

EN	Dear Customer, Gigaset Communications GmbH is the legal successor to Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), which in turn continued the Gigaset business of Siemens AG. Any statements made by Siemens AG or SHC that are found in the user guides should therefore be understood as statements of Gigaset Communications GmbH. We hope you enjoy your Gigaset.	DA	Kære Kunde, Gigaset Communications GmbH er retlig efterfølger til Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), som fra deres side videreførte Siemens AGs Gigaset-forretninger. Siemens AGs eller SHCs eventuelle forklaringer i betjeningsvejledningerne skal derfor forstås som Gigaset Communications GmbHs forklaringer. Vi håber, du får meget glæde af din Gigaset.
DE	Sehr geehrte Kundin, sehr geehrter Kunde, die Gigaset Communications GmbH ist Rechtsnachfolgerin der Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), die ihrerseits das Gigaset-Geschäft der Siemens AG fortführte. Etwaige Erklärungen der Siemens AG oder der SHC in den Bedienungsanleitungen sind daher als Erklärungen der Gigaset Communications GmbH zu verstehen. Wir wünschen Ihnen viel Freude mit Ihrem Gigaset.	FI	Arvoisa asiakkaamme, Gigaset Communications GmbH on Siemens Home and Office Communication Devices GmbH & Co. KG (SHC)-yhtiöksen oikeudenomistaja, joka jatkoj puolestaan Siemens AG:n Gigaset-liiketoimintaa. Käyttöoppaissa mahdollisesti esiintyvät Siemens AG:n tai SHC:n selosteet on tämän vuoksi ymmärrettävä Gigaset Communications GmbH:n selosteina. Toivotamme Teille paljon iloa Gigaset-laitteestanne.
FR	Chère Cliente, Cher Client, la société Gigaset Communications GmbH succède en droit à Siemens Home and Office Communication Devices GmbH & Co. KG (SHC) qui poursuivait elle-même les activités Gigaset de Siemens AG. Donc les éventuelles explications de Siemens AG ou de SHC figurant dans les modes d'emploi doivent être comprises comme des explications de Gigaset Communications GmbH. Nous vous souhaitons beaucoup d'agrément avec votre Gigaset.	SV	Kära kund, Gigaset Communications GmbH övertar rättigheterna från Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), som bedrev Gigaset-verksamheten efter Siemens AG. Alla förklaringar från Siemens AG eller SHC i användarhandboken gäller därför som förklaringar från Gigaset Communications GmbH. Vi önskar dig mycket nöje med din Gigaset.
IT	Gentile cliente, la Gigaset Communications GmbH è successore della Siemens Home and Office Communication Devices GmbH & Co. KG (SHC) che a sua volta ha proseguito l'attività della Siemens AG. Eventuali dichiarazioni della Siemens AG o della SHC nei manuali d'istruzione, vanno pertanto intese come dichiarazioni della Gigaset Communications GmbH. Le auguriamo tanta soddisfazione con il vostro Gigaset.	NO	Kjære kunde, Gigaset Communications GmbH er rettslig etterfølger etter Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), som i sin tur videreførte Gigaset-geskjeften i Siemens AG. Eventuelle meddelelser fra Siemens AG eller SHC i bruksanvisningene er derfor å forstå som meddelelser fra Gigaset Communications GmbH. Vi håper du får stor glede av din Gigaset-enhet.
NL	Geachte klant, Gigaset Communications GmbH is de rechtsopvolger van Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), de onderneming die de Gigaset-activiteiten van Siemens AG heeft overgenomen. Eventuele uitspraken of mededelingen van Siemens AG of SHC in de gebruiksaanwijzingen dienen daarom als mededelingen van Gigaset Communications GmbH te worden gezien. Wij wensen u veel plezier met uw Gigaset.	EL	Αγαπητή πελάτισσα, αγαπητέ πελάτη, η Gigaset Communications GmbH είναι η νομική διάδοχος της Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), η οποία έχει αναλάβει την εμπορική δραστηριότητα Gigaset της Siemens AG. Οι δηλώσεις της Siemens AG ή της SHC στις οδηγίες χρήσης αποτελούν επομένως δηλώσεις της Gigaset Communications GmbH. Σας ευχόμαστε καλή διασκέδαση με τη συσκευή σας Gigaset.
ES	Estimado cliente, la Gigaset Communications GmbH es derechohabiente de la Siemens Home and Office Communication Devices GmbH & Co. KG (SHC) que por su parte continuó el negocio Gigaset de la Siemens AG. Las posibles declaraciones de la Siemens AG o de la SHC en las instrucciones de uso se deben entender por lo tanto como declaraciones de la Gigaset Communications GmbH. Le deseamos que disfrute con su Gigaset.	HR	Poštovani korisnici, Gigaset Communications GmbH pravni je sljednik tvrtke Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), koji je nastavio Gigaset poslovanje tvrtke Siemens AG. Zato sve izjave tvrtke Siemens AG ili SHC koje se nalaze u uputama za upotrebu treba tumačiti kao izjave tvrtke Gigaset Communications GmbH. Nadamo se da sa zadovoljstvom koristite svoj Gigaset uređaj.
PT	SCaros clientes, Gigaset Communications GmbH é a sucessora legal da Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), que, por sua vez, deu continuidade ao sector de negócios Gigaset, da Siemens AG. Quaisquer declarações por parte da Siemens AG ou da SHC encontradas nos manuais de utilização deverão, portanto, ser consideradas como declarações da Gigaset Communications GmbH. Desejamos que tenham bons momentos com o seu Gigaset.	SL	Spoštovani kupec! Podjetje Gigaset Communications GmbH je pravni naslednik podjetja Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), ki nadaljuje dejavnost znamke Gigaset podjetja Siemens AG. Vse izjave podjetja Siemens AG ali SHC v priložnikih za uporabnike torej veljajo kot izjave podjetja Gigaset Communications GmbH. Želimo vam veliko užitkov ob uporabi naprave Gigaset.

- CS** Vážení zákazníci,
společnost Gigaset Communications GmbH je právním nástupcem společnosti Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), která dále přejala segment produktů Gigaset společnosti Siemens AG. Jakékoli prohlášení společnosti Siemens AG nebo SHC, které naleznete v uživatelských příručkách, je třeba považovat za prohlášení společnosti Gigaset Communications GmbH. Doufáme, že jste s produkty Gigaset spokojeni.
- SK** Vážený zákazník,
Spoločnosť Gigaset Communications GmbH je právnym nástupcom spoločnosti Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), ktorá zasa pokračovala v činnosti divízie Gigaset spoločnosti Siemens AG. Z tohto dôvodu je potrebné všetky vyhlásenia spoločnosti Siemens AG alebo SHC, ktoré sa nachádzajú v používateľských príručkách, chápať ako vyhlásenia spoločnosti Gigaset Communications GmbH. Veríme, že budete so zariadením Gigaset spokojní.
- RO** Stimatе client,
Gigaset Communications GmbH este succesorul legal al companiei Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), care, la rândul său, a continuat activitatea companiei Gigaset a Siemens AG. Orice afirmații efectuate de Siemens AG sau SHC și incluse în ghidurile de utilizare vor fi, prin urmare, considerate a aparține Gigaset Communications GmbH.
Sperăm ca produsele Gigaset să fie la înălțimea dorințelor dvs.
- SR** Poštovani potrošaču,
Gigaset Communications GmbH je pravni naslednik kompanije Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), kroz koju je nastavljeno poslovanje kompanije Gigaset kao dela Siemens AG. Stoga sve izjave od strane Siemens AG ili SHC koje se mogu naći u korisničkim uputstvima treba tumačiti kao izjave kompanije Gigaset Communications GmbH.
Nadamo se da ćete uživati u korišćenju svog Gigaset uređaja.
- BG** Уважаеми потребители,
Gigaset Communications GmbH е правоприемникът на Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), която на свой ред продължи бизнеса на подразделението Siemens AG. По тази причина всякакви изложения, направени от Siemens AG или SHC, които се намират в ръководствата за потребителя, следва да се разбират като изложения на Gigaset Communications GmbH.
Надяваме се да ползвате с удоволствие вашия Gigaset.
- HU** Tisztelt Vásárló!
A Siemens Home and Communication Devices GmbH & Co. KG (SHC) törvényes jogutódja a Gigaset Communications GmbH, amely a Siemens AG Gigaset üzletágának utódja. Ebből következően a Siemens AG vagy az SHC felhasználói kézikönyveiben található bármely kijelentést a Gigaset Communications GmbH kijelentésének kell tekinteni.
Reméljük, megelégedéssel használja Gigaset készülékét.
- PL** Szanowny Kliencie,
Firma Gigaset Communications GmbH jest spadkobiercą prawnym firmy Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), która z kolei przejęła segment produktów Gigaset od firmy Siemens AG. Wszelkie oświadczenia firm Siemens AG i SHC, które można znaleźć w instrukcjach obsługi, należy traktować jako oświadczenia firmy Gigaset Communications GmbH.
Życzymy wiele przyjemności z korzystania z produktów Gigaset.
- TR** Sayın Müşterimiz,
Gigaset Communications GmbH, Siemens AG'nin Gigaset işletmesini yürüten Siemens Home and Office Communication Devices GmbH & Co. KG (SHC)'nin yasal halefidir. Kullanma kılavuzlarında bulunan ve Siemens AG veya SHC tarafından yapılan bildiriler Gigaset Communications GmbH tarafından yapılmış bildiriler olarak algılanmalıdır.
Gigaset'ten memnun kalmanızı ümit ediyoruz.
- RU** Уважаемые покупатель!
Компания Gigaset Communications GmbH является правопреемником компании Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), которая, в свою очередь, приняла подразделение Gigaset в свое управление от компании Siemens AG. Поэтому любые заявления, сделанные от имени компании Siemens AG или SHC и встречающиеся в руководствах пользователя, должны восприниматься как заявления компании Gigaset Communications GmbH.
Мы надеемся, что продукты Gigaset удовлетворяют вашим требованиям.

SIEMENS



Gigaset

SE361 WLAN



Contents

Safety precautions	6
The Gigaset SE361 WLAN	7
Local networks with Gigaset products	8
Wired local area network (Ethernet)	9
Wireless local area network (WLAN)	10
Linking a wireless network (WLAN) to an Ethernet (LAN)	12
Features and applications	13
Procedure for installation and configuration	15
First Steps	16
Pack contents	16
System requirements	16
Operating displays and connections	17
Front panel	17
Back panel	18
Setting up the Gigaset SE361 WLAN	19
Connecting the Gigaset SE361 WLAN	20
Making the connection to the DSL or cable modem	20
Making the connection to the PC	21
Connecting to the mains power supply	23
The user interface	24
Launching the user interface	24
The start screen	25
Selecting a language	26
Elements on the user interface	27
Basic Setup Wizard	28
Regional Options	28
Configuring Internet connection	29
Summary	31
Security Setup Wizard	32
Assigning a Password	32
SSID	33
Setting security functions for the wireless network	34
WPA2 / WPA with Pre-shared key (PSK)	34
WEP encryption	35
Access control within the wireless network	38
Saving settings	39

- Configuring the Advanced Settings 40**
- Configuring the Internet connection 41
 - Internet 41
 - Internet Connection 41
 - DNS servers 44
 - MAC address 44
- Firewall 45
 - Setting up access control to the Internet 46
- Setting up the NAT function 47
 - Port triggering 49
 - Port forwarding 50
 - Opening the firewall for a selected PC (Exposed Host) 51
 - Dynamic DNS 52
- QoS (Quality of Service) 53
- LAN configuration 54
 - Assigning static IP addresses to individual PCs 55
- Configuration for wireless connections 56
 - Setting wireless security 58
 - WPA2-PSK and WPA2-PSK / WPA-PSK 58
 - WEP encryption 59
 - Allowed clients 61
 - Repeater function (WDS) 62
- Administration and status information 64**
- Connecting to the Internet manually 64
- Regional Options 65
 - Internet Time 66
- System Password 66
- Setting up Remote Management 67
- Saving and restoring a configuration 68
 - Saving configuration data 68
 - Restoring backups 69
 - Resetting to the factory settings 69
- Reboot 69
- Updating the firmware 69
- Status information 71**
- Overview 71
- Security 72
- Internet 73
- Local Network 74
- Wireless Network 74
- Device 75

Configuring the local network	76
Network configuration with Windows XP	76
Configuring the network	77
Selecting a computer name and workgroup	79
Checking the network settings and completing the installation procedure	79
TCP/IP settings	80
Deactivating the HTTP proxy	82
Configuring the popup blocker	82
Synchronising the TCP/IP settings with the Gigaset SE361 WLAN	83
Network configuration with Windows 2000	84
Installing network services	84
Selecting a computer name and workgroup	85
Installing the TCP/IP protocol	86
TCP/IP settings	88
Deactivating the HTTP proxy	90
Configuring the popup blocker	90
Synchronising the TCP/IP settings with the Gigaset SE361 WLAN	91
Checking the connection to the Gigaset SE361 WLAN	92
 Appendix	 93
Troubleshooting	93
Specifications	97
Authorisation	98
Approval	98
Customer service (Customer Care)	99
Guarantee Certificate United Kingdom	100
Guarantee Certificate Ireland	100
 Glossary	 102
 Index	 114

Safety precautions

- ◆ Only use the power supply unit supplied with your device. Comply with the connection values and ratings when connecting the device to the mains power supply.
- ◆ Protect the device from damp.
- ◆ Never open the device. For reasons of electrical safety, it may only be opened by authorised service technicians.
- ◆ The device may affect medical equipment. Take account of the technical conditions in the relevant environment.
- ◆ Make sure you include the user guide when you pass on your device to somebody else.
- ◆ Do not use the device in or near rooms containing gas or explosive materials.

Trademarks

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

Mozilla Firefox is a registered trademark of the Mozilla Organization.

The Gigaset SE361 WLAN

Your Siemens Gigaset SE361 WLAN is a powerful but easy-to-use device that connects your PC (WLAN) or your local network (LAN) to the Internet without the need for wires (via a DSL or cable modem).

You can connect your PC wirelessly to the Gigaset SE361 WLAN and create a wireless local network (WLAN). For network security, wireless transmission can be encrypted using the WPA standard or 64/128-bit WEP.

The Gigaset SE361 WLAN allows several users to access the Internet simultaneously. A single user account can be shared, if your Internet Provider permits this. If you want to surf the Internet at the lowest possible cost, then the Gigaset SE361 WLAN is a convenient and effective solution.

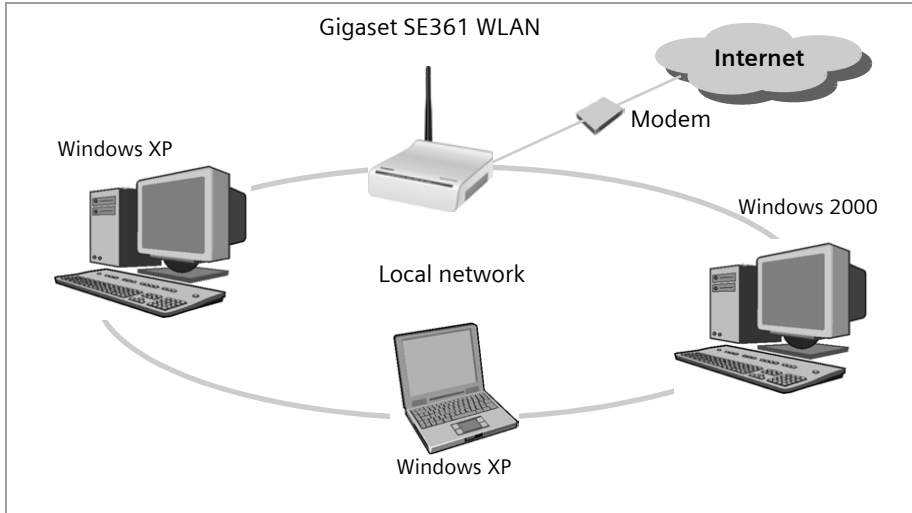
You can connect a DSL or cable modem to the WAN interface of your Gigaset SE361 WLAN.

Despite its extensive range of functions, the Gigaset SE361 WLAN is easy for both experts and non experts to handle. It can be configured and made operational within a few minutes.



Local networks with Gigaset products

You can use the Gigaset SE361 WLAN to set up a local area network, e.g. a home network. All the PCs in this network can communicate with each other and have access to the Internet.



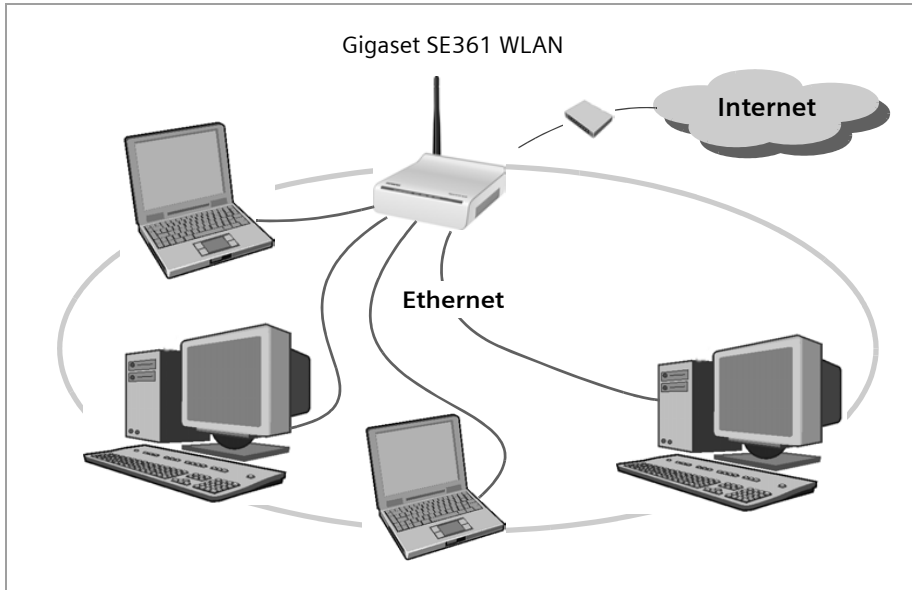
There are various ways in which you can set up the network with a Gigaset SE361 WLAN. You can

- ◆ set up a wired local area network ([Ethernet](#)) and allow the connected PCs access to the Internet (see page 9).
- ◆ set up a wireless local network ([WLAN](#)) and allow the connected PCs access to the Internet (see page 10).
- ◆ set up a local network comprising wireless and wired network components (see page 12).

Wired local area network (Ethernet)

In a wired local area network, PCs communicate with one another via an Ethernet cable. The Gigaset SE361 WLAN establishes the connection between the PCs, which you can connect to the four Ethernet LAN ports. The PCs must be equipped with a network socket (Ethernet). New PCs frequently already have this socket. For older PCs you will need to install an Ethernet network card. An Ethernet cable (CAT5) is used to connect the PC to the Ethernet LAN socket on the Gigaset SE361 WLAN. One cable is supplied with the device; you can obtain additional Ethernet cables from your retailer.

The Gigaset SE361 WLAN 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. For this the PCs have to be equipped with a wireless network adapter (WLAN adapter) such as a Gigaset USB Stick 54 or you can use a PC with a wireless option built in.

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, the infrastructure mode needs an access point such as the Gigaset SE361 WLAN. In infrastructure mode the stations in the network always communicate via this access point. Each station that wants to be part of a wireless network must first be registered 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. 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 SE361 WLAN to connect

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

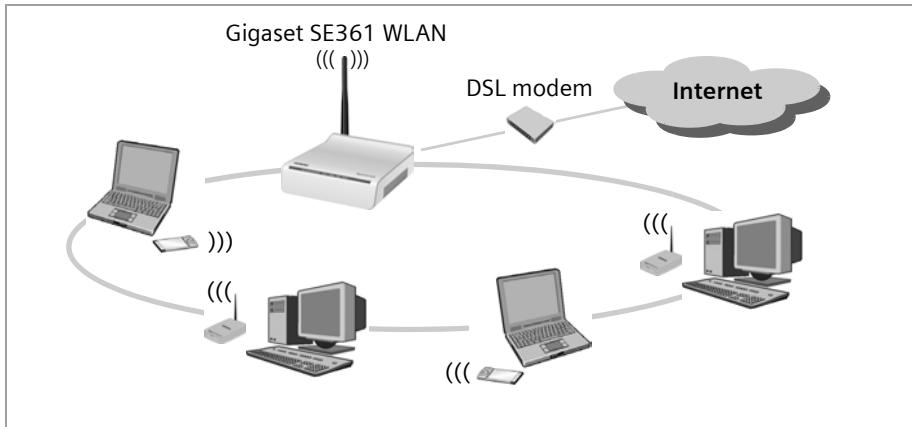
Infrastructure mode is the default configuration of the Gigaset SE361 WLAN. This configuration is described in the quick guide that comes with the device.

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 without any existing network infrastructure, and where participants are on the move.

Linking wireless networks with the Internet

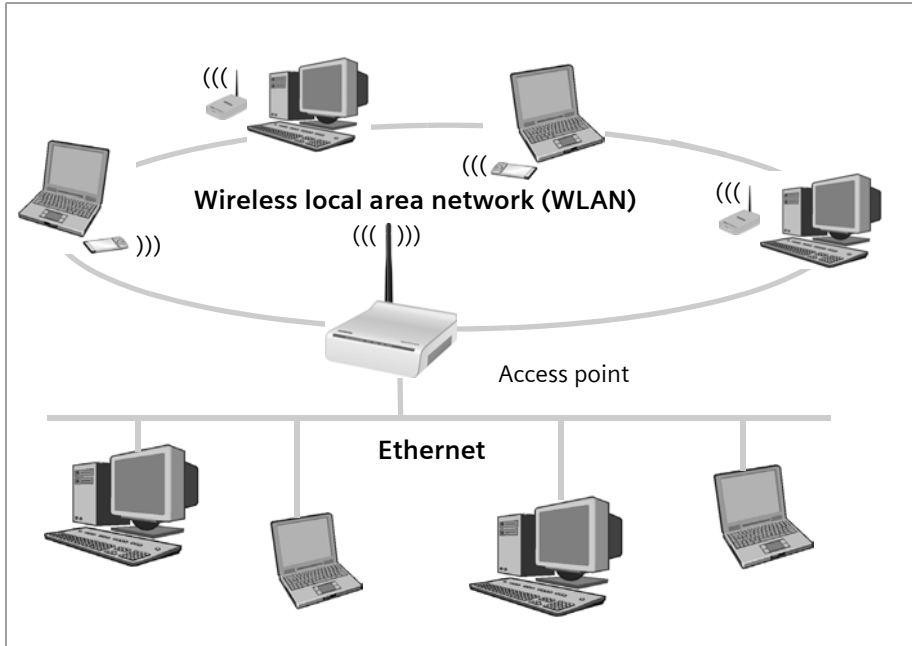
The Gigaset SE361 WLAN has a **WAN** port that permits all stations within its local area network to access the Internet simultaneously. To be able to use this functionality you need a DSL or cable connection and a suitable modem. You can usually obtain the line and a modem from an Internet service provider.



This illustration shows the commonest method of application. One or more PCs communicate wirelessly with the Gigaset SE361 WLAN in infrastructure mode. The Gigaset SE361 WLAN forwards the data to the Internet via a DSL or cable modem. Data from the Internet flows back to the PC along the same route.

Linking a wireless network (WLAN) to an Ethernet (LAN)

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 all the mobile stations into a wireless network in infrastructure mode.



The Gigaset SE361 WLAN 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 SE361 WLAN.

Note:

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. It is therefore not possible for us to provide a general example for this use; configuration must be defined separately for each individual case. We advise having such networks configured by a specialist.

Features and applications

The Gigaset SE361 WLAN's wide range of features make it ideal for a large number of applications, e.g.:

◆ Internet access

The Gigaset SE361 WLAN gives several users access to the Internet when a DSL or cable modem is connected.

- As many DSL providers set up Internet access via the [PPPoE](#) protocol, the Gigaset SE361 WLAN contains an integrated PPPoE [Client](#), which means you no longer need to set up this service on your PC yourself.

– Shared Internet access

If your Internet provider permits this, the Gigaset SE361 WLAN supports Internet access for up to 252 users. In practice, multiple users in your network can surf the Internet simultaneously using just one Internet access.

◆ Setting up a local network

The Gigaset SE361 WLAN permits connections

- for four devices via [Ethernet](#) ports with a transmission speed of 10 or 100 [Mbps](#) (with automatic recognition).
- for up to 32 mobile terminals via a radio interface with a transmission speed of up to 54 Mbps. It complies with the [IEEE 802.11g](#) standard and can work with all products that satisfy the IEEE 802.11g or 802.11b standard.

Using a Gigaset SE361 WLAN 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, e.g. a file server or printer.

◆ Security functions

The Gigaset SE361 WLAN 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 SE361 WLAN for their Internet connections, which makes them 'invisible' on the Internet. The Gigaset SE361 WLAN only allows access from the Internet if this has been requested from within the local area network.

With the firewall the Gigaset SE361 WLAN also offers comprehensive protection against hacker attacks.

- Service filtering and URL filtering

The Gigaset SE361 WLAN can filter Internet access. Here you determine which PCs may access which Internet services.

In addition, you can deactivate access to certain Internet domains and sites (URL filtering).

- Access control and encryption for the local wireless network

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

The Gigaset SE361 WLAN

- The sending power can be adjusted to suit local conditions. If you limit the reach of your wireless network to the size you need, you also make electronic eavesdropping more difficult.
- ◆ Other options
 - [Exposed Host](#)
You can set up a PC on your local network to be a virtual server and release it for unrestricted access from the Internet.
 - Port forwarding
You can release individual services on a PC that is integrated into the network.

Procedure for installation and configuration

1. If your PC does not dispose of an integrated LAN or WLAN interface, first install an Ethernet network card or a wireless [Network adapter](#) such as the Gigaset USB Stick 54 in the PCs you want to connect to the Gigaset SE361 WLAN. The installation process is described in the user guides for these products.

Note:

When installing wireless network adapters: The default [SSID](#) for the Gigaset SE361 WLAN is **ConnectionPoint**.

2. Make the necessary connections (PCs, modem) to the Gigaset SE361 WLAN and switch the device on (see the section entitled "Connecting the Gigaset SE361 WLAN" on page 20).
3. Before the PCs can communicate with the Gigaset SE361 WLAN and with each other in a local network, you must change their network settings. This will normally be the case if you are using the Windows default settings. To find out how to do this, read the section entitled "Configuring the local network" on page 76. First connect just **one** PC to the Gigaset SE361 WLAN. You can then carry out the basic configuration. After that you can connect further PCs.

In a wireless connection you establish the link from the PC's wireless network adapter to the Gigaset SE361 WLAN. This is described in the user guide for the network adapter.

4. Configure the Gigaset SE361 WLAN to activate the device's Internet access (refer to the section entitled "Basic Setup Wizard" on page 28). To do this you will require access data from your Internet service provider.

If you want to use the Gigaset SE361 WLAN's other functions, e.g. the comprehensive security features, use the router's Security Setup (see page 32) or the **Advanced settings** menu(see page 40).

First Steps

Pack contents

The package contains the following items:

- ◆ one Gigaset SE361 WLAN,
- ◆ one mains adapter (230V / 12V 0.5A DC),
- ◆ one cable with RJ45 jacks (CAT5),
- ◆ one CD with a detailed user guide and software for language selection
- ◆ one Quick Start Guide

System requirements

To operate your Gigaset SE361 WLAN you need:

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

Notes:

The maximum data transfer rate for 802.11g-compatible network adapters is 54 Mbps, and for 802.11b-compatible network adapters 11 Mbps.

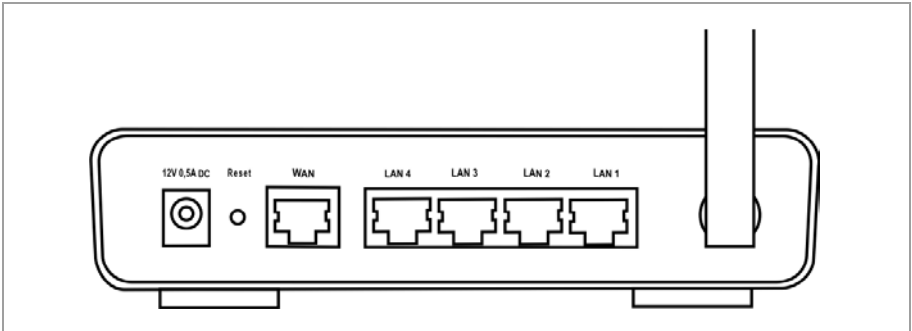
or

- an [Ethernet](#) connection,
- ◆ a Web browser for configuration of your Gigaset SE361 WLAN (recommended products: Microsoft Internet Explorer 6.0 or higher and Mozilla Firefox 1.0 or higher),
- ◆ for Internet access
 - a DSL or cable modem and a splitter (for DSL),
 - the access data for your [Internet Provider](#).

First Steps

LED	State	Status
WLAN	On	The radio interface is activated, no data transmission at present.
	Flashing	The Gigaset SE361 WLAN is sending or receiving data on the radio interface.
	Off	The radio interface is deactivated.
LAN1 – LAN4	On	A device is connected to the relevant LAN port.
	Flashing	The LAN port is sending or receiving data (traffic).
	Off	There is no device connected.

Back panel



The back panel of the Gigaset SE361 WLAN offers the following ports and controls:

Element	Description
12V 0,5A DC	Socket for the mains adapter that comes with the device. Warning: Using the wrong power supply unit may damage the Gigaset SE361 WLAN.
WAN	Socket for connecting to the DSL modem.
LAN4 – LAN1	Four 10/100 Mbps switch ports with automatic recognition (RJ45). You can connect up to four Ethernet devices (such as PCs, a Hub or Switch).

Reset

The reset button is located behind the small opening labelled **Reset**.

- ◆ Reboot function (software reset): Press the button for longer than 1 second but less than 5 seconds to reboot the device. This does not affect the configuration settings.
- ◆ Reset function (returns to factory settings): Press and hold the button for at least 5 seconds to return all settings to the factory settings.

Warning: This will clear all the configuration settings you have made since the initial startup.

Updated firmware will not be affected.

Setting up the Gigaset SE361 WLAN

The Gigaset SE361 WLAN can be set up in any suitable location in your home or office. You do not need any special wiring. However you should comply with the following guidelines:

- ◆ Only operate the Gigaset SE361 WLAN indoors within a temperature range of 0°C to +40°C. Do not position the Gigaset SE361 WLAN near sources of heat. Do not cover the ventilation slots. High temperatures can damage the device.
- ◆ A mains socket for 230V~ and a connection socket for the modem or LAN must be available where you set up the Gigaset SE361 WLAN.
- ◆ Do not position the device in the immediate vicinity of stereo equipment, TV sets or microwave ovens. This may cause interference.
- ◆ Position the Gigaset SE361 WLAN so that it is as near to the centre of your wireless network as possible. Make sure that the position of the Gigaset SE361 WLAN offers optimum reception throughout the house or office. You can improve the reception quality by aligning the antenna (turn and/or tilt).
- ◆ Position the Gigaset SE361 WLAN on a non-slip surface.
- ◆ Do not place the Gigaset SE361 WLAN on any furniture surface that could be affected by the heat from the device.
- ◆ Position the Gigaset SE361 WLAN so that it cannot fall.
- ◆ Lay the cables so that nobody can trip over them.
- ◆ Note that the screws for mounting the Gigaset SE361 WLAN on the wall are not included in the scope of delivery.

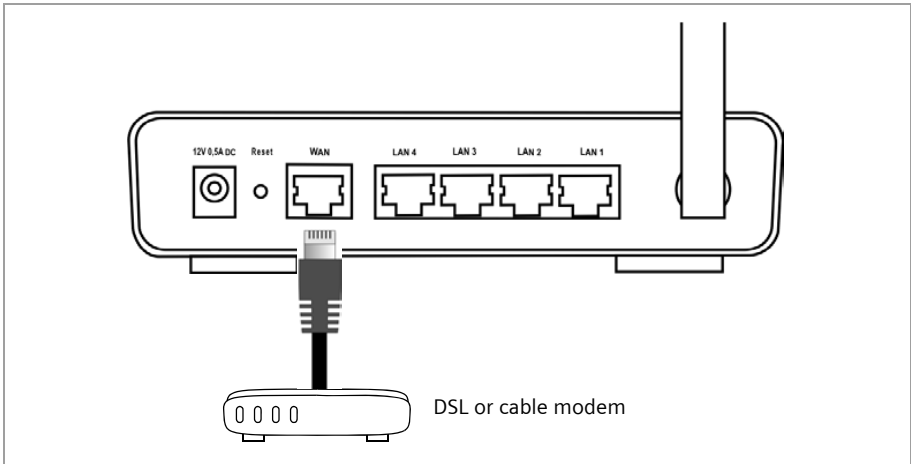
Connecting the Gigaset SE361 WLAN

Before starting to connect PCs to your Gigaset SE361 WLAN, make sure that

- ◆ a wired or wireless [Network adapter](#) is connected to the PC. Please read the user guide that came with the device. Newer PCs and notebooks have wired adapters, and often wireless adapters, built in at the factory.
- ◆ **ConnectionPoint** is entered as **SSID** on the network adapter.

Making the connection to the DSL or cable modem

- ➔ Connect the socket on the back of the router marked **WAN** to your DSL or cable modem with an Ethernet cable.



Note:

Use a category 5 Ethernet cable with RJ45 jacks on both ends for all connections. The cable will normally be included with your modem. However, you can also use the yellow Ethernet cable, which comes with the Gigaset SE361 WLAN.

Making the connection to the PC

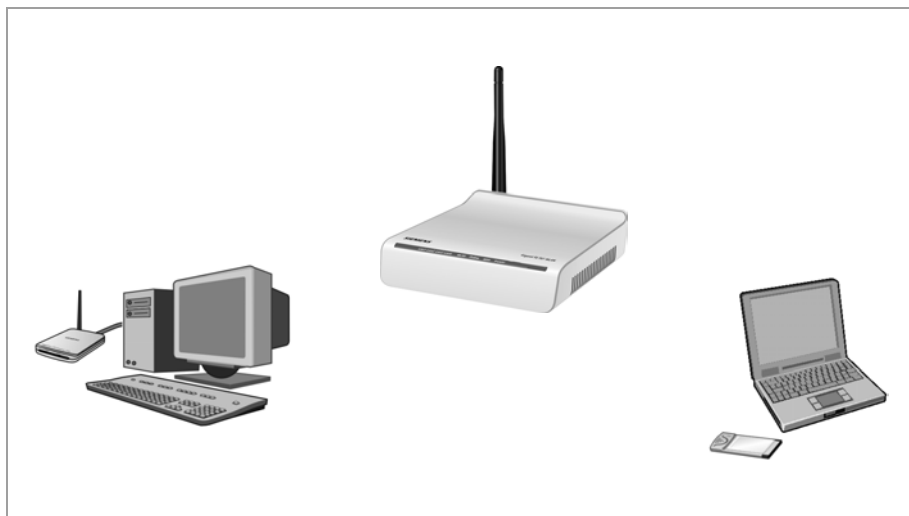
You can connect wired or wireless PCs to your Gigaset SE361 WLAN to create a local area network ([LAN](#)).

Wireless

A wireless connection is made using a wireless network adapter that must be installed in your PC. This can be, for example, a Gigaset USB Stick 54 or another 802.11g or 802.11b-compatible wireless network adapter.

You define a [Radio network](#) by assigning all the devices an identical [SSID](#). You must therefore assign the SSID of the Gigaset SE361 WLAN to the network adapters. The factory set SSID is **ConnectionPoint**.

If the correct SSID has been entered in your PC's wireless network adapter, the wireless link will be established automatically once you connect your Gigaset SE361 WLAN to the mains power supply (see page 23).

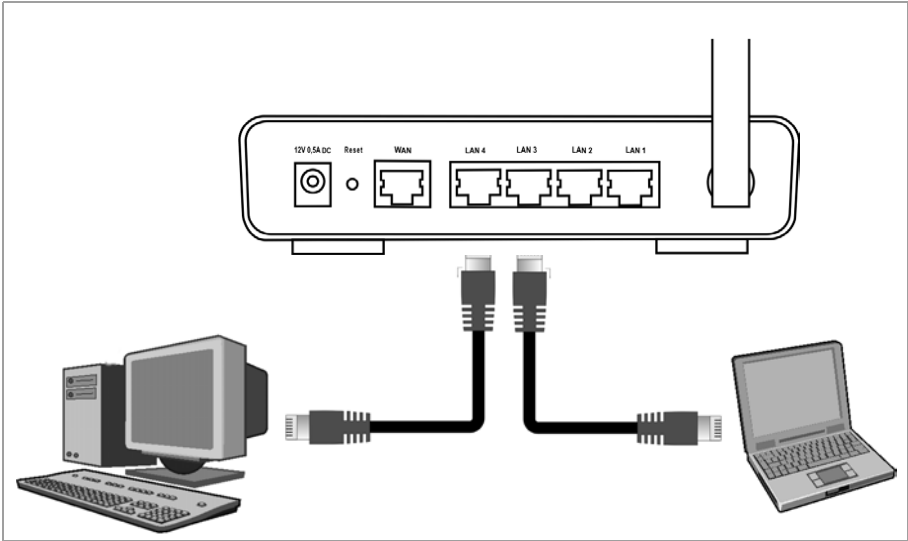


First Steps

Wired

- ➔ Connect one of the yellow LAN sockets (**LAN1 – LAN4**) at the rear of the Gigaset SE361 WLAN to the Ethernet connection on a PC. To do this, use an Ethernet cable with RJ45 jacks (CAT5). You can also use the yellow Ethernet cable supplied with the device.

The four LAN sockets can automatically set the transmission speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, and the transmission mode to **Half duplex** or **Full duplex** depending on the performance of the network adapter in your PC.

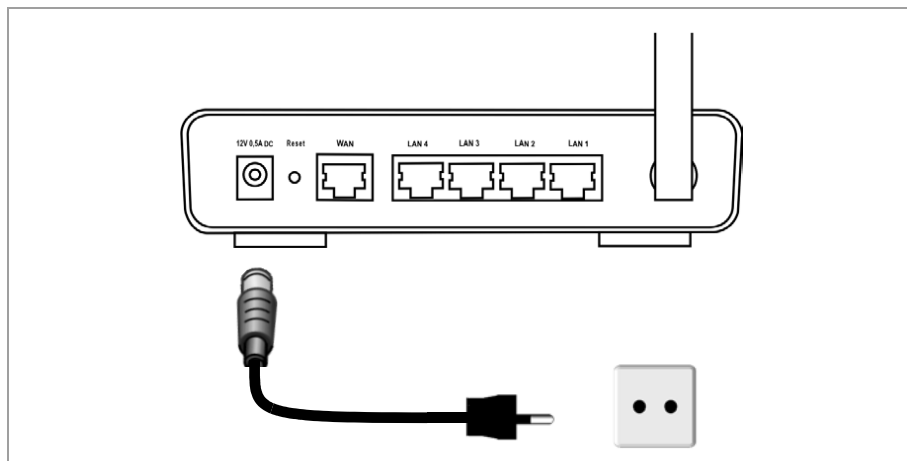


Connecting to the mains power supply

Note:

Only use the mains adapter (12V 0.5A DC) that is supplied with the device.

- ➔ Connect the mains adapter cable to the **12V 0,5A DC** socket on the Gigaset SE361 WLAN.
- ➔ Plug the mains adapter into a mains socket.



Your Gigaset SE361 WLAN is now ready for use:

- ◆ The **power** LED on the front lights up.
- ◆ The **WLAN** LED lights up to indicate that the Gigaset SE361 WLAN is ready to open wireless connections.
The radio link to a PC that is connected by means of a wireless network adapter is established automatically if the network adapter has been configured with the same SSID as the Gigaset SE361 WLAN (see page 21). 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 respective LAN port by means of an Ethernet cable.

In order to communicate via the Gigaset SE361 WLAN, the network must be configured on the connected PCs. This usually takes place automatically (see page 76).

The user interface

Once you have configured the network settings on a PC in your local network, you can then use that PC to configure the Gigaset SE361 WLAN with the aid of the Gigaset SE361 WLAN's user interface. You can use any browser for the configuration, the recommended products are Microsoft Internet Explorer 6.0 or higher, Mozilla Firefox 1.0 or higher.

Note:

To start the configuration environment you might need to deactivate the HTTP proxy for your browser (see page 82 for Windows XP and page 90 for Windows 2000).

If you use Mozilla Firefox or if you use Internet Explorer and Windows XP Service Pack 2, you need to configure the popup blocker (see page 82 for Windows XP and page 90 for Windows 2000).

Launching the user interface

To access the Gigaset SE361 WLAN's user interface:

- ➔ Launch your Web browser.
- ➔ Enter the IP address of the Gigaset SE361 WLAN in the browser's address field.

http://192.168.2.1

A login screen appears for you to enter the password.

- ➔ Enter the password and click on **OK**.

The default password on delivery is **admin**.

Note:

For security reasons you should change the password at a later stage (see page 32).

A page containing security information is displayed.

- ➔ Click on **OK**.

You will now see the start screen.

Note:

If the start page does not show up and the automatic language detection does not work properly (see paragraph "Selecting a language" on page 26), please try to delete the temporary Internet files and Cookies from your browser.

Microsoft Internet Explorer:

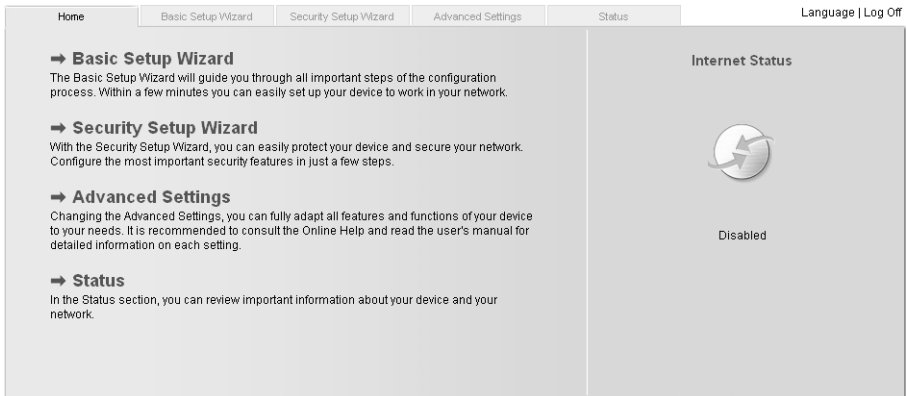
Tools – Internet Options – Delete Cookies and Delete Files

Mozilla Firefox:

Tools – Options – Privacy – Show Cookies – Remove all Cookies.

The start screen

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



Start screen functions

On the start screen you can

- ◆ select the language for the user interface (see page 26),
- ◆ connect to the Internet (see page 68),
- ◆ call up the basic setup wizard, see Basic Setup Wizard (see page 28),
- ◆ call up the wizard for Security Setup Wizard (see page 32)
- ◆ open the **Advanced Settings** menu for additional configuration options (see page 40),
- ◆ open the **Status** menu to obtain status information about the Gigaset SE361 WLAN (see page 64),

You can call up the wizards, the **Advanced Settings** menu and status information from any other screen in the configuration program at any time via the tabs at the top edge of the user interface.

The user interface

The configuration program offers you the following functions:

Basic Setup Wizard	Use this wizard to make the settings required for connecting to the Internet. You can also set the data for your region. This is described on and after page 28.
Security Setup Wizard	This wizard allows you to take precautions against unauthorised access to your Gigaset SE361 WLAN and the local network. For example, you can assign a password and set up encryption for wireless traffic. This is described on and after page 32. For the protection of your network we recommend that you execute this wizard.
Advanced Settings	Additional functions are offered in the Advanced Settings menu. For example, you can back up and restore your configuration data, define access control for PCs, and much more. These configuration steps are optional and can be carried out at a later stage. This is described on and after page 40.
Status	You can view information about the configuration and status of your Gigaset SE361 WLAN in the Status menu. This is described on and after page 71.
Internet Status	You can view the status of your Internet connection and establish a manual connection to the Internet (see page 64).
Language	You can select the language for the user interface (see page 26).

Selecting a language

The user interface can be presented in various languages. During the initial configuration or after resetting the device to the factory settings, the user interface is displayed in German (if the Web browser is also in German) or in English (for all other languages).

- ➔ Click on **Language** at the top right above the screen.
- ➔ If you wish to change the preset language, select the required language from the list.
- ➔ Click **OK** to apply the setting.

You might have to load the file for the language you require. The files are either on the CD-ROM or you can download other languages from the Internet and save them on your PC. Follow the on-screen instructions on the user interface page.

Reboot the device to activate the change. Confirm the reboot in the dialogue field on the screen.

Once the procedure is complete the start screen is shown again.

Elements on the user interface

The user interface Web pages contain the following elements:

Button *Log Off*

You will always find the **Log Off** button on the right above the user interface. If you click on **Log Off**, the session is terminated and the login screen appears again.

Help



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

Buttons and symbols used by the wizards



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

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

Buttons in the *Advanced Settings* menu

OK Transfers the settings you have made to the Gigaset SE361 WLAN configuration.

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

Other buttons may be visible depending on the function in question. These are described in the relevant sections.

Basic Setup Wizard

The Basic Setup Wizard guides you step by step through the general configuration of the Gigaset SE361 WLAN. This includes settings for your region and for your Internet access.

Connection to the [Internet](#) is established via the Gigaset SE361 WLAN for all PCs connected to it. You will need your [Internet Provider's](#) access data for configuration. You should therefore have this data to hand.

Note:

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

The access data is stored in the Gigaset SE361 WLAN during configuration. Before passing the device on to somebody else or having your dealer replace it, you should first restore the configuration to the factory settings (see page 69). If you do not, unauthorised persons will be able to use your Internet access data at your expense.

During initial configuration the first page of **Basic Setup Wizard**, the page for **Regional Options**, is displayed automatically.

- ➔ If you want to execute the Basic Setup Wizard again after the initial configuration, select the **Basic Setup Wizard** entry on the start screen to start configuration.
- ➔ Click on **Next** >.

Regional Options

On this screen you select your present location for the regional settings.

- ➔ Select the country in which you are currently located from the list. You can set for the clock to change automatically to summer time and/or to the time zone as you wish.
- ➔ Select the required option and/or select the time zone for your location.

Configuring Internet connection

You will find the access data you need for configuring the Internet connection in the documentation you receive from your [Internet Provider \(ISP\)](#).

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

To connect your device and your network to the Internet now, please enter the data you have received from your Internet service provider below.

Service provider: Other

Protocol: PPPoE

User name:

Password:

Confirm password:

IP address type: Obtained automatically

Host name: gigaset

MTU: 1492

Connection mode: Connect on demand

Idle time before disconnect: 3 minutes

PPPoE pass-through: On Off

UPnP: On Off

Test Settings

< Back | Next > | Cancel

➔ Select your service provider from the **Service provider** selection menu. If your Internet provider is not included in the list, select the option **Other**.

➔ Enter the data you have been given by your Internet provider.

When you choose your Internet provider from the list, most of the data you need is entered by default on the screen.

You can also often confirm the defaults for the **Other** option.

Check that the **Protocol** complies with the data supplied by your Internet provider.

Note:

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

Basic Setup Wizard

➔ Select how Internet sessions are to be established via the **Connection mode**:

- Select **Always on** if the connection is to remain set up when the Gigaset SE361 WLAN is switched on.

Note:

If you subscribe to a time-based service, this option can result in high connection charges.

- Select **Connect on demand** if applications such as a Web browser or an e-mail program are allowed to connect to the Internet automatically.
- In the **Idle time before disconnect** field, enter a period of time after which the Internet connection is to close down automatically if no data is transmitted (default setting: 3 minutes, range: 1 to 99 minutes).

This time setting only applies to the **Connect on request** option. A permanent connection is achieved using the **Always on** option.

- Select **Connect manually** if you always want to establish and end the connection to the Internet manually. If you subscribe to a time-based service this will save you high connection charges. How to establish a connection manually is described on page 68.

➔ Click on **Test Settings** to check the Internet connection. The device will attempt to connect to the Internet. Any Internet connection already in existence will be closed first.

You will find information about the test steps and results on the **Internet Connection Test** screen.

PPPoE pass-through

PPPoE pass-through enables you to use an additional Internet connection (with another service provider) from one PC. You can find detailed information about this on page 42.

➔ Activate **PPPoE pass-through** if you wish to use this function.

Using UPnP (Universal Plug & Play)

PCs with **UPnP** (Universal Plug & Play) can offer their own network services and automatically use services offered on the network. You can find detailed information about this on page 43.

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

➔ Click on **Next >** to proceed to the next step.

Summary

In the next step the basic settings you have made with the wizard are shown for you to check.

- ➔ If you want to make changes to the settings, click on **< Back**.
- ➔ If you want to confirm the settings, click on **Finish** to close the Basic Setup Wizard.

You will then be taken automatically to the start screen for the **Security Setup Wizard**. If you want to carry this out at a later stage, deactivate the option ***I would like to run the Security Setup Wizard now***. If you deactivate this option a message is output indicating that your system is not secure.

When you finished the Basic Setup Wizard the Gigaset SE361 WLAN is configured and ready to connect to the Internet.

Security Setup Wizard

The **Security Setup Wizard** offers you additional settings that will improve your network security. You can

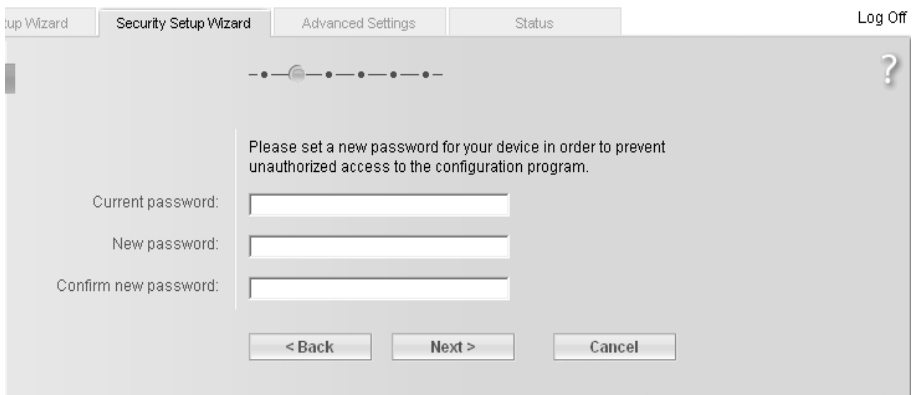
- ◆ assign a Password for configuring the Gigaset SE361 WLAN (see page 32),
- ◆ change the ID for your wireless network (SSID) (see page 33),
- ◆ set [Encryption](#) for wireless traffic (see page 34),
- ◆ limit access to your wireless network to certain PCs (see page 38).

The Gigaset SE361 WLAN's user interface will guide you through the security configuration step by step. Once you have completed a screen, click on **Next >**. If you want to make any changes or check your entries, click **< Back**.

- ➔ Select **Security Setup Wizard** on the start screen or in the tab to start the security configuration if you did not go straight to the start screen for the security settings after making the basic settings.
- ➔ Click on **Next >** to proceed to the next step.

Assigning a Password

In the first step of the setup wizard you can assign a Password for the user interface. On delivery, the configuration of your Gigaset SE361 WLAN is protected with the **admin** Password. To prevent unauthorised changes to the configuration, you should set your own Password and change this Password from time to time.



- ➔ Enter the default password (or the new password you have assigned) in the **Current password** field.
- ➔ Enter a new password in the **New password** field, and repeat it in the **Confirm new password** field.

The Password can be up to 32 alphanumeric characters long. The password is case sensitive. Avoid proper names and all too obvious words. Use a combination of letters and numbers.

Note:

If you ever forget your Password you will have to return the Gigaset SE361 WLAN to its factory settings (see page 18). **admin** is then again assigned as the Password. Please bear in mind that this will return all the configuration settings to the factory settings.

→ Click on **Next >** to proceed to the next step.

SSID

Before the wireless network components can communicate with each other, they must all use the same **SSID** (Service Set Identifier).

On delivery, the Gigaset SE361 WLAN's default SSID is **ConnectionPoint**. For security reasons you should change this SSID and deactivate SSID broadcast.

If this option is enabled, the Gigaset SE361 WLAN will send the SSID in all data transmissions, and your Gigaset SE361 WLAN's SSID will be displayed on all PCs that have a wireless network adapter. In this case eavesdroppers could use the SSID to gain access to your local network.

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

Make a note of the SSID. You will need it to log on your PC.

Note:

The connection to the wireless network adapters will be interrupted until the new SSID has been entered in them as well.

→ Click on **Next >** to proceed to the next step.

Setting security functions for the wireless network

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

Wireless networks are even more strongly exposed to the risk of 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 SE361 WLAN uses effective encryption methods to largely prevent eavesdropping.

You can use the following security mechanisms:

- ◆ WPA2-PSK or WPA2-PSK / WPA-PSK (see page 34)
- ◆ WEP encryption (Wired Equivalent Privacy, see page 35)

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

Note:

If WDS is enabled (see page 62) only WEP is available as encryption method.

You will find further options for setting data encryption in the **Advanced Settings** menu (see page 58).

WPA2 / WPA with Pre-shared key (PSK)

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

WPA-PSK is a special WPA mode for users at home and in small companies without a company authentication server. Encryption keys are automatically generated with the Pre-shared key, automatically changed ("rekeying") and authenticated between the devices after a certain period of time (**Rekey interval**).

Note:

Every PC (network adapter) that requires access to a wireless network protected by WPA must also support WPA. To find out whether and how you can use WPA on your PC, read the user guide supplied with your network adapter.

- ➔ Select the **WPA2-PSK** option if it is supported by all components in your wireless network.
or
- ➔ Select **WPA2-PSK / WPA-PSK** if some or all components in your wireless network support WPA with the TKIP protocol.

- ➔ Enter a key of your choice in the **Pre-shared key** field (min. 8 to max. 63 characters) and confirm it by repeating the entry.

Note:

- ◆ It is very **important** that you make a note of the **Pre-shared key**. You will need this information to configure the wireless network adapters correctly.
- ◆ When you have completed the Security Setup Wizard you must also change the encryption data on the wireless network adapters in the connected PCs since, without the change, they will not be able to access the Gigaset SE361 WLAN's wireless network.

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

WEP encryption

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

If you transmit data wirelessly and not all components in your wireless network support the higher security standard WPA (see page 34), we recommend that you activate [WEP Encryption](#) on these network components.

You can choose either the standard 64-bit keys or the more robust 128-bit keys for encryption. The keys are generated in hexadecimal or in ASCII format. You must use the same keys for encryption and decryption for the Gigaset SE361 WLAN and all your wireless network adapters.

- ➔ Select the **Key length**: 64 or 128-bit.
- ➔ Select the **Input type**, i.e. whether you wish to enter the key manually or have it 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 exactly 10 characters long.
Example of a valid key: 1234567ABC
- With a 128-bit encryption depth the key is exactly 26 characters long.
Example of a valid key: 234567ABC8912345DEF1234567

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

- With a 64-bit encryption depth the key is exactly 5 characters long.
Example of a valid key: GIGA1
- With a 128-bit encryption depth the key is exactly 13 characters long.
Example of a valid key: GIGASET_SE361

- ➔ Confirm the key by entering it again in the field **Confirm key**.

Generating the key by means of a Passphrase

Security Setup Wizard Security Setup Wizard Advanced Settings Status Log Off

It is strongly recommended to enable WPA-PSK security (or WEP security for backward compatibility with older devices) to protect your privacy and restrict access to your wireless network.

Security: WEP

Key length: 128 bits

Input type: Passphrase

Passphrase:

Confirm passphrase:

< Back Next > Cancel

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

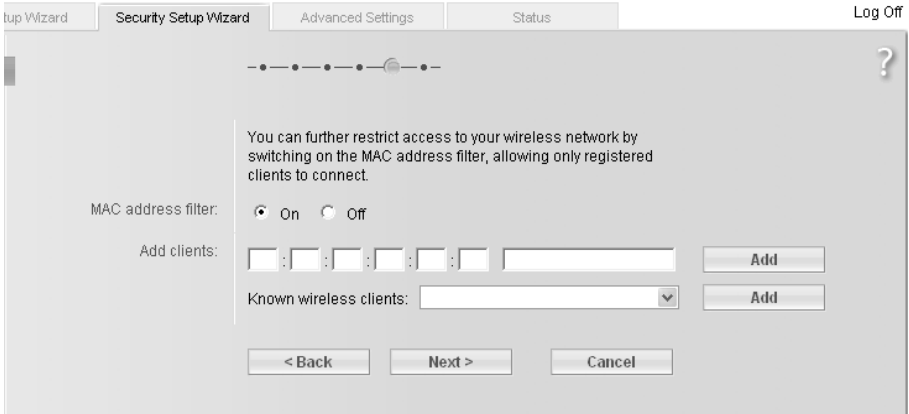
Note:

- ◆ 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 correctly.
- ◆ When you have concluded the Security Setup Wizard you must also change the WEP encryption data on the wireless network adapters in the connected PCs since, without the change, they will not be able to access the Gigaset SE361 WLAN's wireless network.

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

Access control within the wireless network

In this step you can specify which PCs will have wireless access to the Gigaset SE361 WLAN and hence to your LAN. Access control is based on the **MAC address** of the PCs' network adapters. You can enter the MAC addresses for the PCs manually or select them from the list of PCs that are currently logged in.



The default setting for access control is disabled. This means that all PCs that use the correct **SSID** and the right encryption method can log in.

➔ Next to **MAC address filter** select the option **On** to activate MAC filtering.

Entering MAC addresses manually

- ➔ Enter the MAC address of the network adapter. You will normally find this address on a label on the device.
- ➔ Enter a name for the PC.
- ➔ Click on **Add** to add the entry to the list.

Selecting from the list of known PCs

- ➔ Select the required PC from the **Known wireless clients** list. All PCs that are currently logged in to the router with the correct SSID are displayed.
- ➔ Click on **Add** to add the selected PC to the list.

Note:

If you activate MAC access control, you must at least enter the PC from which you are configuring the Gigaset SE361 WLAN. If you fail to do this, you will no longer be able to access the user interface and an error message will be shown.

If, by mistake, you have denied all PCs access to the Gigaset SE361 WLAN you have two options:

- ◆ You can reset the Gigaset SE361 WLAN to the factory settings (see page 18).
- ◆ You can connect a PC to the Gigaset SE361 WLAN using one of the LAN connections (by cable). Since MAC access control only applies to PCs that are connected "wirelessly", you can use this PC to change the configuration.

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

Saving settings

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

➔ Click on **Finish** to close the wizard.

The settings will now be active on your Gigaset SE361 WLAN.

Note:

You must now configure the WEP or WPA key for your PC's wireless network adapter, if this has been configured with other values. Once you have done this you can log in to your Gigaset SE361 WLAN wirelessly again.

Configuring the Advanced Settings

In the **Advanced Settings** menu, you can configure all the options for the Gigaset SE361 WLAN. If you want, you can also make changes to the settings you made using the wizard. The following table shows the options in the menu.

Menu	Description
Internet	<p>This menu comprises all the settings relating to the Internet. You can:</p> <ul style="list-style-type: none">◆ check and change the configuration for Internet access (see page 41) or specify a preferred DNS server (see page 44),◆ configure the firewall, i.e. a number of security and special functions, e.g. access control for local PCs to the Internet or blocking certain Internet sites (see page 45),◆ make the NAT settings needed to provide your own services on the Internet (see page 47),◆ set up dynamic DNS for a static Internet address on your device (see page 52),◆ configure the Quality of Service (see page 53).
Local Network	<p>Here you can change the Private IP address of the Gigaset SE361 WLAN and make settings on the DHCP server (see page 54).</p>
Wireless Network	<p>Here you can configure the options for wireless communication (SSID and encryption) and restrict access to the Gigaset SE361 WLAN (see page 41).</p>
Administration	<p>Here you can make or change various system settings, e.g. assign a password (see page 66), set the time (see page 65), or activate remote administration (see page 67).</p> <p>You can also back up the data on your Gigaset SE361 WLAN or load new firmware (see page 68).</p>

Configuring the Internet connection

If you have configured your Gigaset SE361 WLAN using the two wizards, you will already have 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 options for security settings and limiting access to the Internet as well as for providing your own services on the Internet.

Internet

On the **Internet** screen you can grant or block access to the Internet over your Gigaset SE361 WLAN.

Internet Connection

On this screen you can set up or change the configuration of your Internet connection. Any settings you make here must coincide with the features your Internet provider makes available to you. Incorrect data can lead to problems with your Internet connection.

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

The screenshot shows the 'Internet Connection' configuration screen. 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 main title is 'Internet Connection' with a help icon (?). The configuration options are as follows:

- Service provider: Other (dropdown)
- Protocol: PPPoE (dropdown)
- User name: (text input)
- Password: (text input)
- Confirm password: (text input)
- IP address type: Obtained automatically (dropdown)
- Host name: gigaset (text input)
- MTU: 1492 (text input)
- Connection mode: Connect on demand (dropdown)
- Idle time before disconnect: 3 minutes (text input)
- PPPoE pass-through: On Off
- UPnP: On Off
- IGMP proxy server: On Off

At the bottom, there is a 'Test Settings' button, and 'OK' and 'Cancel' buttons.

Configuring the Advanced Settings

- ➔ Select your Internet provider from the **Service provider** list.
- ➔ Enter the data you have been given by your **Service provider** in the relevant fields.
When you choose your Internet provider from the list, most of the data you need is entered by default on the screen.

You can also often confirm the defaults for the **Other** option.

Check that the **Protocol** complies with the data supplied by your Internet provider.

Note:

To configure the Internet connection successfully all fields must be filled in with the precise details given by your provider.

- ➔ Select how Internet sessions are to be established via the **Connection mode**:
 - Select **Always on** if the connection is to remain set up when the Gigaset SE361 WLAN is switched on.

Note:

If you subscribe to a time-based service, this option can result in high connection charges.

- Select **Connect on demand** if applications such as a Web browser or an e-mail program are allowed to connect to the Internet automatically.
 - In the **Idle time before disconnect** field, enter a period of time after which the Internet connection is to close down automatically if no data is transmitted (default setting: 3 minutes, range: 1 to 99 minutes).
This time setting only applies to the **Connect on demand** option. A permanent connection is achieved using the **Always on** option.
 - Select **Connect manually** if you always want to establish and end the connection to the Internet manually. If you subscribe to a time-based service this will save you high connection charges. How to establish a connection manually is described on page 64.
- ➔ Click on **Test Settings** to check the Internet connection. The device will attempt to connect to the Internet. Any Internet connection already in existence will be closed first.

This displays information on the tests that have been carried out and their results.

You will then be returned to the **Internet Connection** screen. If necessary, you can now correct your entries.

- ➔ If the test was successful, click on **OK** to apply the settings.

PPPoE pass-through

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

- ➔ In the **Advanced Settings – Internet** menu, select the entry **Internet Connection**.
- ➔ Select the **On** option to activate **PPPoE pass-through**.

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

Using UPnP (Universal Plug & Play)

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

Note:

Check whether the UPnP function has been installed in your PC's operating system. If not, you may have to install your operating system's UPnP components. Please consult your PC operating instructions.

As soon as you have installed UPnP in the operating system of a PC and activated it on the router, applications on this PC (e.g. Microsoft Messenger) can communicate via the Internet without you needing to grant explicit authorisation. In this case, the router automatically implements [Port Forwarding](#), see page 50, thereby facilitating communication via the Internet.

You will see a symbol for your Gigaset SE361 WLAN in the taskbar on the PC on which UPnP is installed. Windows XP systems will also include the icon under its Network Connections. Clicking on this icon opens the Gigaset SE361 WLAN's configuration screens.

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

➔ Select **UPnP**.

Note:

When the UPnP function is active, system applications can assign and use [Ports](#) on a PC. This can be a security risk.

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

IGMP proxy server

[IGMP](#) (Internet Group Management Protocol) enables a PC to report its membership of a multicast group to other PCs over the Internet. With multicasting, a PC can send content on the Internet to several other PCs that have registered an interest in the first computer's data and information.

➔ Activate **IGMP proxy server** if you wish to use this function.

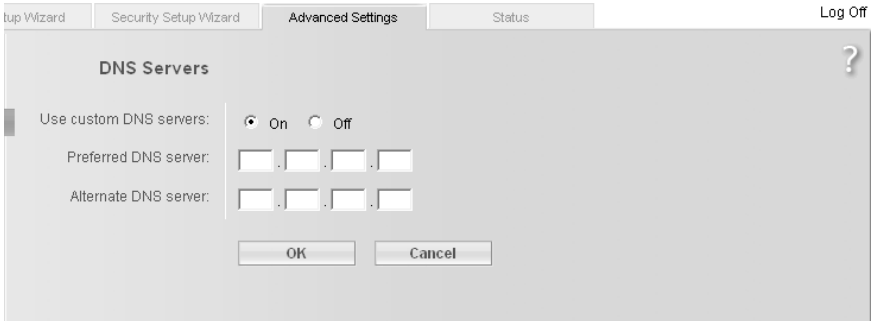
Configuring the Advanced Settings

DNS servers

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.

Normally your Internet provider supplies you with a [DNS server](#), which makes this assignment when the connection to the Internet is set up. If necessary, you can define the DNS server to be used for Internet connections manually.

➔ In the **Advanced Settings – Internet** menu, select the entry **DNS Servers**.



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

➔ Enter the IP addresses for your **Preferred DNS server** and **Alternate DNS server**.

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

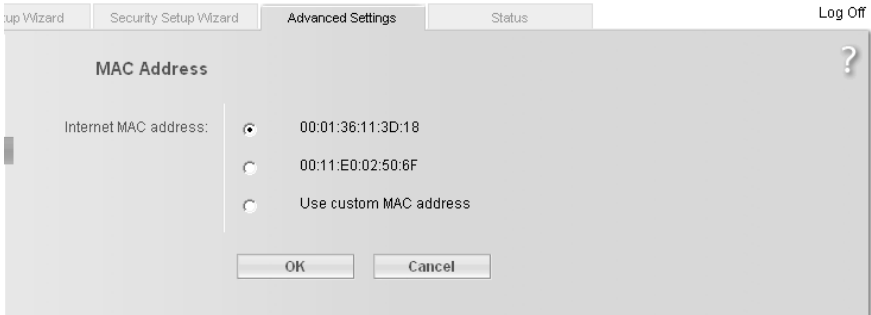
MAC address

If you had Internet access through the same Internet provider before connecting the Gigaset SE361 WLAN, then it is possible that the MAC address of one of your PCs was used for registration when access was configured. In this case, you must either replace the current MAC address with the MAC address registered with the Internet provider or ask your Internet provider to register a new MAC address for your account.

Carry out the following steps:

➔ Connect a PC to the Gigaset SE361 WLAN and open the configuration environment.

➔ In the **Advanced Settings – Internet** menu, select the entry **MAC address**.



- ➔ Select the MAC address that is to apply to the Internet connection:
 - **Use default device MAC address:** You can leave this default setting if the MAC address of the Gigaset SE361 WLAN is used to connect to the Internet.
 - **Use MAC address of this PC:** Select this option if the MAC address of the currently connected PC was previously registered for connecting to the Internet or if you have re-registered the MAC address of the PC on which you are currently working.
 - **Use custom MAC address:** Select this option if you have asked your Internet provider to register a new MAC address and this is not the MAC address of the PC on which you are currently carrying out the configuration.
- ➔ Click on **OK** to apply the settings.

Firewall

The firewall functions of the Gigaset SE361 WLAN include various security functions for your local network.

You can block individual PCs' access to individual services or Internet sites (see page 46).

The firewall functions for the Gigaset SE361 WLAN are activated and configured in the factory. If you wish to deactivate the firewall, carry out the following steps:

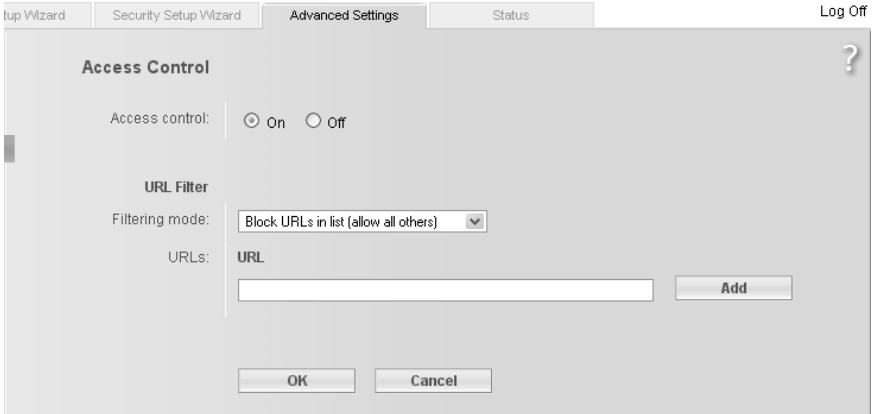
- ➔ In the **Advanced Settings – Internet** menu, select the entry **Firewall**.
- ➔ Select the required option.
- ➔ Click on **OK** to apply the settings.

Setting up access control to the Internet

The **Access Control** function allows you to block access to various Internet services for one or more PCs.

Select **Access Control** in the **Advanced Settings – Internet – Firewall** menu.

➔ Activate the **Access Control** function via the option **On**.



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

URL filter

The URL filter allows you to block access to certain Internet sites or Internet domains, or to limit accesses to certain Internet sites. Once you have entered the relevant URLs you can then create access rules that apply the URL filter to the selected clients in your network.

- ➔ In the **Advanced Settings – Internet – Firewall** menu, select **Access Control**.
- ➔ Select **Filtering mode**, i.e. whether you wish to allow or block access to the URLs in the list.
- ➔ Enter the required URL in the field.
- ➔ Click on **Delete** to delete an entry. Click on **Add** to create a new entry.
- ➔ Click on **OK** to apply the settings.

Setting up the NAT function

Your Gigaset SE361 WLAN comes provided with the NAT (Network Address Translation) function. With address translation, several users on your local network can access the Internet via one or more public IP addresses. In the default setting, all local IP addresses are mapped to your router's public IP address.

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

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

Some applications, such as games on the Internet, require several links, i.e. several ports so that the players can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to the user on the local network. Initially, these applications will not work if Network Address Translation (NAT) is activated.

Using port forwarding (the forwarding of requests to specific ports) you make the router forward requests from the Internet for a certain service, e.g a game, to the appropriate port or ports on the PC on which the game is running.

Port triggering is a specific variant of port forwarding. Unlike port forwarding, in this case the Gigaset SE361 WLAN forwards data from the set port block to the PC which has previously sent data to the Internet via a certain port (trigger port). This means that permission for data transfer is not tied to one specific PC in your network, but only 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. To this trigger port you then assign the public ports that have to be opened for the application.
- ◆ The router checks all outgoing data for port number and protocol. If it recognises a match of port and protocol to 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, it allows the data through and routes it to the right PC. A trigger event always comes from a PC within the local network. If a trigger port is addressed from outside, it is simply ignored by the router.

Configuring the Advanced Settings

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 SE361 WLAN is delivered, the **NAT** function (Network Address Translation) is activated, i.e. all IP addresses of PCs in the local network are mapped to the router's public IP address when accessing the Internet.

You can use the NAT settings for the Gigaset SE361 WLAN to

- ◆ set up port triggering for special applications (see page 49),
- ◆ set up the Gigaset SE361 WLAN as a virtual server by configuring Port Forwarding (see page 50),
- ◆ open the firewall for selected PCs (see page 51).

Note:

For the functions described below you must make sure that the IP addresses of the PCs do not change. If the IP addresses of the PCs are assigned via the DHCP server of the Gigaset SE361 WLAN, you must select the option **Never expires** for the settings on the **Local Network** screen for **Lease time** (see page 55) or assign static IP addresses for the PCs.

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

- ➔ In the **Advanced Settings – Internet** menu, select **Address Translation (NAT)** and mark the required option.

Port triggering

If you configure port triggering for a certain application, define a so-called trigger port and the protocol (TCP or UDP) this port uses. To this trigger port you then assign the public ports that have to be opened for the application.

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

- ➔ To set up port triggering for a service, select **Port Triggering** in the **Address Translation (NAT)** menu.

Local protocol	Local port	Public protocol	Public port	Comment	Enabled
TCP		TCP			<input checked="" type="checkbox"/>
Predefined applications: Battle.net					<input checked="" type="checkbox"/>

- ➔ Select the required application from the **Predefined applications** list.
- ➔ Click on the **Add** button. The data for the required service is entered on the screen.
- ➔ Select the option 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 data traffic.

Note:

You can enter a single port number, several individual port numbers separated by commas, port blocks consisting of two port numbers separated by a hyphen, or any combination of these, e.g. **80 , 90-140 , 180**.

- ➔ **Description:** Enter a description to help you identify different entries.
- ➔ Select the option in the **Enabled** column.
- ➔ Click on the **Delete** button to delete an entry. Click on the **Add** button to add a new entry.
- ➔ Click on **OK** to apply the settings.

Port forwarding

If you configure port forwarding, the Gigaset SE361 WLAN 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 SE361 WLAN needs a mapping table of the port numbers to redirect the service requests to the server that actually provides the service. For this, Port Forwarding has to be configured.

➔ To set up port forwarding for a service, select **Port Forwarding** in the **Address Translation (NAT)** menu.



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

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

- ➔ Select the protocol for the service you are providing from the **Protocol** list.
- ➔ Under **Public port**, enter the port number of the service you are providing.
- ➔ In the **Local port** field, enter the internal port number to which service requests are to be forwarded.
- ➔ In the **Local IP address** field, enter the IP address of the PC which provides the service.

Example: The Web server has been configured to react to requests on port 8080. However, requests from websites enter by port 80 (default setting). 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 port number 80 on the Web server of the PC you have defined with port 8080.

Note:

You can enter a single port number, several individual port numbers separated by commas, port blocks consisting of two port numbers separated by a hyphen, or any combination of these, e.g. **80,90-140,180**.

- ➔ Click on **Add**.
- ➔ Click on **Delete** if you wish to delete the data in the relevant line again.
- ➔ Select the option in the **Enabled** column.
- ➔ Click on **OK** to apply the settings.

Opening the firewall for a selected PC (Exposed Host)

You can set up a client as an exposed host in your local network. Your device will then forward all incoming data traffic from the Internet to this client. This will enable you, for example, to operate your own Web server on one of the clients in your local network and make it accessible to Internet users.

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

Note:

Only one PC per public IP address can be set up as Exposed Host (see also the section entitled "Port forwarding" on page 50).

- ➔ To set up a PC as an Exposed Host, select **Exposed Host** in the **Address Translation (NAT)** menu.

- ➔ Enter the **Local IP address** of the PC that is to be enabled as Exposed Host.
- ➔ Enter a name for the PC in the **Comment** field.
- ➔ Enable the entry by selecting the option.
- ➔ Click on **Add** to add the entry to the list.
- ➔ Click on **Delete** to delete the entry from the list.

Configuring the Advanced Settings

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

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 for your local network's WAN connection assigns the IP address dynamically, the IP address of the router may 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 constantly updated. This is handled by the dynamic DNS service (**DynDNS**). You can use the DynDNS service to assign your Gigaset SE361 WLAN an individual static domain name on the Internet even if it does not have a static IP address.

There are various providers on the Internet who offer a free DynDNS service. The Gigaset SE361 WLAN uses the DynDNS service from **DynDNS.org** and from TZO.org. If you use this DynDNS provider's service, then your service can be reached on the Internet as a subdomain of one of this provider's domains.

If you have activated the device's DynDNS function, it will monitor its public IP address. When this changes, it sets up a connection to the Internet site and updates its IP address there.

Note:

You will have to open an account with the provider before you can use the Gigaset SE361 WLAN's DynDNS function. Follow the instructions on the provider's web site. Enter the user data during configuration of the router.

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

The screenshot shows the 'Dynamic DNS' 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 'Dynamic DNS' with a help icon. The 'Dynamic DNS' section has two radio buttons: 'On' (selected) and 'Off'. Below this is a 'Service provider' dropdown menu with 'DynDNS.org' selected. There are four text input fields: 'Domain name', 'User name', and 'Password'. At the bottom are 'OK' and 'Cancel' buttons.

➔ Activate the **Dynamic DNS** function.

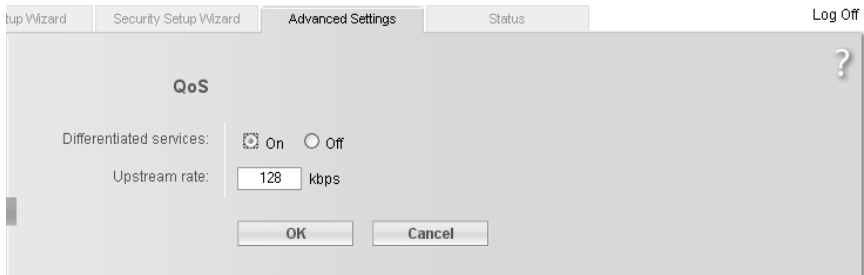
➔ From the **Service provider** list, select the service offering dynamic DNS (DynDNS.org or TZO.com).

- ➔ Enter the **Domain name**, **User name** and **Password**. You will have received the necessary information when registering with your **Service provider**.
- ➔ Click on **OK** to apply the settings.

QoS (Quality of Service)

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

- ➔ In the **Advanced Settings – Internet** menu, select the entry **QoS**.



- ➔ Activate **Differentiated services**, i.e. the prioritisation of certain services for data transfer between your network and the Internet.
- ➔ In the field next to **Upstream rate**, enter the maximum speed of your DSL line for sending data into the Internet. The speed is specified in the contract with your Internet provider.
- ➔ Click **OK** to accept the changes.

LAN configuration

You can use the LAN configuration to define an [IP address](#) for the Gigaset SE361 WLAN and configure the DHCP server.

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

The screenshot shows the 'Advanced Settings' tab of a configuration wizard. It is divided into three main sections: 'Local Network', 'DHCP Server', and 'DHCP clients'.
- **Local Network:** IP address is 192.168.2.1, Subnet mask is 255.255.255.0.
- **DHCP Server:** DHCP server is turned 'On'. Lease time is set to '30 minutes'. First issued IP address is 192.168.2.100, and last issued IP address is 192.168.2.199. Domain name is empty.
- **DHCP clients:** A table with columns for 'MAC address' and 'IP address'. The 'IP address' column contains '192.168.2.' followed by an empty field. An 'Add' button is next to it.
At the bottom are 'OK' and 'Cancel' buttons.

Defining the private IP address for the Gigaset SE361 WLAN

On this screen you can change the device's [IP address](#). The default IP address is 192.168.2.1. This is the Gigaset SE361 WLAN's [Private IP address](#). It is the address under which the device can be reached on the local network. The address can be freely assigned from the block of available addresses. The IP address under which the Gigaset SE361 WLAN can be reached from outside is assigned by the Internet Service Provider.

➔ If you want to assign the Gigaset SE361 WLAN a different IP address, enter it in the fields next to **IP address**.

➔ Select a number from the **Subnet mask** list.

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

Note:

New settings only take effect after rebooting the Gigaset SE361 WLAN. 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 SE361 WLAN has a [DHCP server](#), which is enabled on delivery. As a result, the IP addresses of the PCs are automatically assigned by the Gigaset SE361 WLAN.

Note:

- ◆ If the Gigaset SE361 WLAN's DHCP server is activated, you can configure the network setting on the PC so that the option **Obtain an IP address automatically** is set. To find out how to do this, please read the section entitled "Configuring the local network" on page 76.
- ◆ If you deactivate the DHCP server, you will have to assign a static IP address for the PCs via the network settings.

- ➔ To activate the DHCP server, select **On**.
- ➔ If the DHCP server is active, you can define a **Lease time**. The [Lease time](#) determines the period for which the PCs keep the IP addresses assigned to them without any change.

Note:

If you select the **Never expires** option, the IP addresses are never changed. You must select this option if you want to make NAT or firewall settings using the IP addresses of the PCs, or else you must assign these PCs static IP addresses.

- ➔ Define the range of IP addresses which the Gigaset SE361 WLAN should use to automatically assign IP addresses to PCs. Define the **First issued IP address** and the **Last issued IP address**.
- ➔ You can define the name of a domain (Windows workgroup) in the **Domain name** field.

Assigning static IP addresses to individual PCs

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

- ➔ Enter the **MAC address** and the name of the PC in the **Device name** field.
- ➔ Enter the **IP address** you wish to assign to the PC in the field below.
- ➔ Click on **Add** to add the entry to the list.
- ➔ Click on **Delete** to delete the entry from the list.
- ➔ Click on **OK** to apply the settings.

Configuration for wireless connections

If PCs communicate wirelessly via the Gigaset SE361 WLAN, you should take steps to enhance the security of your wireless network. You make this configuration via the **Advanced Settings – Wireless Network** menu. Here you can

- ◆ activate the Gigaset SE361 WLAN's wireless module (see below),
 - ◆ set the channel and **SSID** (see page 56),
 - ◆ set **Encryption** for wireless traffic (see page 58),
 - ◆ restrict access to the Gigaset SE361 WLAN's LAN (see page 58),
 - ◆ configure the Gigaset SE361 WLAN's repeater function (see page 62).
- ➔ 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' (which is selected), and 'Status'. A 'Log Off' link 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
- Transmission mode: IEEE 802.11b/g (mixed) (dropdown)
- SSID: ConnectionPoint (text input)
- Channel: 6 (dropdown)
- SSID broadcast: On Off
- Sending power: 100 % (dropdown)
- Network performance: Optimize throughput (dropdown)

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

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

Devices can only log in wirelessly if the Gigaset SE361 WLAN's wireless module is activated.

You can now make the settings for your wireless network.

Transmission mode

The Transmission mode defines which **IEEE** standard you use to transmit data in your network. IEEE 802.11g permits data transfer up to 54 Mbps, IEEE 802.11b up to 11 Mbps.

For the best possible data transfer rates in your network select **IEEE 802.11g only**. You can use this mode if the PC has the appropriate network adapter and there are no other WLAN adapters in the vicinity.

To operate clients that have older network adapters in your network, select **IEEE 802.11b/g (mixed)**. If you exclusively use older adapters select **IEEE 802.11b only**.

- ➔ Select the required Transmission mode for your wireless network.

SSID

For the wireless network components to communicate with each other, they must have the same **SSID** (Service Set Identifier).

On delivery, the Gigaset SE361 WLAN's default SSID is **ConnectionPoint**. For security reasons you should change this SSID and deactivate SSID broadcast (see below).

Enter a character string of your choice. The SSID is case sensitive. It can be up to 32 alphanumerical characters long.

Note:

The connection to the wireless network adapters will be interrupted until you enter the new SSID on them as well.

Channel

All the clients in your network use the set radio channel for wireless data transfer. In the case of potential interferences caused by other 2.4 GHz devices in the neighbourhood, you can choose between various channels.

➔ Select the channel to be used for transmitting the data.

SSID broadcast

If this option is enabled (default setting), the Gigaset SE361 WLAN will send the SSID will be sent with all data transmissions, and your Gigaset SE361 WLAN's SSID will be displayed on PCs that have a wireless network adapter. In this case, eavesdroppers could use the SSID to gain access to your local network.

If you disable **SSID broadcast**, your Gigaset SE361 WLAN's SSID will not be displayed. This increases protection against unauthorised access to your wireless network. However, you must make a note of the SSID. You will need it to log on your PC.

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

Sending power

➔ Select the required sending power for your device.

We recommend that you select a sending power with a range to suit the spatial environment of your local network. A range that is much greater makes it easier to eavesdrop on your wireless data transmission.

Network performance

You can optimise Network performance in the following ways:

◆ **Optimize throughput**

maximises the data transmission rate in your network and ensures that data traffic is transmitted immediately.

◆ **Optimize power saving**

optimises power consumption in order to extend standby times for mobile devices in your network, e.g. notebooks, PDAs and WLAN handsets.

Configuring the Advanced Settings

◆ **Custom**

This allows you to adjust the Network performance to suit your needs on the basis of the following items:

- **Beacon interval** defines the interval between two **Beacons**.
Measured in milliseconds, default = 100 msec.
- **DTIM interval** defines the interval between two **DTIMs** for devices in power-saving mode.
Measured in number of beacons, default = 2 beacons.

➔ Choose the desired **Network performance**.

Setting wireless security

If you send data over wireless channels, we recommend that you activate encryption (**WEP** or **WPA**) on your wireless network components.

WPA is a more advanced procedure than **WEP** for protecting wireless networks. Dynamic keys based on TKIP (Temporal Key Integration Protocol) offer increased security. The new **WPA2** standard is based on **AES**. We therefore recommend that you choose **WPA2** or **WPA** encryption if it is supported by all components in your wireless network.

Note:

If **WDS** is enabled (see page 62) only **WEP** is available as encryption method.

➔ In the **Wireless Network** menu, select **Encryption**.

The following security mechanisms are currently available:

- ◆ **WPA2-PSK** and **WPA2-PSK / WPA-PSK** (see page 58)
- ◆ **WEP encryption** (Wired Equivalent Privacy), (see page 59)

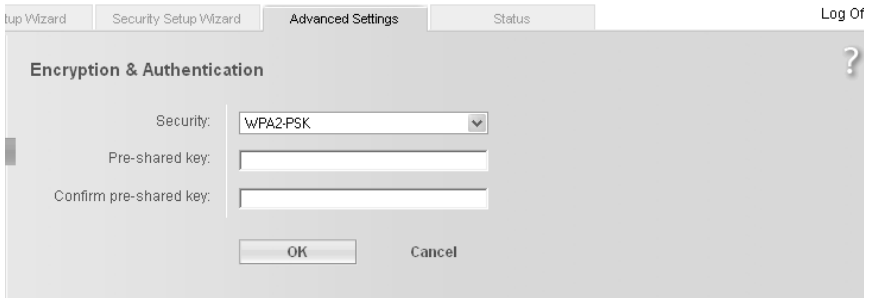
WPA2-PSK and WPA2-PSK / WPA-PSK

WPA with Pre-shared Key (WPA-PSK)

WPA-PSK is a special **WPA** mode that provides encryption protection for users at home and in small companies without a company authentication server. Encryption keys are automatically generated with the Pre-shared Key, and automatically changed (rekeying) and authenticated between the devices after a certain period of time (**Rekey interval**).

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

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

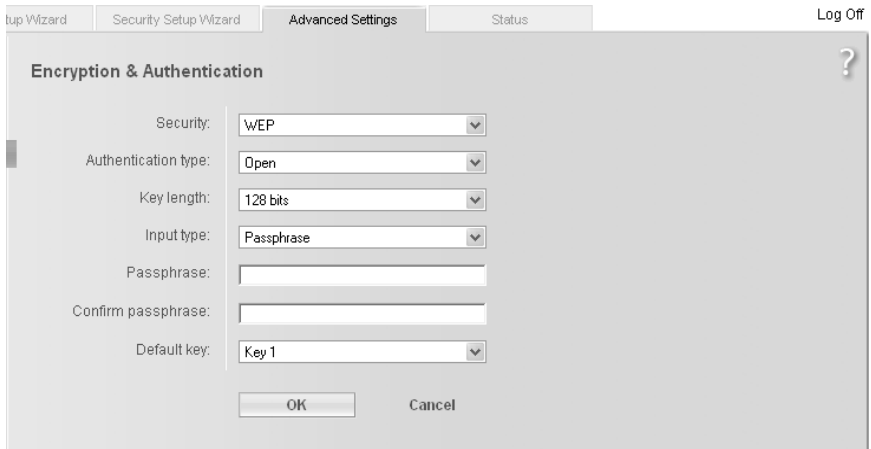


- ➔ Enter a key in the **Pre-shared key** field (up to 32 alphanumeric characters) and confirm it by entering it again.
- ➔ Apply the settings by clicking **OK**.

WEP encryption

If WPA is not supported by all components in your wireless network, we advise you to activate [WEP Encryption](#) on your wireless network components.

- ➔ In the **Security** field, select the **WEP** option.



- ➔ Select the **Authentication type**:
 - Select **Shared** if you want each client to log in to the network with a specified key.
 - Select **Open** to permit data transfer within your wireless network without using a key.

You can choose either the standard 64-bit keys or the more robust 128-bit keys for encryption. The keys are generated in hexadecimal or in ASCII format. You must use the same keys for encryption and decryption for both the Gigaset SE361 WLAN and all your wireless network adapters.

Configuring the Advanced Settings

- ➔ Select the **Key length**: 64 or 128-bit.
- ➔ Select the **Input type**, i.e. whether you wish to enter the key manually or have it generated automatically by means of a **Passphrase**.

Generating the key by means of a Passphrase

- ➔ Enter a **Passphrase** (up to 32 characters) and confirm it by entering it again. Four keys are generated.
- ➔ Select one of the four keys as **Default key**.

Manual key entry

- ➔ Select the **Key type**, **Hex** or **ASCII**.

The screenshot shows a software interface with a tabbed menu at the top containing 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. The 'Advanced Settings' tab is active. In the top right corner, there is a 'Log Off' button. The main area is titled 'Encryption & Authentication' and contains several configuration options, each with a dropdown menu or text input field:

- Security: WEP
- Authentication type: Open
- Key length: 128 bits
- Input type: Key
- Key type: ASCII
- Key 1: [Empty text box]
- Confirm key 1: [Empty text box]
- Key 2: [Empty text box]
- Confirm key 2: [Empty text box]
- Key 3: [Empty text box]
- Confirm key 3: [Empty text box]
- Key 4: [Empty text box]
- Confirm key 4: [Empty text box]
- Default key: Key 1

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

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 exactly 10 characters long.
Example of a valid key: 1234567ABC
- With a 128-bit encryption depth the key is exactly 26 characters long.
Example of a valid key: 234567ABC8912345DEF1234567

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

- With a 64-bit encryption depth the key is exactly 5 characters long.
Example of a valid key: GIGA1

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

Example of a valid key: GIGASET_SE361

- ➔ Enter up to four keys in fields **Key 1** to **Key 4** and confirm these keys by entering them again in fields **Confirm key 1** to **Confirm key 4**.
- ➔ Select one of the four keys as **Default key**.

Note:

- ◆ It is very **important** that you make a note of keys you enter or generate. You will need this information to configure the wireless network adapters correctly.
- ◆ When you have completed configuration you must also change WEP encryption on the wireless network adapters for the connected PCs; if you do not, they will no longer be able to access the Gigaset SE361 WLAN's wireless network.

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

Allowed clients

On this screen you can specify which PCs will have wireless access to the Gigaset SE361 WLAN and hence to your LAN.

- ➔ In the **Wireless Network** menu, select **Allowed Clients**.

The screenshot shows the 'Allowed Clients' configuration window. At the top, there are tabs for 'Setup Wizard', 'Security Setup Wizard', 'Advanced Settings' (which is selected), and 'Status'. A 'Log Off' button is in the top right corner. The window title is 'Allowed Clients' with a help icon (?). Under 'MAC address filter', there are radio buttons for 'On' (selected) and 'Off'. Below this is the 'Add clients:' section with a text input field for MAC addresses (format: . : . : . : . : . :) and an 'Add' button. Below that is the 'Known wireless clients:' section with a dropdown menu and an 'Add' button. At the bottom are 'OK' and 'Cancel' buttons.

The default setting for access control is disabled. This means that all PCs that use the correct **SSID** can log in.

Access control is based on the **MAC address** of the PCs' network adapters.

- ➔ Activate access control via the **On** option in the field **MAC address filter**.

Entering PCs manually:

- ➔ Enter the required PCs with **MAC address** and **Device name** in the appropriate fields.
- ➔ Click on **Add** to add the entry to the list.

Configuring the Advanced Settings

- ➔ Click on **Delete** to delete the entry from the list.
- ➔ Click on **OK** to apply the settings.

Selecting from the list of known PCs

- ➔ From the **Known wireless clients** list (all PCs that currently have access to the Gigaset SE361 WLAN), select the PC you want to add to the access control list.
- ➔ Click on **Add** to add the entry to the list.
- ➔ Click on **OK** to apply the settings.

Note:

If you activate MAC access control, you must at least enter the PC from which you are configuring the Gigaset SE361 WLAN. If you fail to do this, you will no longer be able to access the user interface and an error message will be shown.

If, by mistake, you have denied all PCs access to the Gigaset SE361 WLAN you have two options:

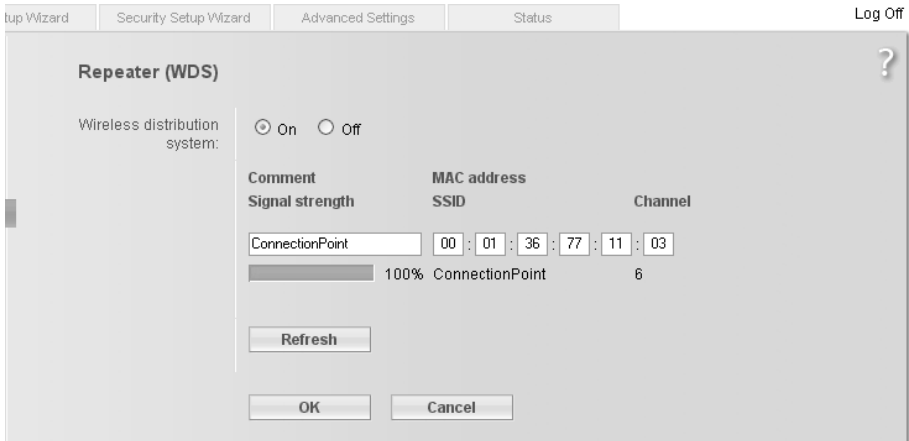
- ◆ You can reset the Gigaset SE361 WLAN to the factory settings (see page 18).
- ◆ You can connect a PC to the Gigaset SE361 WLAN using one of the LAN connections. As MAC access control only applies to PCs that are connected wirelessly, you can use this PC to change the configuration.

Repeater function (WDS)

If you want to use a repeater in your wireless network to extend the range, you must activate the Wireless Distribution System (WDS) function. A repeater installed at the range limit of the access point ensures that the data is forwarded between clients in the access points' wireless network and clients in its own radio coverage area. Repeaters and access points form a common wireless network in which all clients can move about freely. Clients automatically set up a connection to the next access point / repeater ([Roaming](#)). You must determine for security purposes which access points / repeaters are to form a common wireless network.

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

- ➔ Next to **Wireless distribution system**, select the **On** option to activate WDS.



Note:

In order to use WDS (Wireless Distribution System), you have to change your wireless encryption setting. Only WEP is supported for WDS. If WPA2-PSK / WPA-PSK is selected as encryption method an error message is output.

If WDS is activated the page shows the WDS client with the highest signal strength (access point or repeater) to which your Gigaset SE361 WLAN is able to connect.

The following information is displayed:

- the MAC address of the repeater is shown in the **MAC address** field.
- the SSID is shown in the **SSID** field.
- the radio channel used for data transfer is shown in the **Channel** field.
- the **Signal strength** shows the strength of the connection to the repeater in percentage terms.

- ➔ Enter a description that will help you to identify different access points / repeaters in the **Comment** field.
- ➔ To update the display click on **Refresh**. If there is a access point / repeater with higher signal strength close to your Gigaset SE361 WLAN, it is displayed.
- ➔ Apply the settings by clicking **OK**.

Administration and status information

The Gigaset SE361 WLAN user interface includes several helpful functions for administration. You can

- ◆ open an Internet connection manually (see below),
- ◆ select regional options (see page 65),
- ◆ change the system password (see page 66),
- ◆ set up remote administration (see page 67),
- ◆ save, and if necessary restore, configuration data (see page 68),
- ◆ reset the Gigaset SE361 WLAN to the factory settings (see page 69),
- ◆ reboot the device (see page 69),
- ◆ update the firmware (see page 69),
- ◆ view information about the configuration and status of the Gigaset SE361 WLAN (see page 71).

Connecting to the Internet manually

You can set up a manual connection to the [Internet](#).

To open or close an Internet connection manually:

- ➔ Open the Gigaset SE361 WLAN start screen as described on page 24.

If you have already started the configuration environment, click on the **Home** tab at the top left of the window.

If you have not yet started the configuration environment, start it now and log on.

- ➔ Click on **Connect** to open a connection to the Internet.

Regional Options

To operate your Gigaset SE361 WLAN you can select the location, time zone, and the format for entering the date and time, as well as configure the application for a time server for Internet time.

- ➔ In the **Advanced Settings – Administration** menu, select the entry **Regional Options**.

The screenshot shows the 'Regional Options' dialog box with the following fields and options:

- Country:** United Kingdom (dropdown menu)
- Time zone:** (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
- Automatically adjust clock for daylight saving changes:** On Off
- Date format:** dd.mm.yyyy (dropdown menu)
- Time format:** hh:mm:ss (dropdown menu)
- Internet Time**
 - System time:** Not Available
 - Last synchronization with time server:** 10.07.2006, 10:55:12
 - Use custom time servers:** On Off

Buttons: OK, Cancel

- ➔ Select the country in which you are currently located from the list. You can set the clock to change automatically to summer time and/or to the **Time zone** as you wish.
- ➔ Select the required option and/or select the **Time zone** for your location.
- ➔ Select the required format for entering the date and time from the **Date format** and **Time format** lists respectively.

Internet Time

The **System time** for your 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 wish to use your own time server, select the **On** option next to the **Use custom time servers** field.
- ➔ Enter the Internet addresses for the time servers in the **Preferred time server** and **Alternate time server** fields respectively.
- ➔ Click on **OK** to apply the settings.

System Password

You can assign a System Password for the configuration environment of your Gigaset SE361 WLAN, and specify the period after which a session is to end automatically if no further entry is made.

- ➔ In the **Administration** menu, select **System Password**.

The screenshot shows a dialog box titled "System Password" with a question mark icon in the top right corner. The dialog has four tabs at the top: "Setup Wizard", "Security Setup Wizard", "Advanced Settings" (which is selected), and "Status". In the top right corner of the dialog, there is a "Log Off" button. The main area contains the following fields and controls:

- "Current password:" followed by a text input field.
- "New password:" followed by a text input field.
- "Confirm new password:" followed by a text input field.
- "Idle time before log off:" followed by a text input field containing "10" and the label "minutes(1 - 99)".
- At the bottom, there are two buttons: "OK" and "Cancel".

After installation, the configuration of the Gigaset SE361 WLAN is protected by default with the System Password **admin**. To prevent unauthorised changes to the configuration, you should set your own System Password and change it from time to time.

- ➔ If you have already set a System Password, enter the old System Password in the **Current password** field.
- ➔ Enter a new password in the **New password** field, and repeat it in the **Confirm new password** field.

The password may contain up to 32 characters. The password is case sensitive. Avoid proper names and all too obvious words. Use a combination of letters, numbers and special characters.

Note:

If you ever forget your System Password you will have to reset your Gigaset SE361 WLAN (see page 18). Please bear in mind that this will restore **all** the settings to the factory configuration. No System Password will be active either.

Setting Idle time before log off

- ➔ Enter the period in minutes after which the configuration program is to be aborted if no entry is made. The default setting is 10 minutes. If you enter the value 0, the program will never be aborted automatically.
- ➔ Click on **OK** to apply the settings.

Setting up Remote Management

Remote Management enables a PC that is not on your local network to be used to configure the Gigaset SE361 WLAN with a standard Web browser. You can permit Remote Management for one particular PC or for any PCs.

For security reasons this function is only available if you have previously changed the system password for your device (see page 66).

- ➔ In the **Administration** menu, select **System Management**.

The screenshot shows the 'System Management' configuration window. At the top, there are tabs for 'up Wizard', 'Security Setup Wizard', 'Advanced Settings', and 'Status'. The 'Advanced Settings' tab is selected. The window title is 'System Management'. On the right side, there is a 'Log Off' button and a help icon (?). The main content area contains the following settings:

- Remote management:** Radio buttons for 'On' (selected) and 'Off'.
- Port:** A text input field containing '8080'.
- Allowed connections:** A dropdown menu with the text 'Specify IP address range'.
- First IP address:** Four input fields containing '0', '0', '0', and '0' separated by dots.
- Last IP address:** Four input fields containing '0', '0', '0', and '0' separated by dots.

At the bottom of the window, there are two buttons: 'OK' and 'Cancel'.

- ➔ Select the **On** option for **Remote Management** if you wish to allow Remote Management.

You can start remote administration by entering the public IP address in your Internet browser. As many Internet providers change this address each time someone dials in, it is also advisable to use dynamic DNS (see page 52).

- ➔ You can change the **Port** via which you access the configuration program from the Internet, for example in order to hide and protect the configuration program against unauthorised access.
- ➔ **Allowed connections:** You can specify one particular PC or all PCs in a specific IP address block for Remote Management, or permit this function for any PCs. Select the required option from the list.

Note:

If you permit any PCs, then anyone who finds out your password can access this user interface and therefore also your network! If this option is needed, you should always only activate it for a short time.

Remote Management for one particular PC:

➔ In the **IP address** field, enter the IP address of the PC that is to have access to the user interface of the Gigaset SE361 WLAN from outside your local network.

Remote Management for PCs in a specific IP address block:

➔ In the **First IP address** and **Last IP address** fields, enter the IP address block of the PCs that are to have access to the user interface of the Gigaset SE361 WLAN from outside your local network.

Note:

- ◆ The Internet provider might assign the IP address to the PC dynamically. This can then change the IP address. Make sure that the PC that is to access the router from the Internet always has the same IP address.
- ◆ To access the configuration environment via Remote Management, you must enter the **Public IP address** of the Gigaset SE361 WLAN to be maintained in the following format in the browser: **http://x.x.x.x:8080** (x.x.x.x stands for the public IP address of the Gigaset SE361 WLAN).

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

Saving and restoring a configuration

Once you have configured your Gigaset SE361 WLAN, it is advisable to back up the settings. Then you can restore them at any time, should they be accidentally deleted or overwritten.

You can also reset the configuration to the factory settings. You should always do this before passing your device on to others.

- ◆ In the **Administration** menu, select **Save & Restore**.

Saving configuration data

➔ Activate the **Save configuration** option.

This opens a file selection window where you can specify the file you wish to store in the backup file.

➔ On your local PC select a directory to which you wish to store the configuration file, and enter a name for the file.

➔ Click on **Save**.

Once the procedure has been completed, the current configuration data will have been saved to the specified file.

Restoring backups

- ➔ Activate the **Restore configuration** option.
- ➔ In your file system, select the backup file with which you wish to restore the configuration.
- ➔ Confirm the action in the dialog screen that opens by clicking on **OK**.
- ➔ Click on **OK**. The configuration will now be updated.

Resetting to the factory settings

You can reset the Gigaset SE361 WLAN to the factory settings. You should do this before making the device available to others or exchanging it through your dealer. If you do not, unauthorised persons will be able to use your Internet access data at your expense.

- ➔ Select the option **Reset configuration to factory default settings** and click on **OK**.
- ➔ Confirm the action in the dialogue screen that opens by clicking on **OK**.

Note:

You can restart your Gigaset SE361 WLAN if it no longer functions correctly. It should then be ready for use again (see page 18).

Please bear in mind that when the device is fully reset **all** configuration settings will return to the factory settings. This means that you will have to completely reconfigure the Gigaset SE361 WLAN.

Reboot

You can restart your Gigaset SE361 WLAN if it no longer functions correctly. It should then be ready for use again.

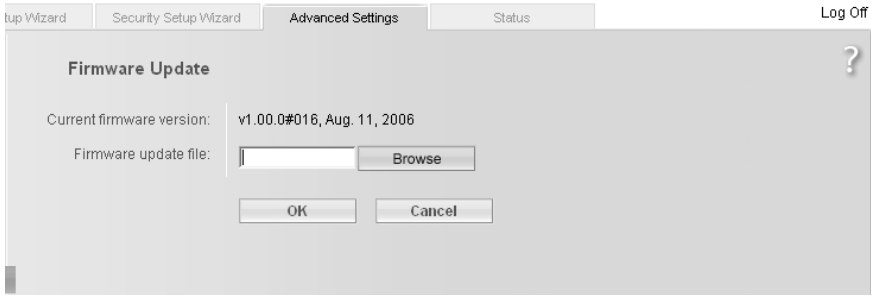
- ➔ In the **Administration** menu, select **Reboot**.
- ➔ Click on **OK** to restart the device.

Updating the firmware

When Siemens or your Internet provider makes a new version of the firmware available, you can update the firmware for your Gigaset SE361 WLAN. To do this you must first download the new firmware onto your PC.

Then proceed as follows:

- ➔ Close down all network activities on your local network.
- ➔ In the **Administration** menu, select **Firmware Update**.



The version of the firmware currently running on your device is displayed in the line **Current firmware version**.

- ➔ Select the **Firmware update target** you want to download. **Bootcode** or **Firmware**:
If new versions of both files are available, first update the boot code.
- ➔ In the **Firmware update file** field, enter the file with the new firmware you have downloaded from the Internet.
- ➔ Click on **OK**.

The firmware will now be updated.

Note:

Do not switch off your Gigaset SE361 WLAN during the updating procedure. Updating can take several minutes.

After successful updating, the device is automatically rebooted. This will take some time. After successful updating, the login screen appears again.

Note:

You can check whether the upgrade process was successful in the **Status** menu on the start screen (see page 71). This displays the current firmware version running on the Gigaset SE361 WLAN.

Status information

You can view information about the configuration and status of the Gigaset SE361 WLAN in the Gigaset SE361 WLAN's **Status** menu. On the first screen you will see an overview of the status of the Internet connection, the local and wireless networks, and the device.

For detailed information you can view the following status screens:

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

To display a status screen, proceed as follows:

- ➔ Select **Status** on the start screen.
- ➔ Select the entry with the information you require.

Overview

The first screen gives you an overview of the current operating status and most important data for your device.

Internet

- ◆ **Connection status**

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

- ◆ **IP address**

The public IP address of your device.

Local Network

- ◆ **IP address**

The local IP address of your device.

- ◆ **DHCP Server**

The status of the DHCP server for your device and, if activated, the number of clients in your network to which IP addresses have been assigned.

Wireless Network

- ◆ **Status**

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

- ◆ **SSID**

The identifier for your wireless network.

Status information

Device

◆ **System time**

Your device's system time.

◆ **Firmware version**

The version of the firmware currently installed in your device.

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

Security

On the **Security** screen in the **Status** menu you will see information about possible security risks for your device and your network.

◆ **System password not changed**

Your device's configuration program is not effectively protected against unauthorised access as you have not changed the password since setup. The section entitled "System Password" on page 66 describes how to avoid this security risk.

◆ **Identification of your wireless network visible or not changed**

Unauthorised users can also find your wireless network easily as you have not changed the ID for your wireless network (SSID) since setup and have not deactivated SSID broadcast. The section entitled "Configuration for wireless connections" on page 56 describes how to avoid this security risk.

◆ **Encryption for your wireless network not activated**

None of the data in your wireless network is encrypted when transmitted and can therefore easily be intercepted. Unauthorised users can also easily access your network, your PCs and your Internet connection by this means. The section entitled "Setting wireless security" on page 58 describes how to avoid this security risk.

◆ **Firewall for your Internet connection turned off**

Your network is not protected against hackers who gain unauthorised access via the Internet. The section entitled "Firewall" on page 45 describes how to avoid this security risk.

◆ **Address translation for your Internet connection turned off**

The clients in your network are not protected against unauthorised access via the Internet. The section entitled "Setting up the NAT function" on page 47 describes how to avoid this security risk.

◆ **One or more of your local clients directly exposed to the Internet**

One or more clients in your network are directly visible to the Internet as exposed hosts and therefore particularly exposed to risk (e.g. hacker attacks). You should only activate this function where it is absolutely necessary (e.g. to operate a Web server) and where other functions (e.g. port forwarding) are not adequate. In this case you should take appropriate measures on the clients concerned. The section entitled "Opening the firewall for a selected PC (Exposed Host)" on page 51 describes how to avoid this security risk.

◆ **Remote management enabled**

Any user, including unauthorised users, who gains knowledge of the system password for your device can access your device's configuration program via the Internet. The section entitled "Setting up Remote Management" on page 67 describes how to avoid this security risk.

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

Internet

On the **Internet** screen in the **Status** menu you will find information about the status of your device's Internet connection.

◆ **Connection status**

Shows the status of the connection to the Internet and, if connected, the duration of the connection. If you have set **Connect on demand** or **Connect manually** as the connection mode (see page 41), you can **Connect** or **Disconnect** the connection to the Internet manually here.

◆ **MAC address**

Shows the public MAC address of your device.

◆ **PPPoE pass-through**

Shows the status of PPPoE pass-through for your DSL or cable connection for establishing Internet connections straight from a PC to your network.

◆ **Address Translation (NAT)**

– **Status**

Shows the status of NAT (Network Address Translation) for your Internet connection.

– **NAT table**

Shows the number of entries currently existing in the NAT table.

Click on **Empty** to delete all currently existing entries in the NAT table.

◆ **Dynamic DNS**

– **Dynamic DNS**

Shows the status of dynamic DNS for your Internet connection.

– **Domain name**

Shows the domain name set for dynamic DNS.

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

Local Network

On the **Local Network** screen in the **Status** menu you will find information about the settings for your local network.

- ◆ **IP address**
Shows the local IP address of your device.
 - ◆ **Subnet mask**
Shows the subnet mask used in the local network.
 - ◆ **MAC address**
Shows the local MAC address of your device for wired data transmission.
 - ◆ **DHCP Server**
 - **Status**
Shows the status of the DHCP server for your device for automatic assignment of IP addresses to clients in your local network.
 - ◆ **DHCP clients**
Shows all clients in your network that have been assigned an IP address. The **Host name** and the **MAC address** of each client are listed for identification. You are also given information about the **IP address** assigned to each client as well as the remaining **Lease time** for the IP address before the client is assigned a new address by the DHCP server.
- ➔ Click on **Refresh** to refresh this screen and update the displayed data.

Wireless Network

On the **Wireless Network** screen in the **Status** menu you will find information about the settings for your wireless network.

- ◆ **Status**
Shows the status of the connection between your device and the wireless network.
- ◆ **SSID**
Shows the identity of your wireless network.
- ◆ **Channel**
Shows the radio channel currently used for transmitting data within your wireless network.
- ◆ **MAC address**
Shows the local MAC address of your device for wireless data transmission.
- ◆ **Wireless clients**
Shows all clients in the wireless network that are currently connected to your device. The **Host name**, the **MAC address** and the **IP address** of each client are listed for identification purposes. You will also see information about the **Uptime** to date of the current connection for each client in your wireless network.

◆ **Repeater (WDS)**– **Status**

Shows the status of the WDS (Wireless Distribution System) used in your wireless network to increase its range.

– **WDS links**

Shows the currently existing number of connections to other access points or repeaters in your wireless network.

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

Device

On the **Device** screen in the **Status** menu you will find information about the most important data for your device.

◆ **System uptime**

Shows your device's operating time since the last system start.

◆ **System time**

Shows the system time for your device.

◆ **Firmware version**

Shows the version of the firmware currently installed in your device.

◆ **Bootcode version**

Shows the version of the boot code currently installed in your device.

◆ **Wireless driver version**

Shows the version of the WLAN driver currently installed in your device.

◆ **System Log**

The system log can give you important information about the functioning of your device and possible problems.

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

Configuring the local network

Once you have set up the hardware and connected all the devices, you must configure the network settings for all the PCs that are to communicate with each other via the Gigaset SE361 WLAN.

In this section we assume that you will use the Gigaset SE361 WLAN's [DHCP](#) service. This means that IP addresses are automatically assigned to the PCs ([Dynamic IP addresses](#)). This is also the device's default setting.

In many cases, however, it is advisable to assign [Static IP addresses](#), for example if you wish to run a wireless network in [Ad-hoc mode](#). How you configure dynamic address assignment on the Gigaset SE361 WLAN is described in the section entitled "LAN configuration" on page 54.

If your network is already set up you can read on from "The user interface" on page 24.

The network configuration varies depending on the Windows operating system you are using. You will find the description for Windows XP on and after page 76, and for Windows 2000 on and after page 84.

Have your Windows Installation CD to hand. You may be prompted to insert it.

Note:

The Windows user interfaces shown in this guide may differ from the one on your screen as a result of individual settings, different versions of Windows or Service Packs. The illustrations always reflect the state after immediate installation.

Network configuration with Windows XP

To integrate a PC with Windows XP into a network that is configured with a Gigaset SE361 WLAN you must carry out the following steps:

1. Configure the network (see below)
2. Select a computer name and workgroup (see page 79)
3. Check the network settings and complete the installation procedure (see page 79)
4. Make the TCP/IP settings (see page 80)
5. Deactivate the http proxy (see page 82)
6. Configure the popup blocker (see page 82)
7. Synchronising the TCP/IP settings with the Gigaset SE361 WLAN (page 83)

Note:

The name of the menu items may differ slightly from one version of Windows XP to another. However, the configuration settings described below apply generally.

Configuring the network

Note:

Make sure that the *Use Windows to configure the settings* function is deactivated.

This can be done as follows:

- ➔ Click on **Start – Settings – Control Panel – Network Connections – LAN or High-speed Internet**.
A window opens showing the properties of this connection.
In some versions of Windows XP, you open this window by right-clicking the Properties menu item.
- ➔ On the **General** tab, click on the **Properties** button.
On the **Wireless Networks** tab, deactivate the option **Use Windows to configure the settings**.

Configuring the network in this case means selecting **Internet Connection** as the connection method. You can do this with the network wizard.

- ➔ Click on **Start - Control Panel**.
- ➔ Open the **Network Connections** screen (by double clicking or by using the right mouse key).
- ➔ Under **Network Tasks** select the option **Set up or modify home network or small office network**.

The network installation wizard is started.

- ➔ Skip the welcome screen and the checklist by clicking twice on **Next**.

You will be prompted to select a connection method.

- ➔ Select **Other Method** and confirm with **Next**.

You will now see a screen listing various connection methods.



- ➔ Select ***This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer***, and click on ***Next***.
- ➔ In the next window select your network adapter and click on ***Next***.
- ➔ Skip the message ***This network configuration is not advisable*** by clicking on ***Next***.

Selecting a computer name and workgroup

You now have to specify a name for the PC and assign it to a workgroup.

- ➔ Enter the name the PC is to appear under in the network. This name must be unique within the network. You can complete the **Computer Description** field or leave it empty. Then click on **Next**.
- ➔ Enter a name for the workgroup the PC is to belong to. This name must be identical for all the PCs in the network. Then continue by clicking on **Next**.

Checking the network settings and completing the installation procedure

You will now see a screen in which you can check the settings you have made and make any changes you want.

- ➔ Click on **Back** if you want to make any changes or click on **Next** if you want to leave them unchanged.

If you do not want to install any more PCs:

- ➔ Select **Only finish the wizard as it is not run on other computers**, and confirm by clicking twice on **Next**.
- ➔ Answer the question **Do you want to restart your computer now?** with **Yes**.

If you want to set up a network on other PCs with Windows XP, you can now create a network installation disk.

- ➔ Select **Create a network installation disk**, and click on **Next**.
- ➔ Follow the on-screen instructions and insert a disk. The necessary data will now be copied. Finally, label the disk **Network installation**.
- ➔ Confirm the next two screens with **Next** and complete the installation procedure by rebooting the PC.

After the reboot your home network will have been installed.

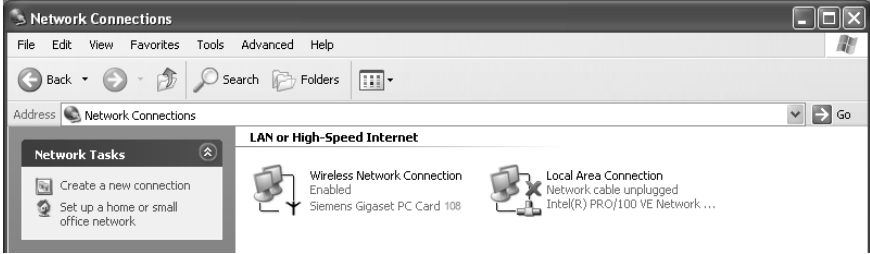
To set up the network on the other PCs with the same settings, insert the disk in the drive and run **Netsetup** with a double click.

Configuring the local network

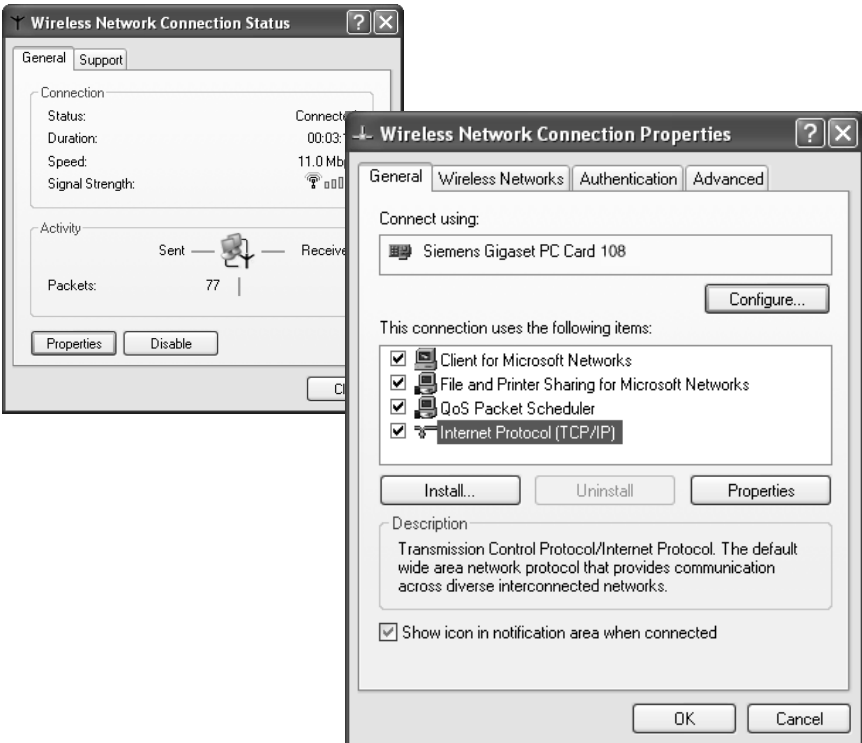
TCP/IP settings

The [TCP/IP Protocol](#) requires certain settings which you should now make or check so that it can function smoothly.

- ➔ Click on **Start – Settings – Control Panel**.
- ➔ Select **Network Connections**.

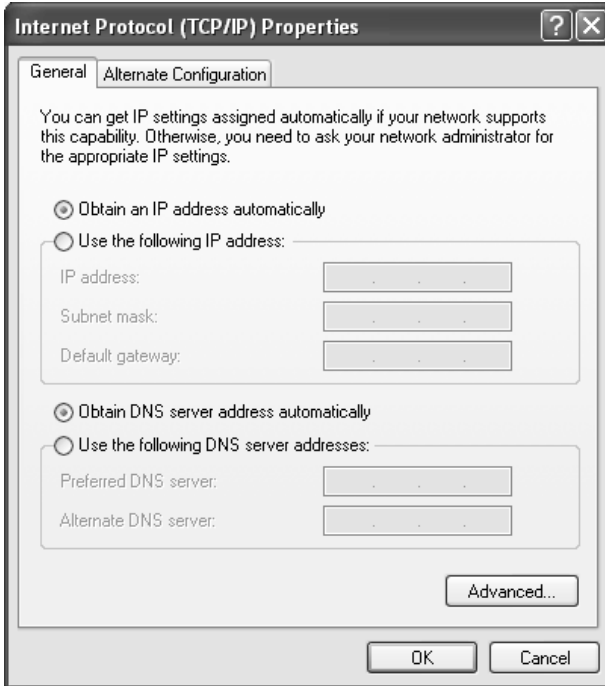


- ➔ Double-click the LAN connection via which you are connected to the Gigaset SE361 WLAN.



- ➔ Click on **Properties**.

- Select **Internet Protocol (TCP/IP)** and click on **Properties**.



- If the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options have already been activated, your PC is already configured for DHCP. Click on **Cancel** and close the following windows with **OK** to save your network configuration.
- If the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options have not yet been activated, activate them now and click **OK**. Close the next windows.

Configuring the local network

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 SE361 WLAN's configuration screens.

The following section describes the procedure for Internet Explorer and Mozilla Firefox. First determine which browser you are using and then follow the appropriate steps.

Internet Explorer

- ➔ Open Internet Explorer. Click on **Tools – Internet Options**.
- ➔ In the **Internet Options** window click on the **Connections** tab.
- ➔ Click on **Settings**.
- ➔ Deactivate all options in the **Settings for Local Network (LAN)** window.
- ➔ Click on **OK** and then **OK** again to close the **Internet Options** window.

Mozilla Firefox

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

Configuring the popup blocker

You must allow popups for the configuration program in order to start it.

Internet Explorer

If you are working with Windows XP Service Pack 2, popups are blocked by default. Carry out the following steps:

- ➔ Right-click on the browser information bar.
- ➔ Select **Allow popups from this screen**.
- ➔ Confirm the dialogue window by clicking on **OK**.

The configuration screens for the Gigaset SE361 WLAN are now allowed as popups.

You can make additional settings for popups within Internet Explorer

- ◆ via the **Tools – Popup Manager** menu item or
- ◆ via **Tools – Internet Options** on the **Privacy** tab.

Mozilla Firefox

Popups are blocked by default. Carry out the following steps:

- ➔ Open Mozilla Firefox. Click on **Tools** and then on **Settings**.
- ➔ On the **Settings** screen, click on the **Web Features** tab.

- ➔ Deactivate the option **Block Popup Windows** on the **Web Features** screen.
- ➔ Click on **OK** to finish.

Synchronising the TCP/IP settings with the Gigaset SE361 WLAN

You have now configured your PC so that it is ready to be connected to the Gigaset SE361 WLAN. You now have to release the old TCP/IP settings and synchronise them with the settings of your Gigaset SE361 WLAN.

- ➔ On the Windows Desktop, click on **Start – Programs – Accessories – Command prompt**.
- ➔ Then enter the **ipconfig /release** command and press the ENTER key.

```

C:\WINDOWS\System32\cmd.exe
C:\>ipconfig /release
Windows IP Configuration

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . : 
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected

C:\>
    
```

- ➔ Then enter the **ipconfig /renew** command and press the ENTER key.

```

C:\WINDOWS\System32\cmd.exe
C:\>ipconfig /renew
Windows IP Configuration

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . : 
    IP Address. . . . . : 192.168.2.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected

C:\>
    
```

If the default IP address (192.168.2.1) of the Gigaset SE361 WLAN was not changed, the IP address should now read 192.168.2.x (with x being a number between 2 and 255). The **Subnet Mask** must always be 255.255.255.0 and the **Standard Gateway** must have the IP address of the Gigaset SE361 WLAN (192.168.2.1). These values confirm that your Gigaset SE361 WLAN is working.

- ➔ Enter **exit** and press the ENTER key to close the **Command prompt** window.

Network configuration with Windows 2000

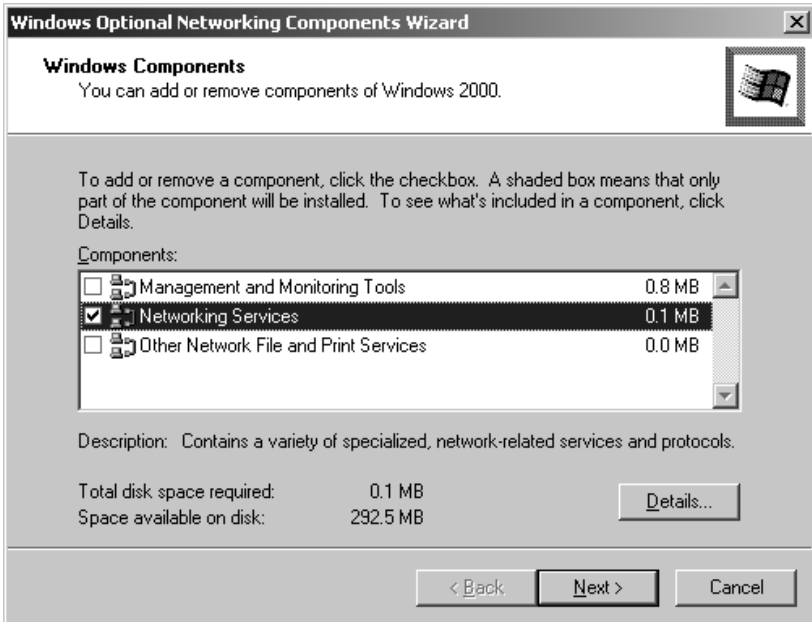
To integrate a PC with Windows 2000 into a network that is configured with a Gigaset SE361 WLAN, you must carry out the following steps:

1. Install the network services (see below).
2. Select a computer name and workgroup (see page 85).
3. Install the TCP/IP protocol (see page 86).
4. Make TCP/IP protocol settings (see page 88).
5. Deactivate the http proxy (see page 90).
6. Deactivate the popup blocker (only on Mozilla Firefox, see page 90)
7. Synchronise the TCP/IP settings with the Gigaset SE361 WLAN (see page 91).

Installing network services

You must install the network services so that the PCs in your network can access shared resources. This is done as follows:

- ➔ Click on **Start – Settings – Control Panel**.
- ➔ Double-click on the **Network and Dial-up Connections** icon.
- ➔ In the left-hand pane click on **Add Network Components**.



- ➔ Now select **Network Services** and click on **Next**.
You will now be prompted to insert the Windows installation CD.

- ➔ Insert the WIN2000 CD and click on **OK** to install all the required components.

Selecting a computer name and workgroup

You now have to specify a name for the PC and define the workgroup to which it is to be assigned.

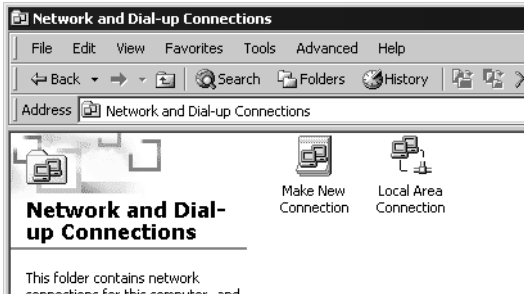
- ➔ In the left-hand pane click on **Network Identification** and then on **Properties**.
- ➔ In the **Computer Name** field, enter the name the PC is to appear under in the network. This name must be unique within the network.
- ➔ In the **Workgroup** field, enter a name for the workgroup. This name must be identical for all the PCs in the network.
- ➔ Confirm this with **OK**.

Configuring the local network

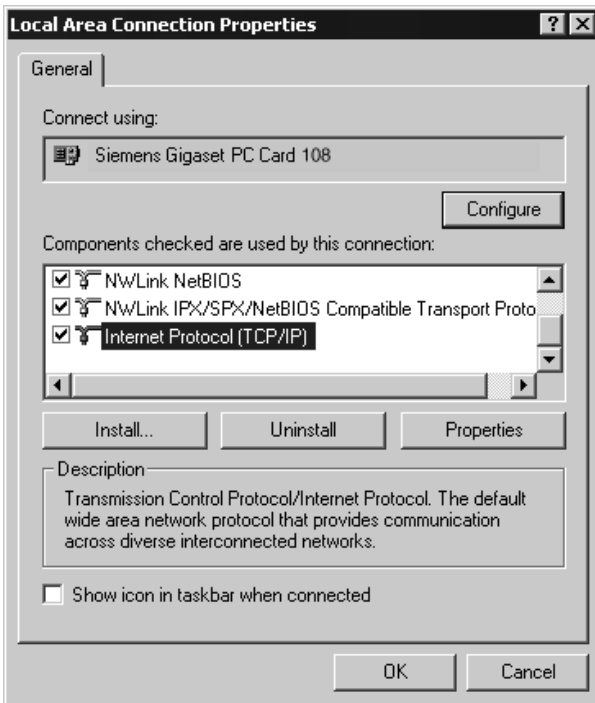
Installing the TCP/IP protocol

The [TCP/IP](#) protocol ensures that the PCs in the network can communicate with each other. You now have to install this [Protocol](#).

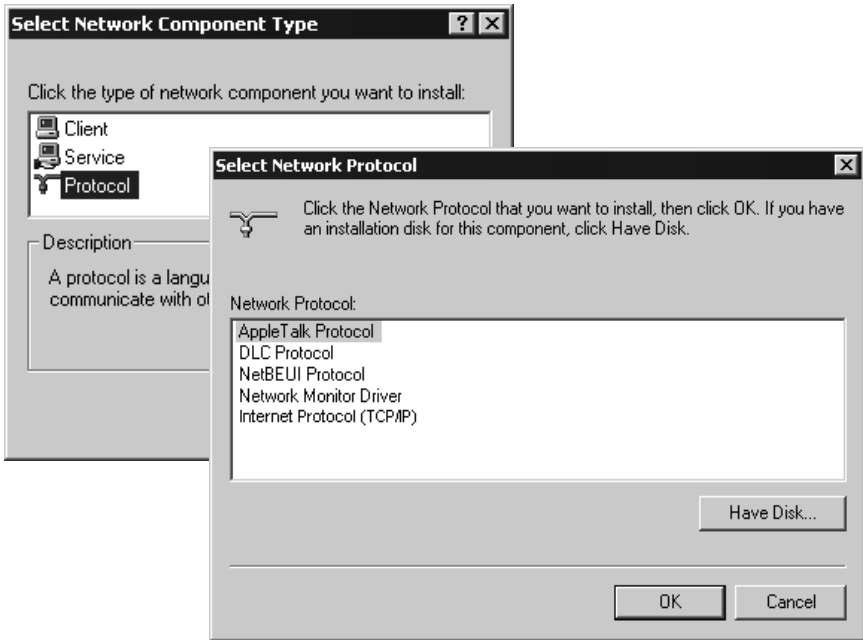
→ Right click to open the **LAN Connection**.



→ In the next window click on **Properties**.



→ Click on **Install**.

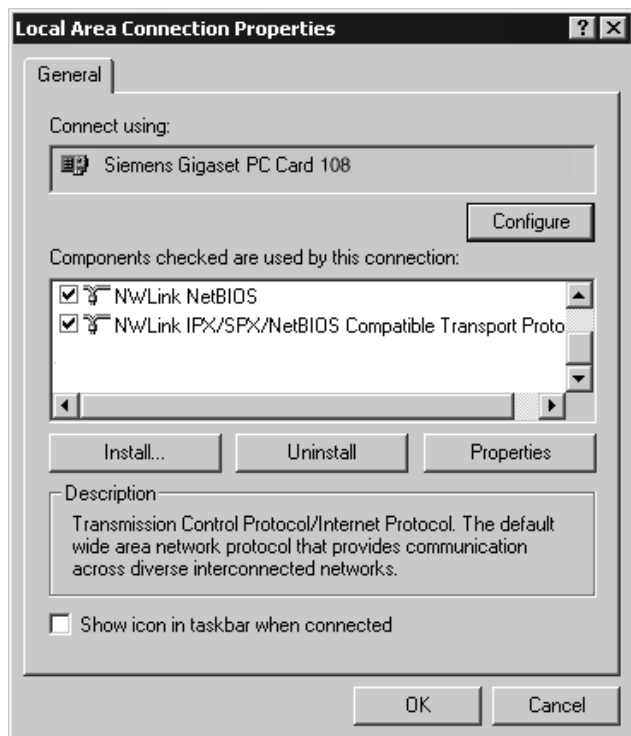


- ➔ Select **Protocol** and click on **Add**.
- ➔ In the **Network Protocol** list, select **Internet Protocol (TCP/IP)**.
- ➔ Click on **OK**.

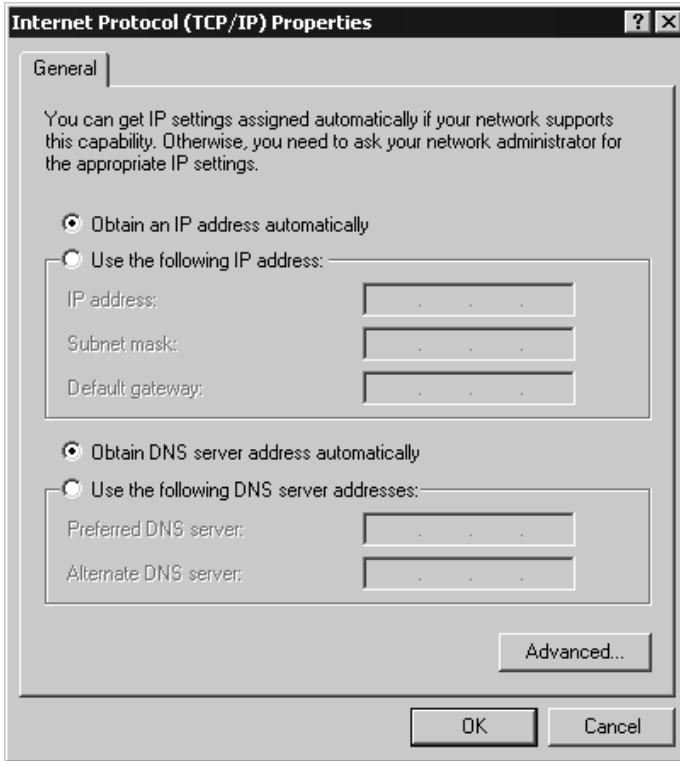
The TCP/IP protocol is now shown in the **LAN Connection Properties** window.

TCP/IP settings

The TCP/IP protocol requires certain settings which you must now make or check so that it can function smoothly.



- ➔ Select **Internet Protocol (TCP/IP)** and click on **Properties**.



- ➔ If the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options have already been activated, your PC is already configured for DHCP. Click on **Cancel** and close the next windows with **OK** to save your network configuration.
- ➔ If the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options have not yet been activated, activate them now and click on **OK**. Close the next windows.

Configuring the local network

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 read your Gigaset SE361 WLAN's configuration screens.

The following section describes the procedure for Internet Explorer and Mozilla Firefox. First determine which browser you are using and then follow the appropriate steps.

Internet Explorer

- ➔ Open Internet Explorer. Click on **Tools – Internet Options**.
- ➔ On the **Internet Options** screen click on the **Connections** tab.
- ➔ Click on **LAN Settings**.
- ➔ Deactivate all options in the **Settings for Local Network (LAN)** window.
- ➔ Click on **OK** and then **OK** again to close the **Internet Options** screen.

Mozilla Firefox

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

Configuring the popup blocker

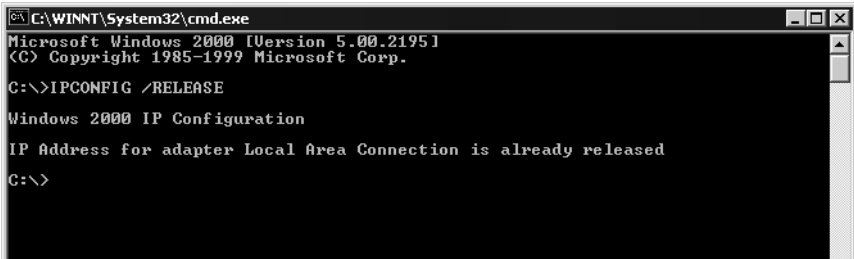
Popups are blocked by default for Mozilla Firefox. If you are using the Mozilla Firefox browser, you must allow popups for the configuration program in order to start it. Carry out the following steps:

- ➔ Open Mozilla Firefox. Click on **Tools** and then on **Settings**.
- ➔ On the **Settings** screen, click on the **Web Features** tab.
- ➔ Deactivate the option **Block Popup Windows** on the **Web Features** screen.
- ➔ Click on **OK** to finish.

Synchronising the TCP/IP settings with the Gigaset SE361 WLAN

You have now configured your PC so that it is ready to be connected to the Gigaset SE361 WLAN. You now have to release the old TCP/IP settings and synchronise them with the settings of your Gigaset SE361 WLAN.

- ➔ On the Windows Desktop, click on **Start – Programs – Accessories – Command prompt**.
- ➔ Then enter the `ipconfig /release` command and press the ENTER key.



```

C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

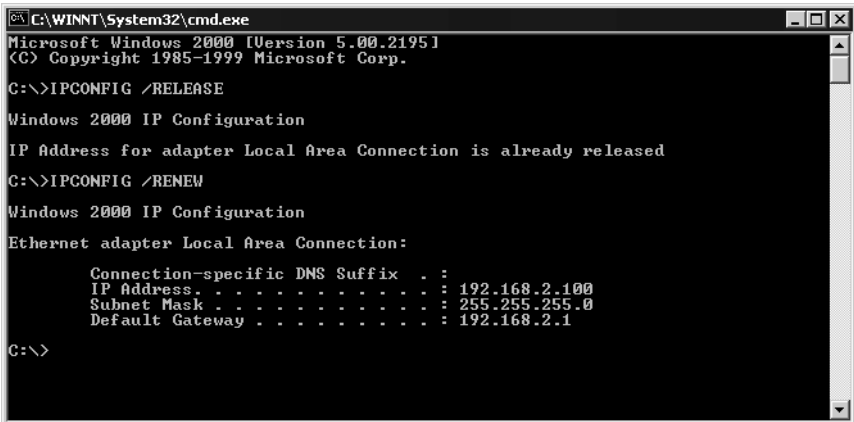
C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP Address for adapter Local Area Connection is already released

C:\>
  
```

- ➔ Then enter the `ipconfig /renew` command and press the ENTER key.



```

C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP Address for adapter Local Area Connection is already released

C:\>IPCONFIG /RENEW

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

C:\>
  
```

If the default IP address (192.168.2.1) of the Gigaset SE361 WLAN has not been changed, the IP address should now read 192.168.2.x (with x being a number between 2 and 255). The **Subnet Mask** must always be 255.255.255.0 and the **Standard Gateway** must have the IP address of the Gigaset SE361 WLAN (192.168.2.1). These values confirm that your Gigaset SE361 WLAN is working.

- ➔ Enter `exit` and press the ENTER key.

Checking the connection to the Gigaset SE361 WLAN

Once the network has been set up on your PC, you can check whether the PC is correctly connected to the Gigaset SE361 WLAN. This can be done as follows:

- ➔ Open **Command prompt**. To do this, click on **Start – Programs – Command prompt**.
- ➔ Enter the command `ping 192.168.2.1`.

Note:

192.168.2.1 is the default IP address for the Gigaset SE361 WLAN. If the IP address has been changed, enter the new IP address.

The `ping` command sends data packets to the Gigaset SE361 WLAN with the specified IP address and checks whether the router responds. If this is the case, the command presents statistics about the connection, e.g. how many data packets were sent, how many received, how long the transfer took, etc. If you can see this information, then the connection to the router is functioning correctly.

If the command does not return any statistics but ends with a time-out, this means that the components cannot communicate with each other. Check the following points:

1. Is the Ethernet cable between the Gigaset SE361 WLAN and the PC correctly connected or is there a wireless connection via a wireless network adapter?

The LED for the LAN connections on the Gigaset SE361 WLAN and the link display for the network card in your PC must light up. For wireless connections the Gigaset WLAN Adapter Monitor must display connection information.

2. Is TCP/IP configured correctly on your PC?

If the Gigaset SE361 WLAN has the IP address 192.168.2.1, your PC's IP address must be between 192.168.2.2 and 192.168.2.255. The default gateway must have the address 192.168.2.1.

3. Does the IP address match the defined subnet mask?

As the [Subnet mask](#) for the Gigaset SE361 WLAN is set to 255.255.255.0 the PC's IP address may differ from the routers' IP address only in the last address field.

If you can successfully address the Gigaset SE361 WLAN with the `ping` command, then the PC has been configured correctly.

Appendix

Troubleshooting

This section describes common problems and their solutions. The Gigaset SE361 WLAN is easy to monitor thanks to its LED displays. Problems can be quickly identified. If you cannot solve connection problems after checking the LED displays, please consult the other sections shown in the following table.

Symptom	Possible cause and remedial actions
Power lamp 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 SE361 WLAN and a power outlet. ➔ Check whether the power outlet and the mains adapter are working properly. If the mains adapter is not working properly, contact our customer care unit (see page 99).
The LAN LED on a connected device does not light up.	<p>No LAN connection.</p> <ul style="list-style-type: none"> ➔ Make sure that the connected device is switched 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 (<100 m). ➔ Check that the network card on the connected device and the cable connections 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, then 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 remedial actions
<p>You cannot connect to the Internet.</p>	<p>➔ Check whether the Connect on Demand option is deactivated. In this case, connections cannot be opened automatically.</p> <p>➔ Select Connect on Demand. Remember that this setting may lead to higher costs if you are billed on the time you use.</p> <p>➔ The connection may have been terminated manually with the Connect on Demand option selected.</p> <ul style="list-style-type: none"> – Open the connection again manually using the Connect button or – restart the Gigaset SE361 WLAN. <p>In both cases, the Connect on Demand setting will be active again.</p> <p>➔ Make sure that you have entered the access data supplied by your service provider correctly.</p> <p>➔ There may be a problem at the service provider end. Get in touch with your service provider.</p>
<p>You cannot open a connection from a wireless device to the Gigaset SE361 WLAN.</p>	<p>The wireless network adapter is not using the correct SSID.</p> <p>➔ Change the SSID on the network adapter.</p> <p>Either encryption is enabled on the Gigaset SE361 WLAN but not on the wireless network adapter, or it is not using the correct key or is using another type of encryption.</p> <p>➔ Activate the same encryption on the network adapter with the correct key.</p> <p>If you do not know the key, you will have to reset the Gigaset SE361 WLAN (see page 18).</p> <p>Warning: Please bear in mind that this will return all the configuration settings to the factory settings.</p>

Symptom	Possible cause and remedial actions
You cannot open a connection from a wireless device to the Gigaset SE361 WLAN.	<p>The Wireless Network function is deactivated.</p> <ul style="list-style-type: none"> ➔ Check whether the Wireless Network function is deactivated and, if so, activate it (see page 56). <p>The PC does not have a wireless connection.</p> <ul style="list-style-type: none"> ➔ Use the Windows device manager (My Computer – Properties) to check whether the network connection is functioning. If you see a red cross or a question mark, then the driver may not have been installed or there is a resource conflict. Follow the Windows instructions to remedy the problem.
The Gigaset SE361 WLAN or other PCs cannot be reached by a PC in the connected LAN with a ping command.	<ul style="list-style-type: none"> ➔ Make sure that TCP/IP has been installed and configured on all the PCs on the local network. ➔ Check that the IP addresses have been correctly configured. In most cases you can use the DHCP function of the Gigaset SE361 WLAN to assign dynamic addresses to the PCs in the LAN. In this case, you must configure the TCP/IP settings of all the PCs so that they obtain their IP address automatically. <p>If you configure the IP addresses in the LAN manually, remember to use subnet mask 255.255.255.x. This means that the first three parts of the IP address on each PC and the Gigaset SE361 WLAN must be identical. The device must also be configured as DNS server.</p>
No connection to the Gigaset SE361 WLAN's configuration interface.	<ul style="list-style-type: none"> ➔ Use the ping command to check whether you can establish a network connection to the Gigaset SE361 WLAN. ➔ Check the network cable between the PC which you want to use to manage the device and the Gigaset SE361 WLAN. ➔ If the PC you want to use is on the router's local network, make sure that you are using the correct IP address administration (see above). ➔ If the PC you want to use is not on the router's local network, it must be authorised via Remote Management.
Password forgotten or lost	<ul style="list-style-type: none"> ➔ Reset the Gigaset SE361 WLAN (see 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 remedial actions
<p>You cannot access a resource (drive or printer) on another PC.</p>	<ul style="list-style-type: none"> ➔ Make sure that TCP/IP has been installed and configured on all the PCs on 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.
<p>The transmission rate is too low.</p>	<ul style="list-style-type: none"> ➔ Radio data transmission depends on the operating environment, for example the building stock or the influence of other devices in the vicinity that transmit in the 2.4-GHz frequency range. ➔ Arrange your WLAN devices closer together. ➔ Change the antenna direction. ➔ Position the device elsewhere. ➔ Switch off other radio sources in the vicinity. They may interfere with data transmission. ➔ Choose a different channel. ➔ Check to see if the problem also arises with a different type of encryption.

Specifications

Interfaces

1 WAN	RJ45, 10Base-T/100Base-TX, Autosensing, MDI/MDIX
4 LAN	RJ45, 10Base-T/100Base-TX, Autosensing, MDI/MDIX
WLAN	IEEE 802.11g or IEEE 802.11b, to connect up to 32 wireless PCs

Wireless properties

Frequency range	2,400 to 2,484 GHz ISM band
Spreading	Direct Sequence Spread Spectrum (DSSS)
Modulation	CCK, OFDM
Number of channels	13: all countries except Japan, USA and Canada 11: USA and Canada
Transmission rate	IEEE 802.11b: up to 11 Mbps IEEE 802.11g: up to 54 Mbps

Operating environment

Temperature	Operating temperature 0 °C to 40°C Storage temperature -20 to 70°C
Humidity	5% to 90% (non condensing)

LED displays

Power
Online (Internet)
WLAN (activity, wireless)
WAN (connection to modem, activity)
LAN1... LAN4 (connection to PC, activity, wired)

Compliance with security conditions and regulations

CE, EN60950

Software

Browser-based configuration environment
NAT, PPPoE
DHCP server and client
NAT, Port Forwarding, Port Triggering, Exposed Host
Security setup
Firewall, prevention of hacker attacks
MAC address filtering
URL filtering,
DoS blocking, SPI
Log file
WEP encryption
WPA2-PSK / WPA-PSK encryption

Authorisation

This device is intended for use worldwide outside the European Economic Area (with the exception of Switzerland) subject to national approval. In France, this device is only intended for internal use within buildings.

Country-specific requirements have been taken into consideration.

We, Siemens Home and Office Communication Devices GmbH & Co. KG, declare that this device meets the essential requirements and other relevant regulations laid down in Directive 1999/5/EC.

A copy of the 1999/5/EC Declaration of Conformity is available at this Internet address: <http://www.siemens.com/qiqasetdocs>.

CE 06820

Approval



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

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

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

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

Customer service (Customer Care)

We offer you support that is fast and tailored to your specific needs!

- ◆ Our **Online Support on the Internet** can be reached any time from anywhere:

<http://www.siemens.com/gigasetcustomer-care>

It provides you with 24/7 support for all our products. It also provides interactive troubleshooting, a list of FAQs and answers plus user guides and current software updates for you to download.

You will also find frequently asked questions and answers in the comprehensive user guide on the supplied CD.

- ◆ For fast and dependable assistance with any repairs or guarantee/warranty claims, contact our **Service Centres** in:

Ireland **18 50 77 72 77**

United Kingdom **08 45 36 70 81 2**

Please have your proof of purchase ready when calling.

Replacement or repair services are not offered in countries where our product is not sold by authorised dealers.

Please address any questions about the DSL or cable connection to your Internet service provider.

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, Siemens 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 Siemens shall vest in Siemens.
- ◆ This Guarantee shall apply to new devices purchased in the European Union. For Products sold in the United Kingdom the Guarantee is issued by: Siemens Home and Office Communication Devices GmbH & Co. KG, 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, Siemens 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 Siemens 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:

- ◆ In the case of new devices and their components exhibiting defects resulting from manufacturing and/or material faults within 24 months of purchase, Siemens 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 Siemens.
 - ◆ 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 Siemens
- ◆ 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 Siemens shall vest in Siemens.
- ◆ 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 Siemens Home and Office Communication Devices GmbH & Co. KG, 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, Siemens 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 Siemens helpdesk on 1850 777 277. This number is also to be found in the accompanying user guide.

Glossary

Access point

An access point such as the Gigaset SE361 WLAN is the central element in a wireless local area network ([WLAN](#)). It handles connection of the wireless-linked network components and regulates data traffic in the wireless network. The access point also serves as an interface to other networks, e.g. an existing [Ethernet](#) LAN or via a modem to the [Internet](#). The network mode for 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](#), e.g. several notebooks in a conference. All the network components are peers. They must be equipped with a wireless [Network adapter](#).

Beacon

Beacons are data packets that are sent by devices in a wireless network to all other devices to indicate that they are available and ready to receive. Beacons are also used to synchronise the wireless network. A beacon interval is the period between two beacons in milliseconds.

Bridge

A bridge connects several network segments to form a joint network, e.g. to build a [TCP/IP](#) network. The segments can have different physical characteristics, e.g. different connections such as [Ethernet](#) and wireless LANs. Linking individual segments via bridges makes it possible to build local networks of practically unlimited size.

See also: [Switch](#), [Hub](#), [Router](#), [Gateway](#)

Broadcast

A broadcast is a data packet that is not directed to a particular recipient but to all the components in a network. The Gigaset SE361 WLAN does not pass broadcast packets on to the Internet; they always remain within the local area network ([LAN](#)) administered by the Gigaset SE361 WLAN.

BSSID

Basic Service Set ID

The BSSID is used for unique differentiation between one wireless network ([WLAN](#)) and 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.

Connect on demand

Connect on demand means that applications such as a 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 a [Flat rate](#). This function can be deactivated at the Gigaset SE361 WLAN to save call charges.

DHCP

Dynamic Host Configuration Protocol

DHCP handles the automatic assignment of [IP addresses](#) to network components. It was developed due to the fact that in large networks – especially the [Internet](#) – defining IP addresses is very complex 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, it also allows address blocks to 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 SE361 WLAN includes a DHCP server and can automatically assign IP addresses to PCs in the local network. You can specify that the IP addresses for certain PCs are never changed.

DHCP server

See [DHCP](#)

DMZ

Demilitarized Zone, see also [Exposed Host](#)

DMZ describes a part of a network that is outside the [Firewall](#). A DMZ is set up, as it were, between a network you want to protect (e.g. a [LAN](#)) and a non-secure network (e.g. the [Internet](#)). A DMZ is useful if you want to offer [Servers](#) services on the Internet which, for security reasons, will not run behind the firewall, or if Internet applications do not function correctly 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.

Glossary

DNS

Domain Name System

DNS permits the assignment of IP addresses to computers or [Domain names](#), which 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 is based on 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 next higher name servers, which again know addresses and the next higher name servers.

DNS server

See [DNS](#)

Domain name

The domain name is the reference to one or more Web servers on the [Internet](#), e.g. siemens.com. The domain name is mapped to the respective [IP address](#) via the [DNS](#) service.

DSL

Digital Subscriber Line

DSL is a data transmission technology in which a connection to the [Internet](#) can be run over normal telephone lines. A DSL connection is supplied by an [Internet Provider](#). It requires a DSL modem.

Dynamic IP address

A dynamic [IP address](#) is assigned to a network component automatically by [DHCP](#). This means that the IP address of a network component can change with every login or at certain intervals.

See also [Static IP address](#)

DTIM

Delivery Traffic Indication Message

A DTIM is a signal that is sent by an access point as part of a [Beacon](#) to a client device in power-saving mode to indicate that a data packet is ready for delivery. The DTIM interval defines the frequency with which a DTIM appears in a series of beacon packets.

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 SE361 WLAN offers [WEP](#) encryption and [WPA](#) encryption for secure data transmission 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 baseband cable with a data transmission rate of 10, 100, or 1000 [Mbps](#).

Exposed Host

Exposed Host refers to a PC outside the firewall.

See also [DMZ](#)

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

A flat rate is a special billing system for [Internet](#) connections. The [Internet Provider](#) charges a monthly fee regardless of the duration and number of logins.

Full duplex

Data transmission mode in which data can be sent and received simultaneously.

See also [Half duplex](#)

Gateway

A gateway is a device used to connect 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](#).

See also Bridge, Hub, Router, Switch

Glossary

Global IP address

See [Public IP address](#)

Half duplex

Operating mode for data transfer. Only one party can receive or send data at any one time.

See also [Full duplex](#)

HTTP proxy

An HTTP proxy is a [Server](#) that network components use for their [Internet](#) traffic. All requests are sent via the proxy.

Hub

A hub connects several network components in a star-topology network by sending all the data it receives from one network component to all the other network components.

See also [Switch](#), [Bridge](#), [Router](#), [Gateway](#)

IEEE

Institute of Electrical and Electronics Engineers

IEEE is an international body that defines network standards, especially to standardise [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 and 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](#)).

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](#) stack. All participants on the Internet can be identified by an [IP address](#). Servers are addressed by [Domain names](#) (e.g. siemens.com). Domain names are assigned to IP addresses by the Domain Name Service ([DNS](#)).

Among the most important Internet services are:

- ◆ electronic mail (email)
- ◆ the World Wide Web (WWW)
- ◆ file transfer (FTP)
- ◆ discussion forums (Usenet / Newsgroups)

Internet Provider

An Internet provider (Internet Service Provider) offers access to the [Internet](#) for a fee.

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

An IP address is a network-wide unique address for a network component in a network based on the [TCP/IP](#) protocol (e.g. in a local area network ([LAN](#)) or on the [Internet](#)). The IP address has four parts (values from 0 to 255) separated by periods (e.g. 192.168.1.1). The IP address consists of the network address and the PC address. Depending on the [Subnet mask](#), one part of the IP address (mostly one, two or three parts) form the network address, the remainder the PC address. You can find out the IP address of your PC by entering `ipconfig` in the command prompt.

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 IP addresses. [DNS](#) is responsible for assigning domain names to IP addresses.

The Gigaset SE361 WLAN has a [Private IP address](#) and a [Public IP address](#).

IP pool range

The Gigaset SE361 WLAN'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, see [Internet Provider](#)

Glossary

LAN

Local Area 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 a wide area network ([WAN](#)) such as the [Internet](#).

With the Gigaset SE361 WLAN you can set up a wired local [Ethernet](#) network and a wireless [IEEE 802.11g](#) standard network ([WLAN](#)).

Lease time

The lease time defines the period for which PCs keep the [Dynamic IP address](#) assigned to them by the [DHCP](#) server without changing it.

Local IP address

See [Private IP address](#)

MAC address

Media Access Control

The MAC address is used for the globally unique identification of a [Network adapter](#). It comprises six parts (hexadecimal numbers), e.g. 00-90-96-34-00-1A. The MAC address is assigned by the network adapter's manufacturer and should not be changed.

Mbps

Million bits per second

Specification of the transfer speed in a network.

MER

MAC Encapsulated Routing

Special form of transmission protocol for the Internet.

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 more [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 on the local network are hidden behind the router's IP address, which is registered on the Internet. Because of this security function, NAT is frequently used as part of a network [Firewall](#). If you want to make services on a PC in the local network available on the Internet despite NAT, you can configure the Gigaset SE361 WLAN as a [Virtual server](#).

Network

A network is a group of devices connected in wired or wireless mode so that they can share resources such as data and peripherals. A general distinction is made between local area networks ([LANs](#)) and wide area networks ([WANs](#)).

Network adapter

A 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 300 and the Gigaset USB Adapter 300 are examples of wireless network adapters.

A network adapter has a unique address, the [MAC address](#).

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 SE361 WLAN 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 area 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](#) that connects network components in a local Ethernet network to the [Internet](#) via an ATM network.

Glossary

PPPoE

Point-to-Point Protocol over [Ethernet](#)

PPPoE is a [Protocol](#) that connects network components in a local Ethernet network to the [Internet](#) via a modem.

Private IP address

The private [IP address](#) (also known as the local IP address) is a network component's address within the local network ([LAN](#)). The network operator can assign any address he or she wants. Devices that act as a link from a local network, such as the Gigaset SE361 WLAN, have a private and a [Public IP address](#).

Protocol

A protocol describes the agreements for communicating in a network. It contains rules for opening, managing and closing a connection, as well as about data formats, time frames and how to handle potential errors. Communication between two applications requires different protocols at different levels, e.g. the [TCP/IP](#) protocols on the [Internet](#).

Public IP address

The public [IP address](#) (also known as global IP address) is a network component's address on the [Internet](#). It is assigned by the [Internet Provider](#). Devices that create a link from a LAN to the Internet, such as the Gigaset SE361 WLAN, have a public and a [Private IP address](#).

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 area network ([LAN](#)).

Repeater

A repeater extends the range of a wireless local area network by relaying data from the [Access point](#) to additional PCs or [Network adapter](#).

Roaming

Roaming extends the range of a wireless LAN by using several [Access points](#) with the same [SSID](#) and the same radio channel and 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 via [Ethernet](#) or [WLAN](#) technology to the [Internet](#).

See also [Bridge](#), [Switch](#), [Hub](#), [Gateway](#)

Server

A server makes a service available to other network components ([Clients](#)). The term "server" is often used to refer to a computer or PC. However, it can also mean an application that provides a particular service such as [DNS](#) or a Web service.

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 Provider](#) gives you 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 network administration 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 a [Dynamic IP address](#), a static IP address never changes.

Subnet

A subnet divides a network into smaller units.

Subnet mask

The subnet mask determines how many parts of a network's [IP address](#) represent the network address and how many parts represent the PC address.

The subnet mask in a network administered by the Gigaset SE361 WLAN is always 255.255.255.0. This means that the first three parts of the IP address form the network address and only the final part is used for the PC address. In this case, the first three parts of the IP address of all network components are therefore always the same.

Glossary

Switch

Like a [Hub](#), a switch is an element used to link different network segments or components. Unlike a hub, however, a switch has its own intelligence, which enables it to forward packets only to the subnet or network component for which they are intended.

See also [Bridge](#), [Hub](#), [Router](#), [Gateway](#)

TCP

Transmission Control Protocol

The TCP [Protocol](#) is part of the [TCP/IP](#) protocol family. TCP handles data transport between communication partners (applications). TCP is a session-based transmission protocol, i.e. it sets up, monitors and terminates a connection for transporting 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.

TKIP

The Temporal Key Integrity Protocol (TKIP) is part of the IEEE 802.11i standard and is used to encrypt data in wireless networks.

UDP

User Datagram Protocol

UDP is a [Protocol](#) from the [TCP/IP](#) protocol family, which handles data transport between two communication partners (applications). Unlike [TCP](#), UDP is a non-session based protocol. It does not establish a static connection. The data packets, so-called datagrams, are sent as a [Broadcast](#). The recipient alone is responsible for making sure the data is received. The sender is not notified about whether or not it is received.

UPnP

Universal Plug & Play

UPnP technology is used to spontaneously link 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 on the network automatically.

URL

Universal Resource Locator

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

Virtual server

A virtual [Server](#) provides a service on the [Internet](#) that runs on another network component, not on the server itself. The Gigaset SE361 WLAN 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 the local network.

WAN

Wide Area Network

A WAN is a wide area network, which is not restricted to one particular area. The Internet is the most frequently used WAN. A WAN is run by one or more public providers to enable private access. You access the Internet via an [Internet Provider](#).

WEP

Wired Equivalent Privacy

WEP is a security protocol defined in the [IEEE 802.11](#) standard. It is used to protect wireless transmissions in a [WLAN](#) against unauthorised access with [Encryption](#) of the data transmitted.

WLAN

Wireless LAN

Wireless LANs enable network components to communicate with a network using radio waves as the transport medium. A wireless LAN can be connected as an extension to an existing wired LAN or it can form the basis for a new network. The basic element of a wireless network is the radio cell. This is the area in which wireless communication takes place. A WLAN can be operated in [Ad-hoc mode](#) or [Infrastructure mode](#).

WLAN is currently specified in the [IEEE 802.11](#) standard. The Gigaset SE361 WLAN complies with standard 802.11g.

WPA

WPA was developed to improve the security provided by [WEP](#). WPA uses more complex procedures to generate keys, e.g. TKIP (Temporal Key Integrity Protocol). In addition, WPA can use an authentication server (e.g. a RADIUS server) to improve security.

WPA-PSK

WPA Pre-shared Key

Variant of [WPA](#) data encryption in which new keys are generated automatically at regular intervals by means of a keyword (Pre-shared Key). The key is updated at defined intervals ([Rekey interval](#)).

Index

Numeric

10 Mbps Ethernet	22
10/100 Mbps switch port	18
100 Mbps Ethernet	22
128-bit encryption	60
128-bit key	35, 59, 61
64-bit key	35, 59, 61

A

Access control	38, 46, 61
blocking services	46
local network	61
Access point	10, 56, 102
Address block for	
IP addresses	54
Ad-hoc mode	10, 102
Advanced Settings	26
features	40
Antenna	19
ASCII key	36, 60
Authorisation	98
Auto connect	103

B

Back panel	18
Backing up configuration data	68
Backup	68
Base station, see Access point	
Basic settings	
summary	31
Basic Setup Wizard	26
configuration	28
Beacon	102
Beacon interval	102
defining	58
Bridge	102
Broadcast	57, 102
Browser	24
BSSID	102

C

Channel	57
---------	----

Checking network settings

(Windows XP)	79
--------------	----

Client	103
--------	-----

Command

exit	91
ipconfig / release	91
ipconfig /renew	91
ping	92

Configuration

resetting to factory setting	69
restoring	69

configuration

security	32
----------	----

Configuration file	68
--------------------	----

Configuration program

elements	27
idle time	67
launching	24
selecting a language	26

Connect on Demand	103
-------------------	-----

Connecting cable modem to router	20
----------------------------------	----

Connection

on demand	30, 42
statistics	92
to router, check	92

Connection duration	30
---------------------	----

Connection method	77
-------------------	----

Connection mode	30, 42
-----------------	--------

Creating a network installation

disk (Windows XP)	79
-------------------	----

D

Data encryption	59
-----------------	----

Deactivating http proxy

Windows 2000	90
Windows XP	82

Defining computer name

Windows 2000	85
Windows XP	79

Defining workgroup

Windows 2000	85
Windows XP	79

DHCP	76, 103
------	---------

DHCP server	55, 103
-------------	---------

- DHCP service, see DHCP
 - Digital Subscriber Line, see DSL
 - DMZ 14, 51, 103
 - DNS 104
 - DNS configuration
 - Windows 2000 89
 - Windows XP 81
 - DNS server 104
 - defining 44
 - Domain name 104
 - Domain Name Service, see DNS
 - DSL 104
 - DSL interface
 - configuring 28
 - DSL modem
 - connecting to router 20
 - DTIM 104
 - DTIM interval 104
 - defining 58
 - Dynamic DNS, see DynDNS
 - Dynamic Host Configuration Protocol,
 - see DHCP
 - Dynamic IP address 76, 104
 - DynDNS 52, 105
 - DynDNS service, see DynDNS
 - DynDNS.org 52
- E**
- Encryption 34, 58, 59, 61, 105
 - WEP 35
 - WPA 34
 - Ethernet 9, 10, 13, 105
 - cable 22
 - linking with a wireless network
 - 12
 - Transmission speed 13
 - Exit command 91
 - Exposed host 14, 51
- F**
- Fast Ethernet 22
 - Features 13
 - Firewall 13, 105
 - activating/deactivating 45
 - configuring 45
 - Flat rate 105
 - Front panel 17
- Full duplex 105
- G**
- Games on the Internet 48
 - Gateway 105
 - Gigaset SE361 WLAN
 - back panel 18
 - configuring 24
 - connecting 20
 - Front panel 17
 - installing 15
 - IP address 24
 - password protection 32
 - possibilities for network setup 8
 - setting up 19
 - wall installation 19
 - Global IP address, see
 - Public IP address
 - Guarantee Certificate 100
- H**
- Hacker attack 13
 - Half duplex 106
 - Help 27
 - Hexadecimal 36, 60
 - Hexadecimal key 36, 60
 - HTTP proxy 106
 - Hub 106
- I**
- Idle time 67
 - IEEE 106
 - Infrastructure mode 10, 106
 - Installation 15
 - Installing network services
 - (Windows 2000) 84
 - Installing TCP/IP protocol for Windows
 - 2000 86
 - Institute of Electrical and Electronics
 - Engineers, see IEEE
 - Internet 107
 - connect on demand 42
 - connection mode 30, 42
 - manual connection 42
 - menu 41
 - service provider 42
 - setting up access control 46

Index

Test Settings	42	LED	
Internet access	7	behaviour after initial connection	23
blocking	41	displays	17
Internet connection		Local area network	13
changing configuration	41	Local IP address, see	
closing manually	64	Private IP address	
connecting manually	64	Local network	7, 108
disconnecting automatically	30, 42	configuring	76
setting up	41	Login page	24
Internet Explorer	16, 24	Login screen	24
Internet protocol, see IP protocol		Logoff	27
Internet provider	42, 107		
Internet time	66	M	
IP address	54, 107	MAC access control list	38, 61
address block	54	MAC address	108
assigning automatically	54, 76	changing registration	44
assigning static	55, 76	cloning	44
dynamic	76, 104	MAC address filter	38
Gigaset SE361 WLAN	24	MAC Encapsulated Routing,	
private	110	see MER	
public	110	MAC table	38
static	111	Mains adapter	
IP address block for DHCP	55	connecting	23
IP address pool	107	port	18
IP protocol	107	Mains power supply, connection to	23
ipconfig / release	91	Manual connection	42
ipconfig /renew	91	Maximum Receive Unit, see MRU	
ISP, see Internet provider		Maximum Transmission Unit, see MTU	
		Mbps	108
		MER	108
K		Mozilla Firefox	16, 24
Key length	36	MRU	108
128-bit (ASCII)	36, 61	MTU	108
128-bit (hexadecimal)	36, 60		
64-bit (ASCII)	36, 60	N	
64-bit (hexadecimal)	36, 60	NAT	47, 109
Key type	36	port forwarding	47
		port triggering	47
L		Network	109
LAN	12, 108	Ad-hoc mode	10
LAN connection		infrastructure	10
creating	22	wired	9
creating wired	22	wireless	10
creating wireless	21	Network adapter	109
LAN port	18	wireless	10, 21
transmission speed	22	Network Address Translation, see NAT	
Lease time	55, 108		

- Network configuration 76
 - Windows 2000 84
 - Windows XP 76
- O**
- Obtaining an IP address automatically
 - Windows 2000 89
 - Windows XP 81
- Open command prompt 92
- Operating state 17
- Optimising network performance . . . 57
- P**
- Pack contents 16
- Passphrase 37
- Password 24, 32
 - assigning 32
 - changing 32
 - forgotten 33
- PC**
- connecting 21
- defining a name
 - (Windows 2000) 85
 - (Windows XP) 79
- IP address 76
- network settings 76
- Ping command 92
- Point-to-Point Protocol over ATM,
 - see PPPoA
- Point-to-Point Protocol over Ethernet,
 - see PPPoE
- Port 109
 - for DSL or cable modem 18
 - for mains adapter 18
 - LAN 18
 - public port 47, 49
 - trigger port 47, 49
- Port forwarding 47, 109
 - setting up 50
- Port number 50, 109
 - mapping 50
- Port triggering 47, 48
 - setting up 49
- PPPoA 109
- PPPoE 13, 110
- Pre-shared key
- Private IP address 110
- Problem solving 93
- Protocol 110
- Public IP address 110
- Q**
- QoS (Quality of Service) 53
- R**
- Radio cell 113
- Radio network 113
 - Ad-hoc mode 10
 - Infrastructure mode 10
- Reboot 19, 69
- Regional options 65
- Rekeying 34, 58
- Releasing TCP/IP settings
 - Windows 2000 91
 - Windows XP 83
- Remote administration 67
- Remote management 110
- Repeater 62
- Reset 19, 69
- Roaming 110
- Router 111
 - dynamic IP address 52
 - IP address 54
 - setting up a local area network 8
- S**
- Safety precautions 6
- Security measures 13
- Security settings 32
 - saving 39
- Security Setup Wizard 26
- Server 111
 - virtual 113
- Service Set Identifier, see SSID
- Simple Mail Transfer Protocol, see SMTP
- Simple Network Management Protocol,
 - see SNMP
- SMTP 111
- SNMP 111
- SSID 15, 33, 57, 111
 - changing 33
 - default setting on router 15
 - hidden 57
 - visible 33, 57

Index

SSID broadcast. 33, 57
Start screen 25
Static IP address. 111
Status
 device 75
 local network. 74
 overview 71
 security 72
 wireless network 74
Status information. 71
Subnet. 111
Subnet mask 111
Super G 16
Switch. 112
Synchronising the TCP/IP settings
 with the router
 Windows 2000. 91
 Windows XP. 83
System password
 assigning 66
 changing 66
System requirements. 16
System time 66

T

TCP 112
TCP/IP 112
TCP/IP network. 76
TCP/IP settings
 Windows 2000. 88
 Windows XP. 80
Temperature range for operation. 19
Time server 66
TKIP. 112, 113
Trademarks 6
Transmission Control Protocol, see TCP
Transmission mode 56
 full duplex 22
 half duplex. 22
Transmission speed 108
 in the Ethernet LAN 13
 in wireless LAN. 13
 LAN port 22
Trigger port 47
Troubleshooting 93

U

UDP 112
UI elements 27
Universal Plug and Play, see UPnP
Universal Resource Locator, see URL
Updating firmware 69
Upgrading firmware 69
UPnP 30, 43, 112
 enabling 43
URL 112
URL filter 46
User Datagram Protocol, see UDP
User interface
 buttons. 27
 launching 24

V

VCI. 105
Virtual server 48, 113

W

WAN 113
WAN interface 11
WDS. 62
WEP 34, 35, 58, 59, 113
 encryption mode 60
 hexadecimal 36
 key length. 36, 60
 passphrase 37
Wide Area Network, see WAN
Wired Equivalent Privacy, see WEP
Wired network 9
Wireless LAN, see WLAN
Wireless network
 access control 38
 encryption 34
Wireless settings 56
WLAN. 10, 12, 113
 network modes. 10
 transmission speed. 13
WLAN adapter 10
WPA 34, 58, 113
 pre-shared key
WPA2-PSK 34, 59
WPA-PSK 34, 59
WPA-PSK, see WPA, Pre-shared Key

Issued by

Siemens Home and Office Communication Devices GmbH & Co. KG

Schlavenhorst 66

D-46395 Bocholt

© Siemens Home and Office Communication Devices GmbH & Co. KG 2006

All rights reserved. Subject to availability.

Rights of modification reserved.

No.: A31008-M1067-R101-1-7619