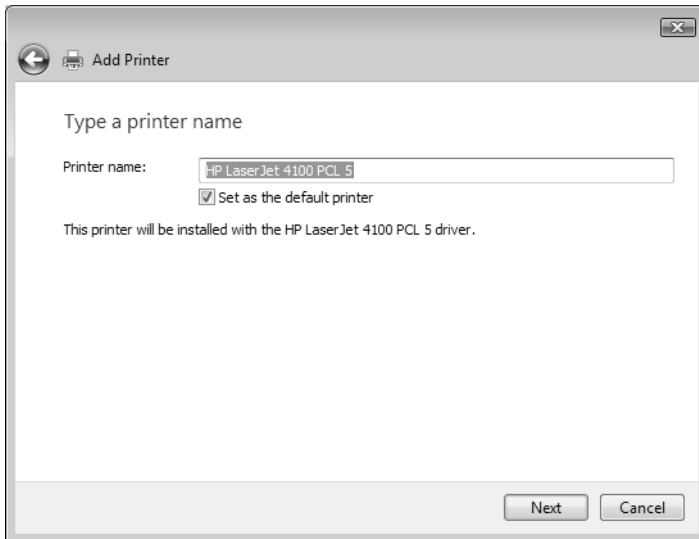
Using the USB port

Windows is searching for the appropriate driver model.



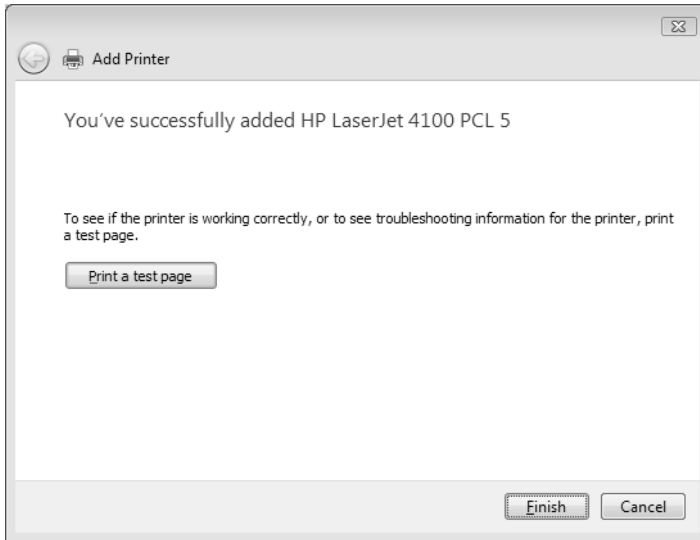
➔ Choose the appropriate driver for your printer and click on **Next**.

After successfully installing the driver you can now define a name for your printer. This is the name which is used to display the printer in the printer list.



➔ Enter a printer name and select the option **Set as the default printer**.

➔ Click **Next**.



- ➔ Click the button to print a test page.
- ➔ Click **Finish**.

Note:

The printer server of the Gigaset SX686 WiMAX does not work bi-directionally. It does not evaluate any of the printer's response messages. For this reason please make sure that your printer is also only configured uni-directionally. You can configure the relevant settings for your printer by choosing **Start – Settings – Printers**.

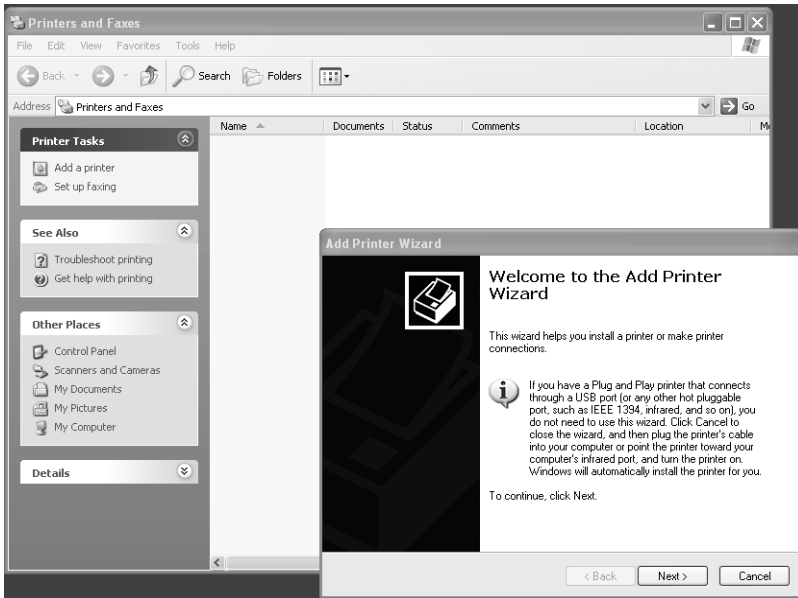
Installing a standard TCP/IP printer port under Windows XP/2000

You can use the standard TCP/IP port driver available in this operating system. Make sure that the Gigaset SX686 WiMAX is connected and can be reached in the network. A printer need not be connected to the USB port on your Gigaset SX686 WiMAX 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.



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

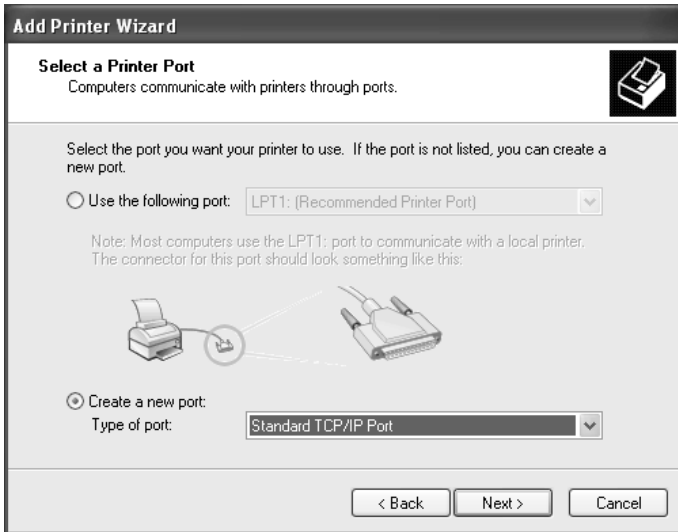


The printer port you are installing will behave like an additional parallel port on the PC. For this reason you must click the option button next to **Local printer** in this window.

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

➔ Click **Next**.

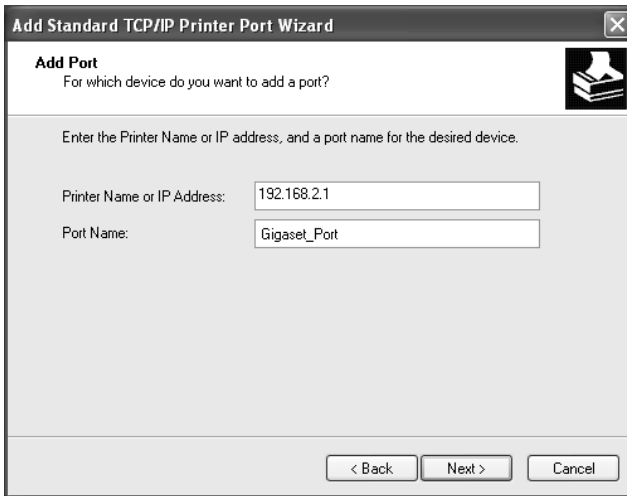
Using the USB port



- ➔ 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**.

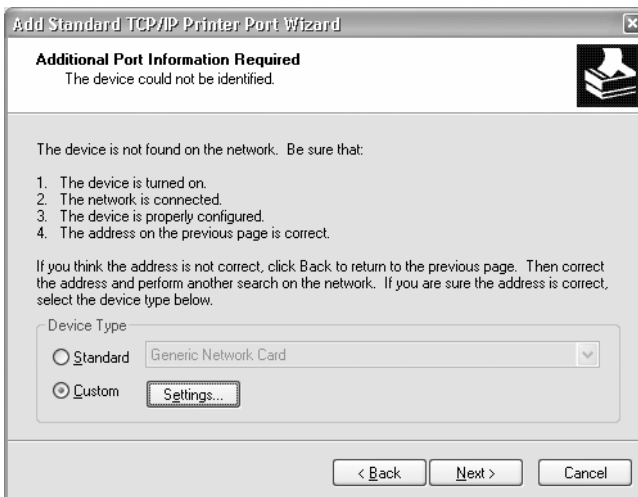


- ➔ In the wizard for setting up a standard TCPI/IP port, click **Next**.



- ➔ In the **Printer Name or IP Address** input field, enter the IP address of the print server (Gigaset SX686 WiMAX): 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_port**.
- ➔ 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.



- ➔ Choose the option **Custom** and click **Settings**.



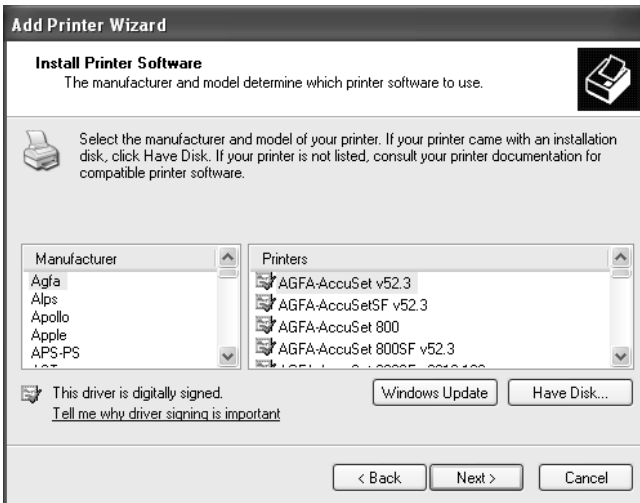
- ➔ Enter the following data in the relevant fields:
 - **Printer name or IP address:** Enter the IP address of the print server.
 - **Protocol** Choose the option **LPR**.
 - **Queue name:** lp0 (lower case: lima, papa, number 0)
 - **LPR Byte Counting Enabled** should not be selected.
- ➔ Click **OK**
- ➔ Click **Next**.

The window for finishing the wizard is opened and shows you all the settings you have made.



→ Click **Finish**.

Once the wizard for installing the printer port is finished, the **Add Printer Wizard** is opened.



→ If you wish to install a printer for this port immediately, click **Next** and follow the instructions of the Add Printer Wizard.

Using the USB port

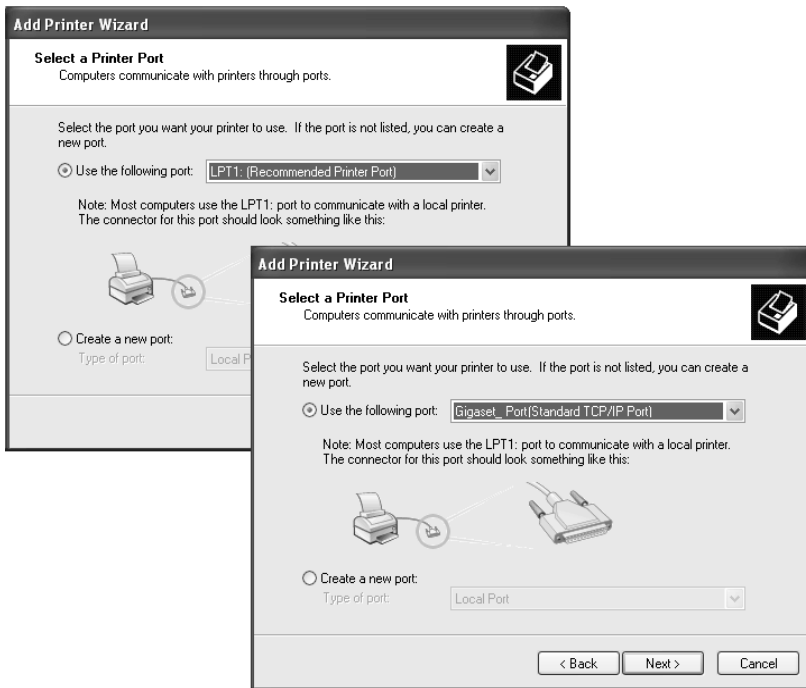
➔ If you do not wish to install a printer until later, click **Cancel**.

Note:

The printer server of the Gigaset SX686 WiMAX does not work bi-directionally. It does not evaluate any of the printer's response messages. For this reason please make sure that your printer is also only configured uni-directionally. You can configure the relevant 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.



- ➔ 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_port (Standard TCP/IP port)**.
- ➔ Click **Next** and finish installing the printer driver as instructed in the windows that follow.

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 SX686 WiMAX.

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**.

➔ 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**.

➔ When the window in which you are prompted to enter the type of connection appears, double-click the port name **Gigaset_port**.

➔ Then continue to install the printer and finish the installation.

Note:

The printer server of the Gigaset SX686 WiMAX does not work bi-directionally. It does not evaluate any of the printer's response messages. For this reason please make sure that your printer is also only configured uni-directionally.

Using the data on a USB mass storage device

To view directories and files which are shared via the Gigaset SX686 WiMAX file server on the USB port within the Windows network, some parameters on your PC must be set correctly.

For most PCs these settings are already defined correctly on delivery, i.e. you usually do not have to do anything. The following sections give some diagnosis information in case problems do occur.


The following description is based on the Windows Vista operating system. The procedure is similar for the other Windows systems. You will find a detailed description of the network configuration for the different Windows systems on the CD-ROM delivered with the device.

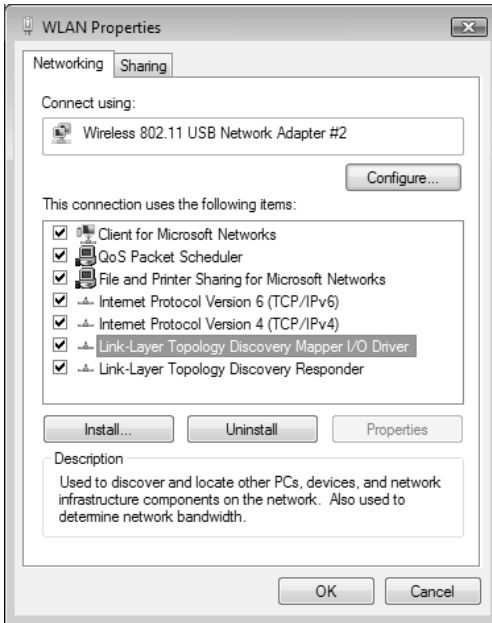
Checking network services

The following services/protocols must be activated for the network connection used:

- ◆ Internet protocol (TCP/IP)
- ◆ File and Printer Sharing for Microsoft networks

You can check it via the **Properties** of the network connection.

- ➔ Click on the network symbol in the taskbar .
- ➔ Open the **Network and Sharing Center**.
- ➔ Click **View status** next to the network connection used to connect your PC to the Gigaset SX686 WiMAX.
- ➔ Click **Properties**.



The check boxes next to the entries

- ◆ Internet Protocol Version 4 (TCP/IPv4)

and

- ◆ File and Printer Sharing for Microsoft Networks

must be marked.

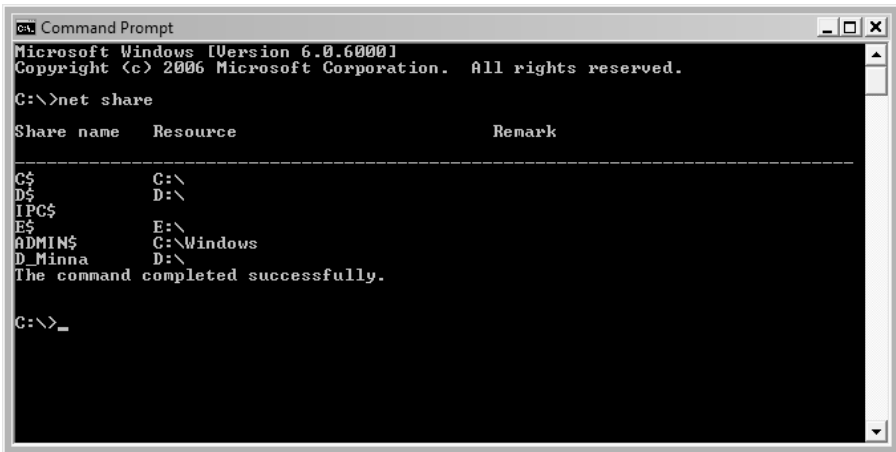
➔ If one of these components is not installed it will have to be installed subsequently. You may need your Windows installation CD.

Share Inter Process Communication for the network

The Inter Process Communication (IPC) functions are used to interchange data between processes on a computer or between multiple computers in a network. To be able to share data on the USB mass storage device on the Gigaset SX686 WiMAX, the IPC must be set to access resources shared in the network (network share).

You can check it as follows:

- ➔ Open the Windows command prompt. From the start menu of the Windows taskbar, click **Start – All Programs – Accessories – Command Prompt**.
- ➔ In the **Command Prompt** window enter the **net share** command and press the ENTER key.



```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\>net share

Share name      Resource          Remark
-----
C$              C:\
D$              D:\
IPC$
E$              E:\
ADMIN$          C:\Windows
D_Minna         D:\
The command completed successfully.

C:\>_
```

- ➔ Check if an **IPC\$** entry exists.
- ➔ If there is no entry, enter the **net share IPC\$** command and press the ENTER key.

Starting the computer browser

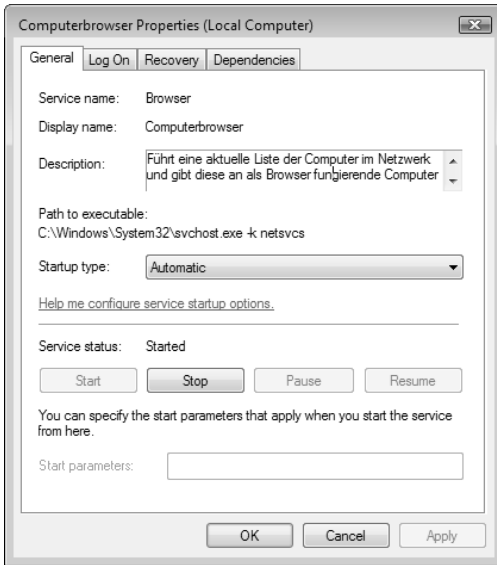
To access resources in the network, the Windows service **computerbrowser** must be started.

You can check it as follows:

- ➔ Open the Control Panel by selecting **Control Panel** from the start menu of the Windows taskbar.
- ➔ Open **System and Maintenance**, then **Administrative Tools** and click on **Services**.

Note: On Windows XP and 2000 systems right-click on the **Workplace** symbol and choose **Administrative Tools**. Double-click on **Services and Applications** and then on **Services**.

- ➔ Check if the status for the **Computerbrowser** entry is **Started**.
- ➔ If **Computerbrowser** is not started, double-click on the entry.



➔ Click on **Start**.

If an error message appears with a content like "..has been started and then stopped again..", you still have to allow file and printer sharing in the Windows firewall (see next section).

Enabling file and printer sharing in the Windows firewall

The Windows firewall must be set to allow file and printer sharing.

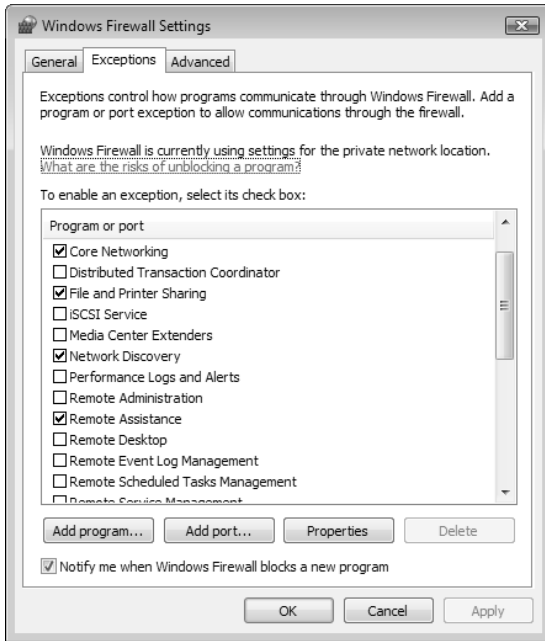
You can check it as follows:

- ➔ Open the Control Panel. For that purpose choose **Control Panel** from the start menu of the Windows taskbar.
- ➔ Click on **Security – Windows Firewall** and then **Starting and Stopping the Windows Firewall**.

Note: On Windows XP systems in the Control Panel choose the **Windows Firewall** entry.

- ➔ Open the **Exceptions** tab.

Using the USB port



The File and Printer Sharing entry must be marked.

Now your Windows system should be able to access the shared data on the Gigaset SX686 WiMAX.

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, consult of the following table. Further information is available on the Internet at <http://www.gigaset.com/customer-care>.

This user guide is based on the software release 7.0.

Make sure the firmware on your device is up-to-date. The latest version can be found on the Internet on the product page www.gigaset.com/gigaset-sx686-wimax.

Symptom	Possible cause and solutions
Power LED does not light up.	<p>No power supply.</p> <ul style="list-style-type: none"> ➔ Check whether the mains adapter is connected to the Gigaset SX686 WiMAX 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 your supplier service.
Status LED does not light up.	<p>No registration to a WiMAX network.</p> <ul style="list-style-type: none"> ➔ Check if the antenna has been moved out of position or the device's alignment has been changed. In this case, restore the original alignment. ➔ Register your Gigaset SX686 WiMAX with the help of the connection wizard; see page 47.
Status LED flashing green	<p>A connection is being established. This is not a fault.</p> <ul style="list-style-type: none"> ➔ Please wait until the connection is established. The LED will then light up permanently.
Status LED is red	<p>The Gigaset SX686 WiMAX is not ready for use.</p> <p>The device may be too hot. In this case, the integrated overheating protector prevents the Gigaset SX686 WiMAX from being damaged. If the temperature rises, the Gigaset SX686 WiMAX automatically reduces data transfer to a minimum. When the temperature exceeds the critical value, the Gigaset SX686 WiMAX switches itself off.</p> <ul style="list-style-type: none"> ➔ Wait until the Gigaset SX686 WiMAX has cooled down.

Symptom	Possible cause and solutions
<p>Status LED is permanently lit red; overheating of the device can be excluded</p>	<p>The Gigaset SX686 WiMAX may be faulty.</p> <ul style="list-style-type: none"> ➔ Restart the Gigaset SX686 WiMAX. If the Status LED remains red after the device has been restarted and does not extinguish, please contact your supplier service.
<p>Only a few LEDs have lit up to display the signal strength (RSSI) and the Status LED is green</p>	<p>If you are using the antenna integrated in the Gigaset SX686 WiMAX,</p> <ul style="list-style-type: none"> ➔ turn the Gigaset SX686 WiMAX until more LEDs light up. Try to place the device even closer to the window and check the signal strength bar in the BAsic Setup wizard for the configuration program.
<p>Additional information on possible errors during WiMAX operation can be found on the Status screen Alarms. Please refer to the section "Alarms" on page 150.</p>	
<p>The LAN LED on a connected device does not light up.</p>	<p>No LAN connection</p> <ul style="list-style-type: none"> ➔ 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.

Symptom	Possible cause and solutions
<p>You cannot connect to the Internet.</p>	<ul style="list-style-type: none"> ➔ Check whether your device is connected to the WiMAX network by checking the Status LED. ➔ Check whether the data entered for your Internet connection matches what your Internet service provider has specified. ➔ Check whether the Connect manually option is activated. If it is, connections cannot be opened automatically. ➔ Select Connect on demand or Always on. 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. <ul style="list-style-type: none"> – Restore the connection again manually using the Connect button or – Restart the Gigaset SX686 WiMAX. <p>In both cases, the Connect on demand setting will be active again.</p>
<p>After a WPS registration attempt, the WLAN LED continues to flash for some time and the required client was not registered.</p>	<ul style="list-style-type: none"> ◆ More than one client has tried to register. ➔ Repeat registration after a short interval. ◆ MAC access control is activated, but the desired client is not in the MAC address list. ➔ Add the client to the MAC address list (see page 71). <p>If the MAC address filter is enabled a WPS registration attempt can not be detected by the device. In this case LED signalling is not possible.</p>
<p>After a WPS registration the WLAN LED shows successful registration but the desired client was not registered.</p>	<p>Maybe an external device has registered with your network.</p> <ul style="list-style-type: none"> ➔ Change the WPA PSK key manually as soon as possible (see page 104) and perform the WPS registration via PIN (see page 101).

Symptom	Possible cause and solutions
<p>You cannot open a connection to the Gigaset SX686 WiMAX from a wireless device.</p>	<ul style="list-style-type: none"> ◆ You attempted to perform WPS registration on the network adapter but the registration button was not activated on the Gigaset SX686 WiMAX. <ul style="list-style-type: none"> ➔ Activate the WPS registration on the Gigaset SX686 WiMAX and activate WPS within the two-minutes interval on the network adapter. ◆ You defined a PIN for WPS registration but the network adapter does not use a PIN or uses a different one. <ul style="list-style-type: none"> ➔ Check the wireless network encryption settings and determine the PIN used by the Gigaset SX686 WiMAX. Enter this PIN on the network adapter. ◆ You defined a PIN for WPS registration at the network adapter but you didn't enter this PIN at the Gigaset SX686 WiMAX PIN or not the right one. <ul style="list-style-type: none"> ➔ Find out the PIN that is used by the network adapter. Enter this PIN on the Gigaset SX686 WiMAX. ◆ The wireless network adapter is not using the correct SSID. <ul style="list-style-type: none"> ➔ Change the SSID on the network adapter or use the WPS function.
<p>You cannot open a connection to the Gigaset SX686 WiMAX from a wireless device.</p>	<ul style="list-style-type: none"> ◆ Either encryption has been activated on the Gigaset SX686 WiMAX but not on the wireless network adapter, or an incorrect key is in use. <ul style="list-style-type: none"> ➔ Activate the required encryption (WPA-PSK or WEP) on the network adapter with the correct key. <p>If you do not know the key, repeat key entry (page 101) via a PC connected via cable to the Gigaset SX686 WiMAX and enter the new key on the network adapter.</p> <p>Otherwise, you can use the WPS function.</p> <p>Alternatively, you can reset the Gigaset SX686 WiMAX (page 19) and then reconfigure encryption.</p> <p>Warning: Please bear in mind that this will reset the entire configuration to the factory settings.</p> ◆ MAC access control is activated, but the PC is not included in the MAC address list. <ul style="list-style-type: none"> ➔ Enter the PC in the MAC address list.

Symptom	Possible cause and solutions
<p>The Gigaset SX686 WiMAX or other PCs cannot be reached by a PC in the connected LAN using a ping command.</p>	<ul style="list-style-type: none"> ➔ 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 SX686 WiMAX 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. <p>If you configure IP addresses in the LAN manually, remember to use the same subnet mask for all PCs in the LAN. This means that the masked part of the IP address on each PC and on the Gigaset SX686 WiMAX has to be identical.</p>
<p>No connection to the configuration environment of the Gigaset SX686 WiMAX.</p>	<ul style="list-style-type: none"> ➔ Use the ping command to check whether you can establish a network connection to the Gigaset SX686 WiMAX. ➔ Check the network cable between the PC you want to use to administer the device and the Gigaset SX686 WiMAX. ➔ If the PC you want to use for administering the device is in the router's local network, make sure that you are using the correct IP address range (see above). ➔ If the PC you want to use for administering the device is not in the router's local area network, this PC must be authorised for remote management.
<p>You cannot conduct VoIP telephone calls.</p>	<ul style="list-style-type: none"> ➔ The access data for your VoIP phones is not entered correctly. Check the access data (see page 117). ➔ You have not assigned the VoIP phone numbers to the telephone port. Check the configuration of the telephone ports and the extensions (see page 121). ➔ Your VoIP configuration is not set up with the correct Codecs. Contact your VoIP provider and assign the correct Codecs (see page 117).
<p>Password forgotten or lost.</p>	<ul style="list-style-type: none"> ➔ Reset the Gigaset SX686 WiMAX (page 19). <p>Warning: Please bear in mind that this will return all the configuration settings to the factory settings.</p>

Symptom	Possible cause and solutions
You cannot access a resource (drive or printer) on a different PC.	<ul style="list-style-type: none"> ➔ 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.

Gigaset SX686 WiMAX functions and their interdependency

The following table shows which functions of your device are possible in which combination. In the case of error, check that the following conditions are fulfilled:

Function	Possible in combination with	Not possible in combination with
WPS	WPA2-PSK/WPA-PSK encryption no encryption	WPA2/WPA authentication WEP encryption
WDS	WEP encryption no encryption	WPA2-PSK/WPA-PSK or WPA2/WPA authentication

Operating information:

◆ USB port

If connecting a device without its own power supply directly to the USB port, please note that the power consumption must not exceed 500 mA. If this value is exceeded, you will have to use a separate power supply unit for your USB device or connect a USB hub with a separate power supply. A USB hard drive and a USB printer can be operated simultaneously on a USB hub.

◆ LAN ports

The LAN ports may only be used for in-house networks. The ports are destroyed externally if there is a power surge.

◆ Telephone 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.

Deactivating HTTP proxy and configuring a pop-up blocker

Before you can start the configuration program of the Gigaset SX686 WiMAX, you might need to adjust the settings described below for your Web browser.

Deactivating the HTTP proxy

Make sure that the [HTTP proxy](#) in your web browser is deactivated. This function must be deactivated so that your web browser can access your Gigaset SX686 WiMAX's configuration pages.

The following section describes the procedure for Internet Explorer and Mozilla Firefox. First decide which browser you wish to use, and then follow the appropriate steps.

◆ Internet Explorer

- ➔ Open Internet Explorer and from the **Tools** menu, select **Internet Options**.
- ➔ In the **Internet Options** window, click the **Connections** tab.
- ➔ Click **LAN Settings**.
- ➔ Deactivate all options in the **LAN Settings** window.
- ➔ Click **OK** and then **OK** again to close the **Internet Options** window.

◆ Mozilla Firefox

- ➔ Open Mozilla Firefox. Click **Tools** and then **Settings**.
- ➔ In the **Settings** window, click **Connection Settings...**
- ➔ In the **Connection Settings** window, select the option **Direct connection to the Internet**.
- ➔ Click **OK** to finish.

Configuring the pop-up blocker

You must allow pop-ups for the configuration program in order to start it.

◆ Internet Explorer

If working with Windows XP Service Pack 2, pop-ups are blocked by default. If the configuration program is blocked carry out the following steps:

- ➔ Right-click on the browser information bar. It is displayed if a page is blocked.
- ➔ Select **Allow popups from this screen**.
- ➔ Confirm the dialogue window by clicking **OK**.

The configuration screens for the Gigaset SX686 WiMAX are now allowed as pop-ups.

You can make additional settings for pop-ups within Internet Explorer via the **Tools – Popup Manager** menu item or via **Tools – Internet Options** on the **Privacy** tab.

Appendix

◆ Mozilla Firefox

Pop-ups are blocked by default. Carry out the following steps:

- ➔ Open Mozilla Firefox. Click **Tools** and then **Settings**.
- ➔ Click on the **Content** icon.
- ➔ Deactivate the **Block Popup window** option.
- ➔ Click **OK** to finish.

Please note:

Should you use a different pop-up blocker, you must configure this accordingly.

Specifications

Interfaces

4 LAN	RJ45, 10Base-T/100Base-TX, Auto-sensing
1 USB	USB 2.0, for printer server or file server (max. 500 mA)
2 FXS	RJ11, for connecting analogue terminals (phone, fax, answering machine)
WLAN	802.11 b/g, for wireless connection of up to 252 PCs
Mains adaptor	Input 100-240 V AC, output 12 V DC / 2.0 A

WiMAX properties

Frequency	2.5–2.7 GHz or 3.4–3.6 GHz
Output power	Max. 26 dBm at 2.5–2.7 GHz, Max. 24 dBm at 3.4–3.6 GHz (Europe)
Power consumption	3–6 W, depending on operating state
Bandwidth	Optional 5.0/7.0 or 10.0 MHz
Type of transmission	TDD
Modulation technique	SOFDMA 512/1024
Subcarrier modulation	QPSK, 16/64 QAM
Encoding rate	1/2, 2/3, 3/4, 5/6
Antenna socket	50 Ohm reverse SMA
Antenna type	2 internal antennae (2xRX, 1xTX) for MIMO Matrix A & B; Type DN1 (EN 302 326-3 V1.2.2) Optional: outdoor antenna
Antenna gain	2,6 GHz: 7 dBi 3,5 GHz: 9 dBi (integrated antennae)
Antenna polarisation	Send direction vertical, Receive direction vertical and horizontal

Wireless properties (WLAN)

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
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)
 Status (WiMAX, status, connection establishment)
 RDDI (WiMAX, signal strength)
 WLAN (activity, wireless)
 LAN1... LAN4 (connection to PC, activity, wired)
 USB (device connection)
 VoIP (connection, activity, Internet telephony)
 Phone1/Phone2 (FXS activity)

Compliance with security conditions and regulations

CE, EN60950

Software

Browser-based configuration environment
 NAT, PPPoE, PPPoA
 DHCP server and client, DynDNS
 NAT, virtual server, DMZ
 Security setup
 Firewall, prevention of hacker attacks
 MAC address filtering
 Log file
 WEP encryption
 WPA encryption
 WPA2 encryption
 WPS
 IEEE 802.1x
 Integrated SIP client

Appendix

Specifications for outdoor antenna (optional)

Model	outdoor antenna
Operating temperature	-40°C to +70°C
Storage temperature	-40°C to +70°C
Frequency	2.5–2.7 GHz or 3.4–3.6 GHz
Antenna socket	50 Ohm
Antenna gain	3,5 GHz: 18 dBi 3,5 GHz: 9 dBi 2,6 GHz: 9 dBi 2,6 GHz: 15 dBi
Antenna polarisation	Vertical, horizontal

Guarantee Certificate United Kingdom

Without prejudice to any claim the user (customer) may have in relation to the dealer or retailer, the customer shall be granted a manufacturer's Guarantee under the conditions set out below:

- ◆ In the case of new devices and their components exhibiting defects resulting from manufacturing and/or material faults within 24 months of purchase, Gigaset Communications GmbH shall, at its own option and free of charge, either replace the device with another device reflecting the current state of the art, or repair the said device. In respect of parts subject to wear and tear (including but not limited to, batteries, keypads, casing), this warranty shall be valid for six months from the date of purchase.
- ◆ This Guarantee shall be invalid if the device defect is attributable to improper treatment and/or failure to comply with information contained in the user guides.
- ◆ This Guarantee shall not apply to or extend to services performed by the authorised dealer or the customer themselves (e. g. installation, configuration, software downloads). User guides and any software supplied on a separate data medium shall be excluded from the Guarantee.
- ◆ The purchase receipt, together with the date of purchase, shall be required as evidence for invoking the Guarantee. Claims under the Guarantee must be submitted within two months of the Guarantee default becoming evident.
- ◆ Ownership of devices or components replaced by and returned to Gigaset Communications GmbH shall vest in Gigaset Communications GmbH.
- ◆ This Guarantee shall apply to new devices purchased in the European Union. For Products sold in the United Kingdom the Guarantee is issued by: Gigaset Communications GmbH, Schlavenhorst 66, D-46395 Bocholt, Germany.
- ◆ Any other claims resulting out of or in connection with the device shall be excluded from this Guarantee. Nothing in this Guarantee shall attempt to limit or exclude a Customers Statutory Rights, nor the manufacturer's liability for death or personal injury resulting from its negligence.
- ◆ The duration of the Guarantee shall not be extended by services rendered under the terms of the Guarantee.
- ◆ Insofar as no Guarantee default exists, Gigaset Communications GmbH reserves the right to charge the customer for replacement or repair.
- ◆ The above provisions does not imply a change in the burden of proof to the detriment of the customer.

To invoke this Guarantee, please contact the Gigaset Communications GmbH telephone service. The relevant number is to be found in the accompanying user guide.

Guarantee certificate Ireland

Without prejudice to any claim the user (customer) may have in relation to the dealer or retailer, the customer shall be granted a manufacturer's Guarantee under the conditions set out below:

Appendix

- ◆ In the case of new devices and their components exhibiting defects resulting from manufacturing and/or material faults within 24 months of purchase, Gigaset Communications GmbH shall, at its own option and free of charge, either replace the device with another device reflecting the current state of the art, or repair the said device. In respect of parts subject to wear and tear (including but not limited to, batteries, keypads, casing), this warranty shall be valid for six months from the date of purchase.
- ◆ This Guarantee shall be invalid if the device defect is attributable to improper care or use and/or failure to comply with information contained in the user manuals. In particular claims under the Guarantee cannot be made if:
 - ◆ The device is opened (this is classed as third party intervention)
 - ◆ Repairs or other work done by persons not authorised by Gigaset Communications GmbH.
 - ◆ Components on the printed circuit board are manipulated
 - ◆ The software is manipulated
 - ◆ Defects or damage caused by dropping, breaking, lightning or ingress of moisture. This also applies if defects or damage was caused by mechanical, chemical, radio interference or thermal factors (e.g.: microwave, sauna etc.)
 - ◆ Devices fitted with accessories not authorised by Gigaset Communications GmbH.
- ◆ This Guarantee shall not apply to or extend to services performed by the authorised dealer or the customer themselves (e.g. installation, configuration, software downloads). User manuals and any software supplied on a separate data medium shall be excluded from the Guarantee.
- ◆ The purchase receipt, together with the date of purchase, shall be required as evidence for invoking the Guarantee. Claims under the Guarantee must be submitted within two months of the Guarantee default becoming evident.
- ◆ Ownership of devices or components replaced by and returned to Gigaset Communications GmbH shall vest in Gigaset Communications GmbH.
- ◆ This Guarantee shall apply to new devices purchased in the European Union. For Products sold in the Republic of Ireland the Guarantee is issued by Gigaset Communications GmbH, Schlavenhorst 66, D-46395 Bocholt, Germany.
- ◆ Any other claims resulting out of or in connection with the device shall be excluded from this Guarantee. Nothing in this Guarantee shall attempt to limit or exclude a Customers Statutory Rights, nor the manufacturer's liability for death or personal injury resulting from its negligence.
- ◆ The duration of the Guarantee shall not be extended by services rendered under the terms of the Guarantee.
- ◆ Insofar as no Guarantee default exists, Gigaset Communications GmbH reserves the right to charge the customer for replacement or repair.
- ◆ The above provisions does not imply a change in the burden of proof to the detriment of the customer.

To invoke this Guarantee, please contact the Gigaset Communications GmbH helpdesk on 1850 777 277. This number is also to be found in the accompanying user guide.

Open Source Software used in the product

The product contains, among other things, embedded Open Source Software, licensed under an Open Source Software License and developed by third parties. These embedded Open Source Software files are protected by copyright. Your rights to use the Open Source Software beyond the mere execution of the program of Gigaset Communications GmbH are governed by the relevant Open Source Software license conditions.

Your compliance with those license conditions will entitle you to use the Open Source Software as foreseen in the relevant license. In the event of conflicts between Gigaset Communications GmbH license conditions and the Open Source Software license conditions, the Open Source Software conditions shall prevail with respect to the Open Source Software portions of the software. A list of the Open Source Software programs contained in this product and the Open Source Software licenses are available on the product CD.

If programs contained in this product are licensed under GNU General Public License (GPL), GNU Lesser General Public License (LGPL) or any other Open Source Software license that requires that source code be made available, and if this software is not already delivered in source code form together with the product, you can request the corresponding source code from Gigaset Communications GmbH by paying a 10 Euro fee for the physical act of transferring the copy. Please send your specific request, together with a receipt indicating the date of purchase, within three years of your purchase, together with the ID number (MAC ID) of the product and the software release number to the following address (please consult the user manual on how to find out these numbers):

Kleinteileversand Com Bocholt

Email: kleinteileversand.com@gigaset.com

Fax: +49 (0)2871 / 91 30 29

Warranty regarding further use of the Open Source Software

Gigaset Communications GmbH provides no warranty for the Open Source Software programs contained in this product, if such programs are used in any manner other than the program execution intended by Gigaset Communications GmbH. The licenses listed below define the warranty, if any, from the authors or licensors of the Open Source Software. Gigaset Communications GmbH specifically disclaims any warranties for defects caused by altering any Open Source Software program or the product's configuration. You have no warranty claims against Gigaset Communications GmbH in the event that the Open Source Software infringes the intellectual property rights of a third party. Technical support, if any, will only be provided for unmodified software.

Open Source Software Used

This product includes software developed by the University of California, Berkeley and its contributors.

Glossary

Access point

An access point, such as the Gigaset SX686 WiMAX, 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](#).

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](#). To avoid this, you can select the manual connect option on the Gigaset SX686 WiMAX.

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 cabling as with [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 SX686 WiMAX 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.

dB

Decibel (a tenth of a Bel)

Logarithmic unit of measurement for ratios between two currents, voltages, sound levels or powers. In order to depict large value differences clearly and graphically, these are given in dB; e.g. 60 dB corresponds to the factor 1000 relative to the voltage drops.

dBm

Decibel milliwatt

Power level in decibels relative to 1 milliwatt.

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 SX686 WiMAX 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

The Gigaset SX686 WiMAX 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.

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

Glossary

(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.

Downlink

Files that your Gigaset SX686 WiMAX receives and forwards to your local network.

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 SX686 WiMAX 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](#) or 1 Gbps.

File Server

See [Server](#)

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.

FTP (File Transfer Protocol)

FTP is a protocol for exchanging files on the Internet. You can use it, for example, to offer files for downloading or to receive files from other users.

Full duplex

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

See also: [Half duplex](#)

FXS

Foreign Exchange Station

Phone port to which an analogue terminal (phone, fax or answer machine) can be connected.

Glossary

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

Hypertext Transfer Protocol

Network protocol for the transmission of data, which is mainly used for transmitting and displaying Internet content.

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 or 5 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](#)).

IEEE 802.16

Standard defined by the [IEEE](#) for WiMAX. Similarly to other standards in the 802 series (e.g. 802.3 [Ethernet](#), 802.11 WLAN), the WiMAX standard is one of the standards for networks. The standard has progressed in accordance with new developments; there are currently two main versions:

- ◆ IEEE 802.16-2004: WiMAX, which specifies the secure location for connection partners.
- ◆ IEEE 802.16e-2005: Mobile WiMAX, which enables wireless cells to be exchanged during data transmission.

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](#) protocol stack. All participants on the Internet can be identified by an [IP address](#). Servers are addressed by [Domain names](#) (e.g. gigaset.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](#)).

Glossary

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](#) protocols (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 SX686 WiMAX has a [Private IP address](#) and a [Public IP address](#).

IPTV

Internet Protocol Television

You receive your provider's television service via the WiMAX connection. To do this, you require an IPTV-capable set-top box and the configuration data of your IPTV provider.

IPoA

IP over ATM

IP pool range

The Gigaset SX686 WiMAX'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 SX686 WiMAX you can set up a wired local [Ethernet](#) network and a wireless [IEEE 802.11g](#) standard network ([WLAN](#)).

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 should not 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 SX686 WiMAX as a [Virtual server](#).

Glossary

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](#).

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 SX686 WiMAX, have a public and a [Private IP 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 SX686 WiMAX 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.

Print server

See [Server](#)

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 SX686 WiMAX, 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 in relation to data formats, time frames and possibly troubleshooting. Communication between two applications requires different protocols at various levels, for example the [TCP/IP](#) protocols for the [Internet](#).

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](#).

Glossary

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](#), Web server, file server or print server.

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 signaling 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.

If the subnet mask is in a network that is administered by the Gigaset SX686 WiMAX, for example 255.255.255.0, that means the first three parts of the IP address form the network number and only the final part can be used for assigning host 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](#)

Glossary

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 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 SX686 WiMAX 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.

WAN

Wide Area Network

A WAN is a wide area network that is not restricted physically to a particular area, for example 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](#).

WDS

Wireless Distribution System

WDS describes the wireless connection between a number of access points.

Web server

See [Server](#)

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.

WiMAX

Worldwide Interoperability for Microwave Access

WiMAX is a modern wireless network technology that enables fast Internet connection even in remote areas where no other connection possibility (e. g. DSL) is available.

Glossary

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 SX686 WiMAX 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](#)).

WPS

Wi-Fi Protected Setup

WPS simplifies the setup of wireless networks.

WPS automatically sets up secure wireless networks. [Access points](#) (or clients with included registrar or external registrar) can automatically generate a network ID ([SSID](#)) and [WPA-PSK Encryption](#) if this was not performed previously. Clients can be connected either by entering a PIN or using special registration buttons on the access point and client.

Index

- Numerics
 - 10/100 Mbps switch port. 16
 - 128-bit encryption. 99
 - 128-bit key 64, 98
 - 64-bit key 64, 98
- A
 - Access control 66, 78, 101
 - local area network 101
 - Access point 21, 91, 180
 - Address block for
 - IP addresses 89
 - Ad-hoc mode. 21, 180
 - Ad-hoc network. 21
 - Advanced Settings
 - features 69
 - Advanced setup. 43
 - AES 63, 180
 - Alarm display. 144
 - Alarms. 143
 - functional 144
 - physical 146
 - reset. 144
 - Antenna 29
 - choose 47
 - integrated 30
 - outdoor antenna 31
 - Anti-DoS firewall 77
 - Area code
 - Internet telephony 113
 - ASCII key 65, 99
 - Attack detection 77
 - Authentication server 96
 - Auto connect. 180
- B
 - Backing up configuration data 133
 - Backup 133
 - Bandwidth for VoIP 106
 - Base station see Access point
 - Baseline. 12, 167
 - Basic settings. 43
 - configuration. 46
 - summary 58
- Bridge 180
- Broadcast. 92, 180
- Browser 41
- BSSID 181
- Buttons 45
- C
 - Call forwarding 112
 - Call waiting 112
 - Calling line identification restriction . 112
 - Care 7
 - Cleaning 7
 - Client. 181
 - CLIR 112
 - Command
 - net share 164
 - Computerbrowser 164
 - Configuration
 - resetting to factory setting 134
 - restoring. 134
 - security. 59
 - Configuration file. 133
 - Configuring popup blocker. 173
 - Confirmation tone
 - negative 129
 - positive 129
 - Connecting
 - outdoor antenna. 33
 - Connection mode. 73
 - Connection on request. 73
 - Connection service
 - priority 71
 - VLAN tag 71, 73
 - Connectors. 16
 - Country settings. 130
- D
 - Data encryption 98
 - dBm. 181
 - Deactivating the HTTP proxy. 173
 - DHCP 181
 - DHCP server 89, 181
 - Dialling plans 113
 - Displaying the operating state . . . 14, 39

Index

- Disposal 8
- Disposal (Switzerland) 7
- DMZ 18, 181
- DNS 182
- DNS server 182
 - defining 75
- Domain name 182
- Domain Name Service see DNS
- DoS attack 77, 182
- Downlink 182
- Dynamic DNS see DynDNS
- Dynamic Host Configuration Protocol,
see DHCP
- Dynamic IP address 182
- DynDNS 85, 183
- DynDNS service, see DynDNS
- DynDNS.org 85, 86

- E**
- ECO 12
- Encryption 94, 98, 183
 - WEP 64
 - WPA 63
- Ethernet 17, 20, 21, 183
 - transmission speed 17
- Ethernet network
 - linking with a wireless network . . . 23
- Exposed host 84
- Extending wireless coverage 24
- Extensions 109

- F**
- Features 17
- File and Printer Sharing 162
- File server 117
 - partition list 118
 - sharing directories 118
- Firewall 18, 183
 - activating/deactivating 76
 - attack detection 77
 - configuring 76
 - security level 77
 - Windows 165
- Flat rate 183
- Full duplex 183
- Functional Alarms 144
- FXS 183

- G**
- Games on the Internet 81
- Gateway 184
- Gigaset SX68x WiMAX
 - configuring 41
 - connectors 16
 - default settings 32
 - Ethernet network setup 20
 - installation 32
 - IP address 41
 - password protected 60
 - possibilities for network setup 19
 - setting up 29
- Global IP address see Public IP address
- GNU General Public License 179
- GNU Lesser General Public License . . 179
- GPL 179
- Guarantee Certificate 177, 178

- H**
- Hacker attack 18
- Hacker attacks 182
- Hacker protection 77
- Half duplex 184
- Help 45
- Hexadecimal key 65, 99
- HTTP 184
- HTTP proxy 184
- Hub 184

- I**
- Idle time 132
- IEEE 184
- IEEE 802.1 Q 71, 73
- IEEE 802.11 184
- IEEE 802.16 185
- Infrastructure mode 21, 185
- Installation 32
- Installing printer driver
 - Windows XP/2000 160
- Institute of Electrical and Electronic
Engineers see IEEE
- Inter Process Communication see IPC
- Internet 70, 185, 186
 - connection mode 73
 - connection on request 73
 - manual connection 73

- menu 70
- service provider 72
- setting up access control 78
- setting up multiple connection
 - services 71
- Internet access 12
- Internet connection
 - changing configuration 72
 - closing manually 44
 - disconnecting automatically 73
 - opening manually 44
 - setting up 72
- Internet Explorer 28, 41
- Internet protocol 162
- Internet protocol see IP protocol
- Internet service provider . . . 72, 185, 186
- Internet telephony 12, 25
 - analogue phone 105
 - dialling plans 113
 - quick dial 115
 - setting up 105
 - VoIP settings 106
- Internet time 131
- IP address 88, 186
 - address block 89
 - assigning automatically 88
 - assigning static 89, 90
 - dynamic 182
 - Gigaset SX68x WiMAX 41
 - private 189
 - public 188
 - static 191
- IP address block for DHCP 89
- IP address pool 186
- IP protocol 186
- IPC 164
- IPoA 186
- IPTV 186
- ISP see Internet service provider

- K**
- Key length 64
 - 128 bit (ASCII) 65, 99
 - 64 bit (ASCII) 65, 99
 - 64 bit (hexadecimal) 65, 99
- Key type 65

- L**
- LAN 23, 187
 - configuration 88
- LAN port 16
- Lease time 89
- LED
 - behaviour after initial connection . . 39
 - WPS registration 37
- LED displays 39
- LGPL 179
- Local area network see LAN
- Local IP address see
 - Private IP address
- Login screen 41

- M**
- MAC access control list 66, 101
- MAC address 187
- MAC address filter 66
- MAC Encapsulated Routing
 - see MER
- MAC table 66
- Mains adapter
 - port 16
- Manual connection 73
- Maximum Receive Unit see MRU
- Maximum Transmission Unit see MTU
- Mbps 187
- MER 187
- Mobile network 21
- Mozilla Firefox 28, 41
- MRU 187
- MTU 187

- N**
- NAT 80, 187
 - port forwarding 80
 - port triggering 80
- Negative confirmation tone 129
- Network 188
 - ad-hoc 21
 - infrastructure 21
 - wired 20
 - wireless 21
- Network adapter 188
 - Ethernet 20
 - wireless 21

Index

- Network Address Translation . . . 80, 187
- Network component
 - mobile 21
- Network printer 147
- network share 164
- New encryption 95

- O
- Open Source Software 179
- outdoor antenna 31

- P
- Passphrase 65
- Password 41, 60
 - assigning 60
 - changing 60
 - forgotten 60
- Permanent Virtual Circuit see PVC
- Phone
 - analogue 25, 105
- Phone port 16
 - splitter 16
- Phonewords 115
- Physical alarms 146
- Picking up call 112
- PIN 27
- Point-to-Point Protocol over ATM
 - see PPPoA
- Point-to-Point Protocol over Ethernet
 - see PPPoE
- Popup blocker 173
- Port 188
 - for mains adapter 16
 - LAN 16
 - public port 80, 82
 - trigger port 80, 82
- Port forwarding 80, 188
 - setting up 83
- Port number 84, 188
 - illustration 83
- Port triggering 80, 81
 - setting up 82
- Positive confirmation tone 129
- PPPoE 189
- PPPoE pass-through 55, 73
- Print server 123

- Printer
 - connecting 161
 - on the USB port 116
- Printer interface
 - configuring 147
- Printer port (TCP/IP), installing
 - later installation 160
- Printer port installing
 - Windows Vista 148
 - Windows XP/2000 154
- Printer wizard 149, 155
- Private IP address 189
- Problem solving 167
- Protocol 189
- Public IP address 188
- PVC 189

- Q
- Quality of service (QoS) 189
- Quick dial 115
- Quick dial numbers 115

- R
- Radio network 194
 - infrastructure mode 21
- Radio settings 91
- Radio status 138
- RADIUS server 96
- Reboot 16, 134
- Reboot function 16
- Regional settings 53
- Rekeying 63
- Remote management 133, 189
- Removing hardware safely 117
- Repeater 24, 103
- Reset button 16
- Reset function 16
- Resetting 134
- Roaming 190
- Router 190
 - dynamic IP address 85
 - IP address 88
 - setting up a local area network 19

- S
- Safety 7
 - disposal (Switzerland) 7

- Safety precautions 7
 - Security
 - disposal 8
 - safety precautions 7
 - Security architecture, WEP 98
 - Security functions 26
 - Security measures 18
 - Security settings 43, 59
 - saving 68
 - Server 190
 - virtual 193
 - Service Set Identifier see SSID
 - Session Initiation Protocol see SIP
 - Setting up 29
 - Signal strength
 - WiMAX 52
 - Simple Mail Transfer Protocol see SMTP
 - Simple Network Management Protocol
 - see SNMP
 - SIP 190
 - SIP client 110
 - SIP proxy server 110
 - SIP user accounts 111
 - SMTP 190
 - SNMP 191
 - Software release 12, 167
 - Specifications 174
 - SPI (Stateful Packet Inspection),
 - see SPI
 - SSID 26, 37, 61, 191
 - changing 61
 - concealed 92
 - visible 61, 92
 - SSID broadcast 61, 92
 - Start screen 42
 - Static IP address 191
 - Status
 - Alarms 143
 - device 142
 - local area network 140
 - overview 136
 - radio 138
 - security 137
 - telephony 142
 - wireless network 141
 - Status information 136
 - Subnet 191
 - Subnet mask 191
 - Super G 191
 - Switch 191
 - System log 135
 - System password
 - assigning 131
 - changing 131
 - System requirements 28
 - System time 131
- T**
- TCP 192
 - TCP/IP 192
 - TCP/IP port for printer 160
 - Telephone ports 110
 - Telephony
 - basic settings 56
 - call answering and forwarding . . . 126
 - call forwarding 112
 - call waiting 125
 - calling line identification
 - restriction 112, 125
 - conference call 126
 - consultation 125
 - exchange settings 128
 - extensions 109
 - function keys 124
 - important information 105
 - internal call 124
 - internal phone number 111
 - tooggling 125
 - VoIP account 56
 - Time server 131
 - Trademarks 7
 - Transmission Control Protocol see TCP
 - Transmission mode 92
 - Transmission rate
 - upstream 106
 - Transmission speed 187
 - in the Ethernet LAN 17
 - in wireless LAN 17
 - Trigger port 80
 - Troubleshooting 167
- U**
- UDP 192
 - Universal Plug and Play see UPnP

Index

- Universal Resource Locator see URL
- UPnP 55, 74, 192
 - enabling 74
- URL 192
- USB 116
 - file server 117
 - print server 123
 - Web server 120
- USB data carrier 116
- USB port 116
- User Datagram Protocol see UDP
- User interface
 - buttons 45
 - elements 45
 - Help 45
 - idle time 132
 - logout 45
 - starting 41
- V
- Vanity 115
- VCI 192
- Virtual Channel Identifier see VCI
- Virtual Path Identifier see VPI
- Virtual server 18, 81, 193
- VLAN tag 71, 73
- Voice over IP see Internet telephony
- VoIP account 56
- VoIP bandwidth 106
- VoIP see Internet telephony
- Volume, change for telephone calls . 107
- VPI 193
- W
- WAN 193
- WDS 103
- Web server 120
 - FTP 122
 - HTTP service 121
- WEP 62, 64, 94, 95, 98, 193
 - encryption mode 99
 - hexadecimal 65
 - key length 64, 99
 - passphrase 65
- Wide Area Network see WAN
- Wi-Fi Protected Setup see WPS
- WiMAX 193
- WiMAX antenna
 - align 48
 - choose 47
 - fine tuning 52
- WiMAX interface 22
- WiMAX network
 - search 49
- Windows firewall 165
- Wired Equivalent Privacy see WEP
- Wired network 20
- Wireless cell 194
- Wireless LAN see WLAN
- Wireless network
 - access control 66
 - ad-hoc mode 21
 - name 26
- WLAN 21, 23, 194
 - external antenna 16
 - operating modes 21
 - Switch off 16
 - Switch on 16
 - transmission speed 17
- WLAN adapter 21
- WPA 63, 194
 - AES 63
 - pre-installed key
 - pre-shared key 194
- WPA2-PSK 62, 96
- WPA-PSK 63, 96
- WPA-PSK, see WPA, pre-installed key
- WPS 26, 57, 59, 93
 - LED display during registration 37
 - registration 93
 - registration via button 26
 - registration with PIN 27
- WPS registration
 - via own PIN 94
 - via PIN of the partner device 94
 - via push button 93

Issued by
Gigaset Communications GmbH
Schlavenhorst 66, D-46395 Bocholt
Gigaset Communications GmbH is a trademark licensee of Siemens AG.

© Gigaset Communications GmbH 2008
All rights reserved. Subject to availability.
Rights of modification reserved.

www.gigaset.com
A31008-N919-R101-3x-7619

v 2.0
10.2008