

SIEMENS

tiscali



Gigaset SE587 WLAN dsl

Gigaset

Contents

Contents

The Gigaset SE587 WLAN dsl	4
The device	4
Front Panel	5
Back Panel	5
LED displays	6
Safety precautions	7
Features and applications	7
Configuring the Gigaset SE587 WLAN dsl	8
Configuring the local network	9
The user interface	10
Starting the user interface	10
User interface functions	11
Elements in the user interface	12
Status information	12
DSL Status	12
Internet	13
Internet Status	13
PVC Connection	13
Local Network	14
Wireless Network	14
Device	15
Basic configuration	15
Basic Setup	15
LAN configuration	17
Advanced configuration	20
Wireless Settings	20
Basic Wireless Settings	20
Wireless Security	21
Security	24
Access Restrictions	25
Applications and Gaming	27
Port Forwarding	28
DMZ	29
Administration	30
Management	30
Log	32
Factory Defaults	33
Firmware Upgrade	33
Configuration Management	34

Local network configuration	36
IP addresses	36
Computer names and workgroups	37
Setting up a wireless network	38
Windows XP	38
Windows Vista	39
Mac OS X	41
Network configuration with Windows Vista	42
Showing networks	42
Changing the settings for IP addresses	43
Selecting a computer name and workgroup	45
Network configuration with Windows XP	45
Showing networks	45
Changing the settings for IP addresses	46
Selecting a computer name and workgroup	49
Network configuration with Windows 2000	49
Showing networks	49
Changing the settings for IP addresses	50
Selecting a computer name and workgroup	52
Network configuration with Windows 98, SE, ME	52
Setting up a PC as a client for Microsoft networks	52
Selecting a computer name and workgroup	53
Installing the TCP/IP protocol	54
Making TCP/IP settings	55
Network configuration with Mac OS X	58
Showing networks	58
Changing the settings for IP addresses	59
Selecting a computer name	60
Synchronising TCP/IP settings with the Gigaset SE587 WLAN dsl	60
Windows Vista, Windows XP, Windows 2000	60
Windows 98 SE, ME	62
Mac OS X	63
Checking the connection to the Gigaset SE587 WLAN dsl	63
Establishing the IP and MAC addresses in the network	64
 Appendix	 66
Troubleshooting	66
Specifications	69
Authorisation	70
 Glossary	 71
 Index	 84

The Gigaset SE587 WLAN dsl

The Gigaset SE587 WLAN dsl

The Siemens Gigaset SE587 WLAN dsl is a powerful but easy-to-use communications device for connecting your PCs or local area network (LAN) to the Internet (via ADSL) or for connecting a set-top box to watch IPTV. The Gigaset SE587 WLAN dsl contains an integrated ADSL modem enabling you to access the Internet easily.

You can connect your PCs wirelessly to the Gigaset SE587 WLAN dsl and create a wireless local area network (WLAN). For network security, wireless transmission is encrypted by default using the WPA standard.

The Gigaset SE587 WLAN dsl allows several users to access the Internet simultaneously. A single user account can be shared if Tiscali, your Internet service provider, permits this. If you want to surf the Internet and watch IPTV at the lowest possible cost, the Gigaset SE587 WLAN dsl is a convenient and simple solution.

The Gigaset SE587 WLAN dsl has an extensive range of functions but remains simple to use. It can be configured and operational within a few minutes by running the set-up CD delivered with the device.

The device



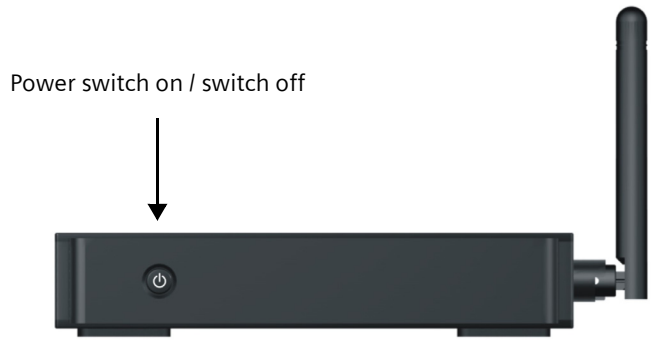
Bottom

The label on the bottom of the device shows the serial number and the preset wireless security settings (SSID and WPA key).

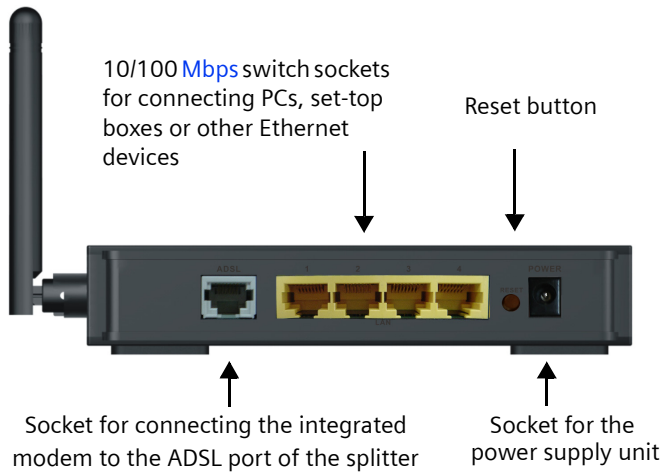
SIEMENS	S30853-S1083-L171	WLAN SSID:
UK use only	Serial number:	Tiscali00067A
		WPA Key:
CLV001659		A53610A66274
CE0682		Date code: 00 PCB: XB

Schablone 2004_08_26

Front Panel



Back Panel



Reset Button

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.

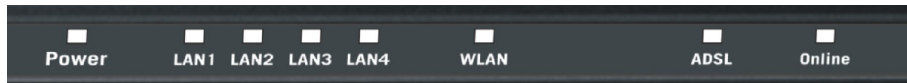
Warning: This will clear all the configuration settings you have made since the initial startup. Do not perform this action without first consulting the Tiscali hotline.

⚡	Only use the power supply unit that comes with the device. Using the wrong power supply unit may damage the device.
---	---

The Gigaset SE587 WLAN dsl

LED displays

The upper side of the device has LED displays that show the operating state and simplify installation and troubleshooting in the network.



The LEDs show the following:

LED	State	Status
Power	On (green)	The device is powered on and has been booted successfully.
	Flashing (green)	System is booting.
	Off	The device is powered off.
	On (red)	The device cannot be booted or a malfunction has been detected.
LAN1 – LAN4	On	A device is connected to the relevant LAN port and a connection has been established.
	Flashing	The LAN port is transmitting or receiving data (traffic).
	Off	There is no device connected or the connected device is powered off.
WLAN	On	The wireless interface is activated, no data transmission at present.
	Flashing	The device is transmitting or receiving data on the wireless interface.
	Off	The wireless interface is deactivated.
ADSL	On	The device is connected to the ADSL port of the splitter and the ADSL connection has been synchronised successfully.
	Flashing	The ADSL connection is being synchronised.
	Off	There is no connection to the ADSL port of the splitter or the ADSL connection cannot be synchronised.
Online	On (green)	A connection to the Internet has been established. *)
	Flashing (green)	The device is transmitting or receiving data from or to the Internet.
	Off	There is no Internet connection.
	On (red)	Device attempted to establish an Internet connection and failed.

*) If the Internet session is dropped due to an idle timeout, the light will remain green as long as a DSL connection is still present.

Safety precautions

- ◆ Only use the router with the mains adapter supplied.
- ◆ The mains adaptor provided is only designed for use in the UK. If the adaptor is to be used in other countries, ensure the specification ratings are not exceeded.
- ◆ Protect the equipment from moisture.
- ◆ Never open the router. For reasons of electrical safety, the router may only be opened by authorised service staff.
- ◆ The router may affect medical electronic equipment. If in doubt consult the supplier of the medical equipment.
- ◆ Make sure you pass on this information sheet if you pass on your router to someone else.

Features and applications

The Gigaset SE587 WLAN dsl's wide range of features makes it ideal for a large number of applications:

Internet access

The Gigaset SE587 WLAN dsl allows several users access to the Internet simultaneously.

- ◆ Since many ADSL providers permit communication with end users via the PPPoA protocol, the Gigaset SE587 WLAN dsl has an integrated client for this protocol. It is therefore no longer necessary to install this service on your PC.
- ◆ The Gigaset SE587 WLAN dsl supports shared Internet access for up to 253 users. This means several users in your network can surf the Internet simultaneously, all using the same Internet account.
- ◆ The Gigaset SE587 WLAN dsl allows the connection of a set-top box which enables you to watch Internet television (IPTV).

Setting up a local area network

The Gigaset SE587 WLAN dsl offers the following possibilities:

- ◆ Up to four devices (PCs, a [Hub](#) or [Switch](#)) connected via [Ethernet](#) ports with a transmission speed of 10 or 100 Mbps (with automatic recognition).
- ◆ Up to 253 mobile terminals connected via a wireless interface with a transmission speed of up to 54 Mbps. It complies with IEEE 802.11g standard and can work with all products that satisfy [WLAN](#) Standard IEEE 802.11b or 802.11g.
- ◆ Using the Gigaset SE587 WLAN dsl makes it easy to set up a network at home or in small offices. For example, users can exchange data in the network.
- ◆ The Gigaset SE587 WLAN dsl supports [DHCP](#) for dynamic IP configuration of the local area network and [DNS](#) for domain name mapping.

The Gigaset SE587 WLAN dsl

Security functions

The Gigaset SE587 WLAN dsl offers comprehensive security measures:

- ◆ **Firewall** protection against unauthorised access from the Internet
With the firewall, the Gigaset SE587 WLAN dsl offers comprehensive protection against hacker attacks.
- ◆ **Network Address Translation (NAT)**
All PCs in the local area network use the **Public IP address** of the Gigaset SE587 WLAN dsl for their Internet connections, which makes them 'invisible' on the Internet. The Gigaset SE587 WLAN dsl only allows access from the Internet if this has been requested from within the local area network.
- ◆ **DMZ (Exposed Host)**
This allows you to release one PC in your local area network for unlimited access from the Internet. Note that in this case your local area network will no longer be adequately protected against Internet attacks.
- ◆ **Service filtering and domain blocking**
The Gigaset SE587 WLAN dsl can filter Internet access. Here you determine which PCs may access which Internet services.
Additionally you can disable access to certain Internet domains (URL blocking).
- ◆ **Encryption for the wireless network**
The Gigaset SE587 WLAN dsl is delivered with a preset individual encryption (WPA2-PSK/WPA-PSK with pre-shared key). You will find the corresponding information on the label on the bottom of the device. Your wireless network is therefore protected against unauthorised access.

If there are wireless network adapters of your PCs that do not support this encryption method, you can use another encryption method (WEP) to prevent unauthorised access to your wireless LAN or to make data illegible to unauthorised parties (see page 23).

Configuring the Gigaset SE587 WLAN dsl

Having performed the installation steps on the set-up CD, your Gigaset SE587 WLAN dsl is now ready for use. No further configuration is normally required.

Your device is also preconfigured with individual security settings (SSID and encryption) for secure wireless operation.

However, if you want to change specific configuration settings or make advanced configuration changes to your Gigaset SE587 WLAN dsl, a browser-based configuration user interface is provided which can be operated via your Internet browser. This is described from page 10 onwards.

In addition, the user interface provides detailed status information on operation and configuration and offers helpful administration options. These are described in the chapters "Status information" on page 12 and "Administration" on page 30.

Information for experienced users

The default settings for your Gigaset SE587 WLAN dsl are:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0
- Radio channel: Automatic
- SSID: individual preset
- Encryption: WPA-PSK (with pre-shared key), individual preset

The individual preset SSID and pre-shared key are shown on the label on the bottom of the device (see page 4).

Important operation information

If you operate a SIP phone on your Gigaset SE587 WLAN dsl please mind that it will maintain the Internet connection even if it is in stand-by mode. This can result in high connection charges if you are on a time-based or volume-based tariff. In this case it is recommended to use a flat-rate tariff.

Configuring the local network

In order to communicate via the Gigaset SE587 WLAN dsl, the **network configuration** may have to be set up correctly on the connected PCs.

This usually occurs automatically with

- ◆ **Windows Vista (32 and 64)**
- ◆ **Windows XP**
- ◆ **Windows 2000** or
- ◆ **Mac OS X**

operating systems provided you have not made any changes to the standard settings for the network configuration.

With **Windows 98 SE or ME** initial network configuration may be necessary.

If you require information on how to configure computers correctly for working in a Local Network (LAN) or in a Wireless Local Access Network (WLAN), please refer to the chapter "Local network configuration" on page 36.

Trademarks

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

Mac OS X is a registered trademark of Appel Inc.

Mozilla Firefox is a registered trademark of the Mozilla Organization.

The user interface

The user interface

You have performed the steps on the start-up CD and successfully connected a computer to the Gigaset SE587 WLAN dsl. You can now use the browser-based user interface for a more detailed configuration of the Gigaset SE587 WLAN dsl or to get information on the configuration and operation. As Internet browser we recommend Microsoft Internet Explorer V 6.0 or higher, or Mozilla Firefox V 1.0 or higher.

Note:

To start the configuration environment, you may need to deactivate the HTTP proxy for your browser.

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

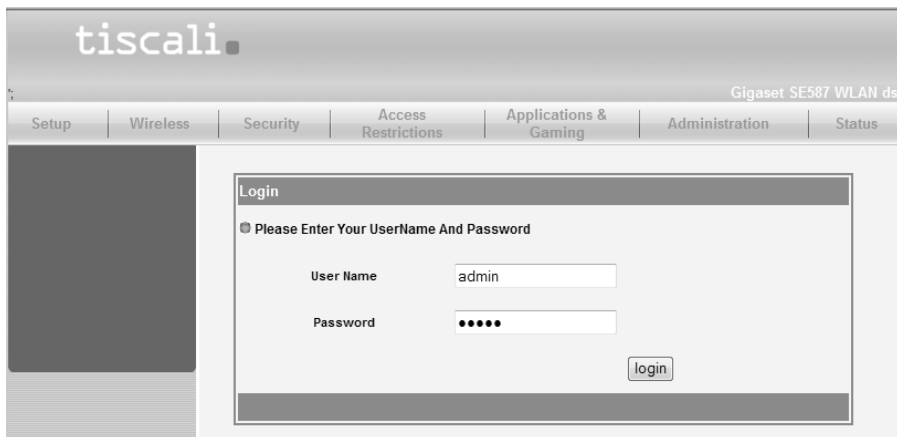
If you use a firewall, it must allow connection to the Gigaset SE587 WLAN dsl. For details, refer to the user guide for your firewall. If necessary deactivate the firewall while you configure your Gigaset SE587 WLAN dsl.

Starting the user interface

To access the user interface of the Gigaset SE587 WLAN dsl:

- ➔ Start your Internet browser.
- ➔ Enter the IP address of the Gigaset SE587 WLAN dsl in the browser's address field:
http://192.168.1.1

The login screen appears.



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

- ➔ Enter the password.
- ➔ Click **Login**.

The user interface is opened displaying the **Status** pages first (see page 12).

The configuration program ends automatically if no entry is made within a time period of 10 minutes.

Note:

- ◆ For security reasons you should change the predefined password at a later stage.
- ◆ You can set up more user IDs and assign passwords via the user interface.

For information on how to set up new user IDs and change the predefined password see section "Management" on page 30.

User interface functions


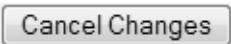

The user interface provides the following menus:

Status	You can view information about the configuration and status of the Gigaset SE587 WLAN dsl in this menu. This is described from page 12 onwards.
Setup	Use this menu to make the settings required for connecting to the Internet. You can also make settings for your local network. This is described from page 15 onwards.
Wireless	This menu allows you to set up your wireless network. You can make the basic settings (e.g. SSID and channel) and set up encryption for wireless traffic. This is described from page 20 onwards.
Security	Here you can enable or disable the firewall of your Gigaset SE587 WLAN dsl. This is described on page 24.
Access Restriction	You can restrict the access to the Internet for specific PCs and for specific services. This is described from page 25 onwards.
Applications and Gaming	This menu allows you to configure the NAT firewall of the device. In particular port forwarding and DMZ can be configured (see page 27).
Administration	The Gigaset SE587 WLAN dsl user interface provides several helpful functions for administering your device. This is described from page 30 onwards.

Status information

Elements in the user interface

The user interface screens contain the following buttons:

	Transfers the settings you have made to the Gigaset SE587 WLAN dsl configuration.
	Deletes all the entries on a screen since the last time you clicked Save Settings .
	Click the help link to display explanations about the current user interface screen.

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

Status information

Information about configuration and the status of the Gigaset SE587 WLAN dsl is displayed in the **Status** menu of the user interface.

Detailed information is available on the following status screens:

- ◆ **DSL Status**
- ◆ **Internet**
- ◆ **Local Network**
- ◆ **Wireless Network**
- ◆ **Device**

The Status pages are updated automatically at regular intervals.

DSL Status

You will find detailed information about the status and operation of the device's DSL connection on the **DSL Status** screen in the **Status** menu.

This page shows whether the DSL connection has been established successfully. The DSL connection is active if the parameter **Connected** has the value **ON** (green coloured).

The additional information provided on this screen is highly technical and can be used by service personnel for a detailed analysis and trouble shooting in the case of an error.

- ➔ In the **Status** menu, select **DSL Status**.
- ➔ Click **Refresh** to refresh this screen and update the displayed data.

Internet

The **Internet** page shows information about the configuration of the Internet connection(s).

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

Internet Status

PVC Connection	Select the virtual connection (PVC), for which the following information should be displayed. Three PVCs have been configured. Modification of the factory configuration for these PVCs can result in loss of service (see page 16).
Internet Connection Type	Connection type of the selected connection (see page 16).
IP address	Public IP address currently assigned to the device.
Subnet Mask	Subnet mask used in the public network.
MTU	Maximum Transmission Unit allowed for data transmission in the network.
Primary DNS server	IP address of the assigned DNS server .
Secondary DNS server	IP address of the alternate DNS server, if available.

PVC Connection

QoS	(Quality of Service) ATM Traffic Class used.
Pcr Rate	(Peak Cell Rate) Maximum rate at which the sender can send cells over the virtual connection.
Scr Rate	(Sustained Cell Rate) Maximum average rate at which cells can be sent over the virtual connection.
VCI	(Virtual Channel Identifier) Channel and destination that ATM traffic will use.
VPI	(Virtual Path Identifier) Path and destination that ATM traffic will use.

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

Status information

Local Network

The **Local Network** page shows information about the local network settings.

➔ In the **Status** menu, select **Local Network**.

MAC Address	Local MAC address of the device's LAN interface.
IP Address	Local IP address of the device.
LAN Subnet Mask	Subnet mask used in the local network.
DHCP Server	Shows if the DHCP server of the device is enabled or disabled.
Start IP Address	First IP address in the IP range which can be assigned to a client by the DHCP server.
End IP Range	Last IP address in the IP range which can be assigned to a client by the DHCP server.

The **DHCP Server Active IP/MAC Table** shows the clients in the network that currently have been assigned an IP address by the Gigaset SE587 WLAN dsl DHCP server. The following information is displayed for each client:

- **IP Address**
- **MAC Address**
- **Lease Time** (remaining time before the DHCP server will assign a new IP address)
- **Host Name**

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

Wireless Network

The **Wireless** page shows information about the wireless network settings.

➔ In the **Status** menu, select **Wireless**.

Authentication	Security mode used for encryption (see page 21).
Encryption	Encryption method used.
MAC Address	MAC address of the device's wireless interface.
Mode	Wireless network mode set for data transmission (see page 20)
SSID	Wireless network ID (see page 20).
Allowed Channels	Channels which are allowed for wireless communication
Current Channel	Radio channel that is currently being used for data transfer in the wireless network.
Transmit Rate	Transmission rate currently set.
Max Frame Burst	Maximum time, in microseconds, that the device transmits IEEE 802.11g wireless traffic only.

RTS Threshold RTS (Ready to send) Threshold defines the latency between the message "Ready to send" and the sending of the next data packet.

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

Device

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

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

Firmware Version Firmware version currently installed on your device.

System Time System time for your device.

System Uptime Your device's operating time since the last time the system was started in the format HH:MM:SS.

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

Basic configuration

The **Setup** menu contains all the functions required for setting up your device for connection to the Internet and for establishing your local network.

Basic Setup Set up the Internet connection for one or more virtual connections (see below).

Local Network Define the basic settings for the local network and configure the DHCP server (see page 15).

Basic Setup

The **Basic Setup** page shows the current Internet configuration of your device. In order to grant access to the Internet to users in your local network, the Internet connection on your device must be set up correctly. This is performed when you execute the start-up CD and you do not need to change any parameter on this page.

Note:

The access data is saved in the Gigaset SE587 WLAN dsl during configuration. If the device is passed on to someone else for any reason, you should always first restore the factory settings (page 33). Otherwise, unauthorised persons may use your Internet access at your expense.

The device's configuration user interface allows you to configure additional Internet connections if necessary. However, all the settings you make here must coincide with the features your **Internet service provider** Tiscali makes available to you. False informa-

Basic configuration

tion can lead to problems with your Internet connection. If you want to set up your Internet connection manually or set up additional virtual connections you need your Internet service provider's access data and technical information for the configuration. You will find the access data you require in the documentation you received from Tiscali. The configuration details are not described in this document.

➔ In the **Setup** menu, select **Basic Setup**.

Use **Tiscali - data PPPoA** Interface for Internet Access

Internet Setup

PVC selection

Tiscali - data PPPoA

Internet Connection Type

PPP over ATM

Description: Tiscali - data PPPoA

Encapsulation Method: VcMux

VPI: 0 (Range 0-255)

VCI: 38 (Range 32-65535)

Authentication: Auto

User Name:

Password:

pppoa Connection Mode: Always on

NAT: ON OFF

Save Settings Cancel Changes

At the top of this page you can choose which of the configured interfaces (data PPPoA or data IPoEoA) should be used for Internet access. This should be set to PPPoA unless advised otherwise by Tiscali.

PVC selection

The Gigaset SE587 WLAN dsl allows you to configure different virtual connections (called **PVC**) which can share the same physical connection (DSL) at the same time. For each connection the access data of Tiscali is required.

The Tiscali standard connections (data PPPoA, IPTV or data IPoEoA) cannot be changed. If required, you can change the **User Name** and the associated **Password** for the connection.

Configuring further connections

In addition, you can configure a **PPPoA** or **PPPoE** connection or a Bridge connection according to the RFC 2684.

Basic configuration

- ➔ If you want to configure a connection, select **(empty)** from the **PVC selection** option menu.
- ➔ You have to specify the **Internet Connection Type**, so that the Gigaset SE587 WLAN dsl works correctly with your ISP's equipment.
- ➔ Enter the data required according to the **Internet Connection Type** you have chosen.
- ➔ Click **Save Settings** to apply your settings.

LAN configuration

You can use the LAN configuration to change the **IP address** of the Gigaset SE587 WLAN dsl and configure the **DHCP server**.

- ➔ In the **Setup** menu, select **Local Network**.

Local Network Setup

Router IP

Local IP Address

Subnet Mask

Network Address Server Settings (DHCP)

ON OFF

Use Default Range YES NO

Client Lease Time

DHCP Server fixed IP/MAC Mappings

Operation	IP Address	Mac Address	Lease Time(Sec)
add <input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="0"/>

Time Setting

Operation	Server Address Or Hostname
del <input type="checkbox"/>	<input type="text" value="192.168.1.1"/>
add <input type="checkbox"/>	<input type="text"/>

Time Zone

Manual Setting Time

Daylight Saving YES NO

Basic configuration

Defining the private IP address for the Gigaset SE587 WLAN dsl

On this screen you can change the device's [Private IP address](#). The preset IP address is 192.168.1.1. This is the address under which the device can be reached in the local network. It can be freely assigned from the block of available addresses. The IP address under which the Gigaset SE587 WLAN dsl can be reached from outside is assigned by Tiscali. The default [Subnet mask](#) for the local network administered by the Gigaset SE587 WLAN dsl is 255.255.255.0.

➔ If you want to assign a different IP address to the Gigaset SE587 WLAN dsl, enter your chosen IP address in the fields next to **Local IP address**.

Make sure you note which subnet mask is set when assigning the IP address. If you are retaining the default subnet mask, the first three parts of the IP address must be identical for all network components (including routers).

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

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

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

Note:

- ◆ You can only change the last part of the subnet mask at the moment (even if further parts are displayed as editable).
- ◆ New settings can only be made after the Gigaset SE587 WLAN dsl has been rebooted. If necessary reconfigure the IP address on your PC (including one that is statically assigned) so that it matches the new configuration.

Configuring the DHCP server

The Gigaset SE587 WLAN dsl has a [DHCP server](#) for which the factory setting is active. Consequently, the IP addresses of the PCs are automatically assigned by the Gigaset SE587 WLAN dsl.

Note:

- ◆ If the DHCP server for the Gigaset SE587 WLAN dsl is activated, you can configure the network setting on the PC so that the option **Obtain an IP address automatically** is set up. For further information, refer to the section "Local network configuration" on page 36.
- ◆ If you deactivate the DHCP server, you will have to assign a static IP address for the PCs that use the network settings.

➔ To activate the DHCP server, select **ON**.

If the DHCP server is active, you can define the IP address range the DHCP server should use for assigning IP addresses to the clients.

➔ Select **YES** for **Use Default Range** if you want the device to assign IP addresses in the range 1-254 (if the router's IP address is 192.168.1.1 the addresses from 192.198.1.2 - 192.198.1.254 are used).

Basic configuration

- ➔ Select **NO** for **Use Default Range** and define the range of IP addresses the Gigaset SE587 WLAN dsl should use to automatically assign IP addresses to the PCs. Define the **Start IP Address** and the **End IP Address**.
- ➔ The lease time indicates how long the client may use the allocated IP configuration before the DHCP server can assign a new IP address. Choose a value from the **Client Lease Time** option menu.

DHCP Server fixed IP/MAC Mappings

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).

- ➔ Select the **add** box to activate the fields in a row to create a new entry.
- ➔ Enter the **IP Address** you wish to assign to the PC.
- ➔ Enter the **MAC Address** of the PC to which you want to assign a static IP address.
- ➔ Enter a specific lease time in seconds for the PC in the **Lease Time(Sec) field**.
- ➔ Select the **del** box to delete the entry from the list.

Time Setting

For operating your Gigaset SE587 WLAN dsl, you can set a time server, select the time zone or set the time and date manually.

- ➔ If a time server is available in your network select the **add** box and enter the IP address or host name of the time server in the **Server Address or Hostname** field.
- ➔ Select the **del** box to delete an entry from the list.
- ➔ Select the **Time Zone** for your location from the list.
- ➔ If you want to enter date and time manually use the **Manual Setting Time** field. Enter the value in the format: YYYY:MM:DD:HH:MM:SS.
- ➔ Enable or disable the **Daylight Saving** option depending on your location.

- ➔ Click **Save Settings** to apply all your settings on this page.

Advanced configuration

Advanced configuration

Wireless Settings

If you have implemented wireless PC communication via the Gigaset SE587 WLAN dsl, you should improve the security of your wireless network via the **Wireless** menu. You can carry out the following functions:

Basic Wireless Settings Activate or deactivate the wireless module of the device and specify basic settings for your wireless network, for example **SSID** or **Channel** (see below).

Wireless Security Set up [Encryption](#) for wireless transmissions (see page 21).

Basic Wireless Settings

➔ In the **Wireless** menu, select **Basic Wireless Settings**.

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

Devices can only log in wirelessly if the wireless module of the Gigaset SE587 WLAN dsl is activated.

You can now make the settings for the wireless network.

Wireless Network Mode

Your Gigaset SE587 WLAN dsl provides wireless data transfer according to the [IEEE 802.11](#) standard. The IEEE 802.11g standard permits data transfer up to 54 Mbit/s and the IEEE 802.11b standard up to 11 Mbit/s. Choose **G only** to ensure the best possible data transfer rates in your network. To operate clients with older wireless network adapters in your network, select **MIXED**. If you only operate IEEE 802.11b clients in your network choose **B only**.

➔ Select the required **Wireless Network Mode** for your wireless network.

Wireless Network Name (SSID)

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

The SSID for the Gigaset SE587 WLAN dsl is individually preset. The preset SSID is shown on the label on the bottom of the device (see page 4).

You can change the SSID if required and for security reasons you can deactivate SSID broadcast.

- ➔ Enter a character string of your choice. The SSID is case-sensitive. It can contain up to 32 characters. Use a combination of letters, digits and special characters.

Note:

The connection to the wireless network adapters will be interrupted until you have connected them with the new SSID.

Wireless Channel

All clients in the network use the same radio channel for wireless data transfer.

The channel is selected automatically by default (**Auto Channel** is enabled). If required, you can choose manually between various channels, depending on your current location.

To choose the channel manually:

- ➔ Disable the **Auto Channel** option.
- ➔ Select the **Wireless Channel** for your wireless network.

Wireless SSID broadcast

If this option is enabled (default setting), the Gigaset SE587 WLAN dsl will send the SSID in all data transfers and the SSID of the Gigaset SE587 WLAN dsl will be displayed on PCs that have a wireless network adapter. In this case, hackers could use the SSID to detect your network.

If you deactivate **Wireless SSID broadcast**, the SSID of the Gigaset SE587 WLAN dsl will not be displayed. This increases protection against unauthorised access to your wireless network. Make a note of the SSID. You will need it to log on to the PC.

- ➔ Select **Disable** to deactivate **Wireless SSID broadcast**.
- ➔ Click **Save Settings** to apply all your settings on this page.

Wireless Security

For your security data transmission in your wireless network is encrypted by default. Access to your wireless network is only granted to authenticated clients.

The Gigaset SE587 WLAN dsl is delivered with preset individual encryption (WPA-PSK/ WPA2-PSK with pre-shared key). You will find this key on the label on the bottom of the device.

Advanced configuration

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

Note:

If you change the encryption, wirelessly connected clients are disconnected until you update the security setting on the wireless network adapters again.

The following security mechanisms are available:

- ◆ **WPA-PSK/WPA2-PSK** (WiFi-Protected Access)
- ◆ **WEP** encryption (Wired Equivalent Privacy)

WPA-PSK (WPA with pre-shared key) offers greater security than WEP. You should therefore select WPA-PSK encryption if it is supported by all components in your wireless network. WPA-PSK is an efficient method for protecting wireless networks. Dynamic keys, based on the **AES** (WPA2-PSK) or **TKIP** (WPA-PSK), offer increased security.

- ➔ In the **Wireless Network** menu, select **Wireless Security**.
- ➔ Select the desired encryption method from the **Security Mode** option menu.

WPA-PSK/WPA2-PSK Select this option for WPA-PSK or WPA2-PSK encryption.

WEP Select this option for WEP encryption.

Disabled Select this option if you want to deactivate the encryption of the wireless data transmission. It is not recommended to deactivate encryption.

WPA-PSK and WPA2-PSK

- ➔ Select **WPA-PSK/WPA2-PSK** from the **Security Mode** option menu.

The screenshot shows a configuration window titled "Wireless Security". It has a "Security Mode" dropdown menu currently set to "WPA-PSK/WPA2-PSK". Below it is a text input field for "WPA Shared Key" containing the text "Gigaset587". At the bottom right of the window are two buttons: "Save Settings" and "Cancel Changes".

- ➔ Enter a key in the **WPA Shared key** field (up to 32 characters). Use a combination of letters, digits and special characters.

Note:

Make a note of the key that you have entered. You will need this information to configure the wireless network adapters properly.

- ➔ Click **Save Settings** to apply your settings.

Advanced configuration

WEP encryption

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

You can choose either the standard 64-bit key or the more robust 128-bit key. The keys are generated in hexadecimal format. You must use the same keys for encryption and decryption for the Gigaset SE587 WLAN dsl and all your wireless network adapters.

➔ Select **WEP** from the **Security Mode** option menu.

The screenshot shows the 'Wireless Security' configuration window. The 'Security Mode' dropdown is set to 'WEP'. The 'Key Length' dropdown is set to '64 bit'. The 'Authentication Type' dropdown is set to 'Open System'. The 'Default Transmit Key' dropdown is set to 'key1'. There is a 'Passphrase' input field with a 'Generate' button next to it. Below the passphrase field are four input fields labeled 'key 1', 'key 2', 'key 3', and 'key 4', each containing the hexadecimal string '00-00-00-00-00'. At the bottom of the window are two buttons: 'Save Settings' and 'Cancel Changes'.

➔ Select **64 bit** or **128 bit** from the **Key Length** option menu.

➔ If you don't use an authentication server in your network keep the value **Open System** for the parameter **Authentication type**. Otherwise choose **Shared Key**.

You can enter up to four keys manually or generate them automatically by means of a passphrase.

Generating keys by means of a Passphrase

➔ Enter a **Passphrase** (up to 32 characters).

➔ Click **Generate** to create the keys.

Generating keys manually

➔ Enter up to four keys in fields **Key 1** to **Key 4**.

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

An example of a valid key: 12-34-56-7A-BC

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

An example of a valid key: 23-45-67-AB-C8-91-23-45-DE-F1-23-45-67

Allowed characters are 0-9 and A-F.

Advanced configuration

- ➔ Select one of the four keys as the **Default Transmit Key**. This is the key which should currently be used for encryption.

Note:

- ◆ It is very **important** that you make a note of the key(s) that have been entered or generated. You will need this information to configure the wireless network adapters properly.
- ◆ When you have concluded the configuration you must change the WEP encryption in the wireless network adapters for the connected PCs in the same way, as they will not otherwise be given access to the wireless network of the Gigaset SE587 WLAN dsl.

- ➔ Click **Save Settings** to apply your settings.

Security

The firewall functions of the Gigaset SE587 WLAN dsl include various security functions for the local network. They are activated by default and configured in the factory. If you want to deactivate the firewall, carry out the following steps:

- ➔ In the **Security** menu, select **Firewall**.

Firewall

Firewall ON OFF

Save Settings Cancel Changes

- ➔ Select the **OFF** option.
- ➔ Click **Save Settings** to apply your settings.

Access Restrictions

The **Access Restriction** function allows you to define rules for blocking access to the Internet for various services and for one or more PCs. You can permit or block access to URLs at certain times.

➔ In the **Access Restrictions** menu, select **Internet Access**.

Internet Access

● IP Filters

Operation	Host IP Address	Direction
add <input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="both"/>

● Port Filters

Modify	Protocol	Start Port	End Port	Inbound Deny	Outbound Deny
<input type="checkbox"/>	<input type="text" value="TCP"/>	<input type="text" value="80"/>	<input type="text" value="80"/>	<input type="text" value="false"/>	<input type="text" value="true"/>
<input type="checkbox"/>	<input type="text" value="UDP"/>	<input type="text" value="53"/>	<input type="text" value="53"/>	<input type="text" value="true"/>	<input type="text" value="true"/>
<input type="checkbox"/>	<input type="text" value="TCP"/>	<input type="text" value="53"/>	<input type="text" value="53"/>	<input type="text" value="true"/>	<input type="text" value="true"/>
<input type="checkbox"/>	<input type="text" value="TCP"/>	<input type="text" value="21"/>	<input type="text" value="21"/>	<input type="text" value="false"/>	<input type="text" value="true"/>
<input type="checkbox"/>	<input type="text" value="TCP"/>	<input type="text" value="23"/>	<input type="text" value="23"/>	<input type="text" value="false"/>	<input type="text" value="true"/>
<input type="checkbox"/>	<input type="text" value="TCP"/>	<input type="text" value="25"/>	<input type="text" value="25"/>	<input type="text" value="false"/>	<input type="text" value="true"/>
<input type="checkbox"/>	<input type="text" value="TCP"/>	<input type="text" value="110"/>	<input type="text" value="110"/>	<input type="text" value="false"/>	<input type="text" value="true"/>
<input type="checkbox"/>	<input type="text" value="TCP"/>	<input type="text" value="119"/>	<input type="text" value="119"/>	<input type="text" value="false"/>	<input type="text" value="true"/>
<input type="checkbox"/>	<input type="text" value="UDP"/>	<input type="text" value="7070"/>	<input type="text" value="7070"/>	<input type="text" value="true"/>	<input type="text" value="true"/>
<input type="checkbox"/>	<input type="text" value="TCP"/>	<input type="text" value="1720"/>	<input type="text" value="1720"/>	<input type="text" value="true"/>	<input type="text" value="true"/>
<input type="checkbox"/>	<input type="text" value="TCP"/>	<input type="text" value="1503"/>	<input type="text" value="1503"/>	<input type="text" value="true"/>	<input type="text" value="true"/>
<input type="checkbox"/>	<input type="text" value="TCP"/>	<input type="text" value="22"/>	<input type="text" value="22"/>	<input type="text" value="true"/>	<input type="text" value="true"/>
<input type="checkbox"/>	<input type="text" value="UDP"/>	<input type="text" value="123"/>	<input type="text" value="123"/>	<input type="text" value="true"/>	<input type="text" value="true"/>

● URL Filters

Operation	Domain Filter	Start Time (hh:mm:ss)	End Time (hh:mm:ss)
add <input type="checkbox"/>	<input type="text"/>	<input type="text" value="00:00:00"/>	<input type="text" value="00:00:00"/>

Rule For All Above Allow Deny

Advanced configuration

IP Filters

In the IP filter list you can add the PCs for which access should be restricted.

- ➔ Select the **add** box to activate the fields in a row to create a new entry.
- ➔ In the **Host IP Address** field, enter the IP address of the respective PC. How to find out the IP addresses of the individual PCs is described in chapter "Local network configuration" on page 36.
- ➔ From the **Direction** option menu, select the kind of communication to which the restriction should apply:
 - inbound** Internet access is restricted to outgoing data traffic.
 - outbound** Internet access is restricted to incoming data traffic.
 - both** Both incoming and outgoing data traffic with the Internet are restricted.
- ➔ Select the **del** box to delete an entry from the list.

Port Filters

In the port filter list you can define ports or port ranges to restrict the access of specific Internet services. Each Internet service uses a specific port for communication. The following table shows some important port numbers of Internet services:

Internet service	Protocol	Port number
FTP	TCP	21
ssh / pcAnywhere	TCP	22
Telnet	TCP	23
SMTP	TCP	25
TFTP	TCP	53
HTTP	TCP	80
POP3	TCP	110
NNTP	TCP	119
HTTPS	TCP	443
T.120	TCP	1503
H.323/Q931	TCP	1720
DNS	UDP	53
NTP	UDP	123
RealServer / QuickTime	UDP	7070

- ➔ Select the **Modify** box to activate the fields in a row. You can change the values if required.
- ➔ Select the **Protocol** used by the service(s) and enter the **Start Port** and the **End Port** of the port range to be restricted. To specify one specific service with one port number enter the same port number in the **Start Port** and the **End Port** field.
- ➔ From the **Inbound Deny** and **Outbound Deny** option menus choose if the rule should apply to incoming and/or outgoing traffic.

URL filter

The URL filter allows you to block or allow access to specific Internet domains.

- ➔ Select the **add** box to activate the fields in a row to create a new entry.
 - ➔ Enter the URL of the domain to be blocked or allowed in the **Domain Filter** field. The domain is blocked or allowed including all subdomains.
 - ➔ In the **Start Time** and **End Time** fields you can define a time period for which the domain filter should apply.
 - ➔ Use the **Rule For All Above** option to specify if the domains entered in the list should be blocked or allowed. If you select **Allow** only the domains contained in the list can be accessed from the users of your network. If you select **Deny** only the domains contained in the list are blocked. All other domains can be accessed.
 - ➔ Select the **del** box to delete an entry from the list.
- ➔ Click **Save Settings** to apply all your settings on this page.

Applications and Gaming

The Gigaset SE587 WLAN dsl comes equipped with the **NAT** (Network Address Translation) function. With address mapping, several users in the local network can access the Internet via one or more public IP addresses. All the local IP addresses are assigned to the router's public IP address by default.

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

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

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

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

When the Gigaset SE587 WLAN dsl is supplied, the NAT function is activated, i.e. all IP addresses of PCs in the local network are converted to the router's public IP address when accessing the Internet.

Advanced configuration

You can use the NAT settings to configure the Gigaset SE587 WLAN dsl to carry out the following tasks:

- ◆ Set up the Gigaset SE587 WLAN dsl as a virtual server by configuring Port Forwarding (see below).
- ◆ Open the NAT firewall for a selected PC (page 29).

Port Forwarding

If you configure Port Forwarding, the Gigaset SE587 WLAN dsl outwardly assumes the role of the server. It receives requests from remote users under its public IP address and automatically redirects them to local PCs. The private IP addresses of the servers on the local network remain protected.

Internet services are addressed via defined port numbers. The Gigaset SE587 WLAN dsl needs a mapping table of the port numbers to redirect the service requests to the servers that actually provide the service.

➔ In the **Applications & Gaming** menu, select **Port Forwarding**.

Port Forwarding						
Operation	Interface	Protocol	Public Port	Local Port	Local IP	
add <input type="checkbox"/>	ipwan	tcp	65535	65535	0.0.0.0	
add <input type="checkbox"/>	ipwan	Predefined Applications:		FTP	0.0.0.0	
			Save Settings		Cancel Changes	

You can choose a service from a list of predefined applications or create an entry manually.

- ➔ Select the **add** box to activate the fields in a row to create a new entry.
- ➔ If more than one interface is configured select the **Interface** for which the port forwarding should apply from the option menu.
- ➔ Select the required application from the **Predefined applications** list.
- ➔ Enter the IP address of the PC that provides the service in the **Local IP** field. How to determine the IP addresses of the individual PCs is described in chapter "Local network configuration" on page 36.

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

- ➔ Select the **add** box to activate the fields in a row to create a new entry.
- ➔ If more than one interface is configured select the **Interface** for which the port forwarding should apply from the option menu.
- ➔ 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.

Advanced configuration

- ➔ In the **Local port** field, enter the internal port number to which service requests are to be forwarded.
- ➔ Enter the IP address of the PC that provides the service in the **Local IP** field. How to find out the IP addresses of the individual PCs is described in chapter "Local network configuration" on page 36.

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

- ➔ Select the **del** box to delete an entry.
- ➔ Click **Save Settings** to apply your settings.

DMZ

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

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

Note:

Only one PC per public IP address (interface) can be set up as a DMZ.

- ➔ In the **Applications & Gaming** menu, select: **DMZ**

Operation	Interface Name	Current Host IP
add <input type="checkbox"/>	ipwan	0.0.0.0

Save Settings Cancel Changes

- ➔ Select the **add** box to activate the fields in a row to create a new entry.
- ➔ If more than one interface is configured select the **Interface** for which the DMZ should apply from the option menu.
- ➔ Enter the IP address of the PC that is to be enabled as DMZ in the **Current Host IP** field.
- ➔ Click **Save Settings** to apply your settings.

Administration

Administration

The Gigaset SE587 WLAN dsl user interface includes several helpful functions for administering your device.

- Management** provides functions to enable or restrict access to the configuration user interface (page 30).
- Log** displays logged information about the operation (page 32).
- Factory Defaults** allows you to reset the Gigaset SE587 WLAN dsl to the factory settings (page 33).
- Firmware Upgrade** allows you to update the firmware of the device (page 33).
- Config Management** offers functions to back up and, if necessary, restore the configuration data of your device (page 34).

Management

Your Gigaset SE587 WLAN dsl allows you to restrict access to the device's configuration to specific local or remote users.

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

Authentication

User	Comment	Operation
admin	Admin user	<input type="button" value="Edit User"/>
<input type="button" value="Add New User"/>		

Remote Management

Remote Access Disabled

UPnP

UPnP IGD Enabled Disabled

Authentication

To access the configuration user interface of your Gigaset SE587 WLAN dsl users must login with a user ID and an assigned password. The existing user IDs are shown in the authentication list. You can change the preset password for the default user **admin** here.

Creating a new user ID

➔ To create a new user click on **Add New User**.

Username

Password

Comment

➔ Enter a **Username** and a **Password** for the new user.

➔ Enter a **Comment** which makes it easier to identify the user.

➔ Click on **Create User** to create the new entry.

The new user is shown in the list.

Editing an existing user entry

In order to change the password or the comment for a user use the **Edit User** function.

➔ In the row of the respective user, click on **Edit User**.

Username admin

Password

Comment Admin user

➔ Change the desired property.

➔ Click on **Save Setting** to apply your changes.

Remote Management

You can decide if remote access to the configuration user interface of your Gigaset SE587 WLAN dsl is to be enabled or not. It is disabled by default.

The port number a remote user will have to enter in the browser's address bar for remote management is 80. This means that, if the router's public IP address is for example 12.34.56.78, the user will have to type http://12.34.56.78:80 into the browser's address bar to access the user interface of the Gigaset SE587 WLAN dsl.

➔ To enable remote access, if disabled, click on **Enable**.

➔ To disable remote access, if enabled, click on **Disable**.

The action is executed immediately.

Administration

UPnP IGD (Universal Plug and Play)

UPnP allows devices to offer their own network services and automatically use services offered in the network. UPnP IGD (Internet Gateway Device) comes with a solution for routers which support NAT (Network Address Translation, see page 27). NAT traversal for UPnP enables UPnP packages to pass through a router or firewall without problems and without user interaction.

- ➔ Enable or disable the UPnP IGD feature.
- ➔ Click **Save Settings** to save and apply all the changes on this page.

Log

During operation important events and information about how the device functions and possible problems are logged. The **Log** page displays the logged information.


- ➔ In the **Administration** menu, select **Log**.

Time	Event
2 days, 00:00:03	im:Changed iplan IP address to 192.168.1.1
2 days, 00:00:20	webserver:Changed iplan IP address to 192.168.1.3
2 days, 00:01:40	security:Session -- Prot: 2, 0.0.0.0:0 > 239.255.255.250:0 49.363 ~ 110.919 size 64/0 time-out

- ➔ Specify which information is to be displayed from the option menu. You can choose between the following levels:
 - All events** All events are displayed.
 - Configuration errors** Only configuration errors are displayed.
 - Syslog messages** All events contained in the system log are displayed.
- ➔ Click **View** to display the desired information.
- ➔ Click **Clear** to remove logged information from the screen and delete it from the device's memory.

Factory Defaults

You can reset the Gigaset SE587 WLAN dsl to the factory settings. You should do this only if you want to make the device available to others or exchange it through the dealer. In this case unauthorised persons could use the Internet access data at your expense.

	Do not perform this action without first consulting the Tiscali hotline.
---	--

➔ In the **Administration** menu, select **Factory Defaults**.

Factory Defaults

Restore Factory Defaults

Reset to factory default settings

➔ Select **Reset to factory default settings** and click **Restart**.

A window will appear prompting you to confirm the procedure.

Note:

If the Gigaset SE587 WLAN dsl is not operating correctly, you can reboot it by switching it off and restarting it. It should then be ready for use again.

Please bear in mind that when the device is fully reset, **all** configuration settings are returned to the factory settings. This means that you will have to completely reconfigure the Gigaset SE587 WLAN dsl.

Firmware Upgrade

If Tiscali releases a new version of the firmware, you can update the firmware of the Gigaset SE587 WLAN dsl. To do this you must first download the new firmware onto your PC.

➔ In the **Administration** menu, select **Firmware Upgrade**.

Upgrade Firmware


Please select file to upgrade

Warning

Upgrading to any firmware other than Tiscali approved firmware may disable access to the internet or TV services. Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button. **Upgrade must NOT be interrupted!**

Administration

- ➔ In the text field, enter the file with the new firmware that you have downloaded from the Internet or click **Browse** to search for the file in your PC's file system.
- ➔ Click **Upgrade**. The firmware will now be updated.

	Do not switch off the Gigaset SE587 WLAN dsl during the updating procedure and do not interrupt the power supply. Switching off the device can make it unusable. The update can take several minutes.
---	--

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

To see whether the upgrade procedure was completed successfully, check the current software version displayed on the **Device** page in the **Status** menu (page 15).

Configuration Management

When the Gigaset SE587 WLAN dsl has been configured, it is recommended that you back up the settings. This means you can restore the settings at any time if they are accidentally deleted or overwritten.

- ➔ In the **Administration** menu, select: **Config Management**.



Backing up configuration data

- ➔ Click **Backup** to start saving.
- You can then set the location in which the backup file is to be saved in a file selection window.
- ➔ Select a local directory on your PC where you want to save the configuration file and enter a file name.
 - ➔ Click **Save**.

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

Restoring the saved configuration

- ➔ In the text field, enter the file with the saved configuration or click **Browse** to search for the file in your PC's file system.
- ➔ In the file system, select the backup file that you want to use to restore the configuration.
- ➔ Click **Restore**.

The configuration will now be updated.

Local network configuration

Local network configuration

Modern computers running Windows Vista, Windows XP, Windows 2000 or Mac OS X operating systems are usually already configured on delivery to operate without difficulty in a wired local network (Ethernet/LAN) or wireless network (WLAN). The connection to a router or access point is established automatically in this case.

Note:

You can check whether your PC already has a connection to a router or access point by simply entering the **ping** command at the command prompt of your Windows operating system or at the Terminal of your Mac OS X. Please refer to Section „Checking the connection to the Gigaset SE587 WLAN dsl“ on page 63 for further details.

If there is no connection to a Gigaset SE587 WLAN dsl as yet, you may need to adapt the network settings on the computer.

- ◆ You have to define the network name and the encryption on the computer for a wireless connection (see page 38).
- ◆ Network addresses (IP addresses) are normally assigned automatically. To change the default settings of your operating system for assigning IP addresses, you have to change the TCP/IP settings. You will find further information about this topic in the Section "IP addresses" after a short introduction. The TCP/IP settings for the various operating system variants are then described from page 42 onwards.
- ◆ If you are still using Windows 98, you will need to install TCP/IP and set up a network on the PC if your PC has not been operated previously in a network (see page 52).

IP addresses

Every PC in the network must have a unique network address, referred to as the IP address, so that it can be accessed by and differentiated from the other components in the network.

Your Gigaset SE587 WLAN dsl is equipped with a DHCP server, which performs the addressing in the network independently. This means that the IP addresses are automatically assigned to the computers (dynamic IP addresses).

Under normal circumstances you therefore do not have to do anything because the **Obtain an IP address automatically (Using DHCP for Mac OS X)** option is set when the network is set up.

It is advisable in some cases, however, to assign static IP addresses, for example if you wish to run a wireless network in ad-hoc mode or want to make PC services available on the Internet. In this case, you have to change the network settings of the PCs and configure static IP addresses.

Information on assigning static IP addresses

You define the private IP addresses for the computers in your local network yourself. Addresses from an address block reserved for private use should be used. This is the address block

192.168.0.1 - 192.168.255.254

Example:

PC 1: 192.168.1.2

PC 2: 192.168.1.3 etc.

Please remember:

The IP addresses you can assign also depend on the subnet mask for your network. The subnet mask used limits the IP addresses that can be assigned as it determines how many parts of the IP address of a network represent the network number and how many the computer number.

255.255.255.0 is normally used in a private network as the subnet mask. This means the first three parts of the IP address form the network number and the final part can be used for assigning computer numbers. The first three parts of the IP address of all network components are therefore always the same. In the case of subnet mask 255.255.0.0, the first two address parts would have to be identical.

An example of subnet mask 255.255.255.0 is given below.

For example, this is correct:

Address of access point: 192.168.1.1

Computer 1: 192.168.1.12

Computer 2: 192.168.1.60 ...

This is incorrect:

Address of access point: 192.168.1.1

Computer 1: 192.168.2.2

Computer 2: 192.168.3.3

Computer names and workgroups

When your network is being set up, your computer is assigned a name. This is carried out when the operating system is installed (with the exception of Windows 98), i.e. your computer already has a computer name when it is delivered. The computer name is the name under which your computer is displayed in the network view.

You can change the computer name, if desired.

Windows operating systems

When your network is set up, your PC is assigned to a workgroup. This is carried out when the operating system is installed (with the exception of Windows 98), i.e. your PC has already been assigned by default to a standard working group (usually WORKGROUP). The workgroup includes a number of PCs that belong to a network and can share common resources, such as printers and files. You can change the workgroup to which your PC has been assigned.

Local network configuration

Setting up a wireless network

A wireless network connection is made using a wireless adapter that must be installed on your computer. You may first have to connect a wireless adapter to your notebook or your computer. For example, this can be a Gigaset USB Adapter, a Gigaset USB Stick or a Gigaset PC Card, but also a different IEEE 802.11n, 802.11g or 802.11b-compatible wireless adapter. If you are using this type of wireless adapter, you can set up the connection to the wireless network using the relevant software. Instructions for this can be found in the user manual for your wireless adapter.

Most modern notebooks already have a wireless adapter fitted when delivered. In this case, you should use the tools provided by the operating system to connect the PC, notebook or Mac to the wireless network.

We explain below how to connect a PC or notebook to a wireless network using Windows XP SP2, Windows Vista and Mac OS X.

To set up the connection, you need the network name (SSID) of your wireless network and the key defined on the Gigaset SE587 WLAN dsl for encrypting wireless data traffic.

Note:

The preset SSID and WPA key are shown on the label on the bottom of the device.

Carry out the following steps:

- ➔ Start your notebook or your computer. Make sure your wireless adapter is switched on. Notebooks generally have a switch for this purpose as well as an LED as a function display.

Windows XP

If Windows XP receives signals of wireless networks in the current environment this will be indicated by the symbol for the wireless network connection in the status area of the taskbar.



- ➔ Right-click the icon in this case and choose the **Show available wireless networks** option.

If the icon for the wireless network connection is not displayed, you could also proceed as follows:

- ➔ Choose **Start - Control Panel - Network Connections - Wireless Network Connections**

Or

- ➔ Double-click the **Network Environment** icon on the desktop.
- ➔ Click **Show network connections** in the column on the left.
- ➔ Double-click the **Wireless Network Connections** icon.

The list of available and visible wireless networks (WLANs) is displayed (see page 39).

Windows Vista

- ➔ Click the network symbol in the status area of the taskbar to display the wireless networks in the current environment.
- ➔ Click **Connect or disconnect**.



A list of all available wired and wireless networks (WLANs) is displayed (see page 39).

Note:

The automatic wireless configuration service must be started so that Windows can display and manage wireless networks. If nothing is displayed on your PC despite there being wireless networks within range, check whether the service is started and start it if necessary.

Windows Vista:

- ➔ Click **Start – Control Panel – System and Maintenance – Administrative Tools**.
- ➔ Double-click **Services**.
- ➔ Check whether the **Automatic WLAN Configuration** service is started and start it if necessary by clicking **Start** in the column on the left.

Windows XP:

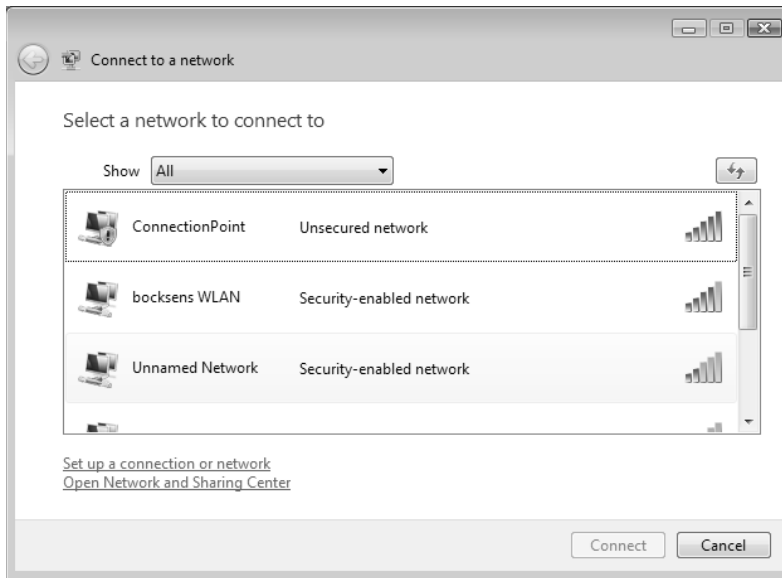
- ➔ Click **Start - Control Panel**.
- ➔ Click **Administrative Tools** and then **Services**.
- ➔ Check whether the service **Wireless Zero Configuration** is started and start it if necessary by clicking **Start** in the column on the left.

Network list

All wireless networks that can be seen at the current location appear in the network list. If the SSIDs of the wireless networks are set to invisible they are not displayed. Windows shows the status of each wireless network graphically and provides information on the signal strength, the network name and whether security settings were made for the respective network.

An example for Windows Vista is given below.

Local network configuration



➔ To sign your computer on to your own wireless network, double-click the name (SSID) of your network.

If encryption is defined on the Gigaset SE587 WLAN dsl, you will be asked to type in the key entered there (WEP key or Pre-Shared Key).

➔ Enter the appropriate key.

➔ Click **Connect**.

The wireless connection is established automatically.

Mac OS X

If Mac OS X receives signals of wireless networks in the current environment this will be indicated by the symbol for the wireless network connection in the status area of the menu bar.



If Mac OS X sees wireless networks without security settings in the current environment, a message appears after booting the computer stating that you can connect your computer to an open network. Even if your router has no security settings in the default mode, you should avoid working with an unsecured wireless network. First carry out the security settings of your router.

➔ Click the symbol for the wireless network connection in the status area of the menu bar.

A list opens showing all wireless networks available in the second section.



Note:

AirPort (WLAN) must be activated so that Mac OS X can display and manage wireless networks. If nothing is displayed on your Mac despite there being wireless networks within range, check whether AirPort is activated and activate it if necessary.

➔ You can find this setting in the first section of the list for the wireless networks. If AirPort is deactivated, click the option **AirPort: On**.

Network list

All wireless networks that can be seen at the current location appear in the network list. If the SSIDs of the wireless networks are set to invisible they are not displayed.

➔ To sign your computer on to your own wireless network, click the name (SSID) of your network.

If encryption is defined on the Gigaset SE587 WLAN dsl, you will be asked to type in the key entered there (e. g. WEP key or Pre-Shared Key).

➔ Enter the appropriate key.


➔ Click **Connect**.

The wireless connection is established automatically.

Local network configuration

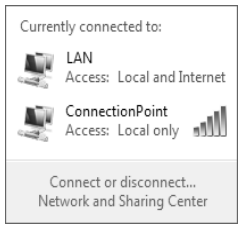
Network configuration with Windows Vista

Showing networks

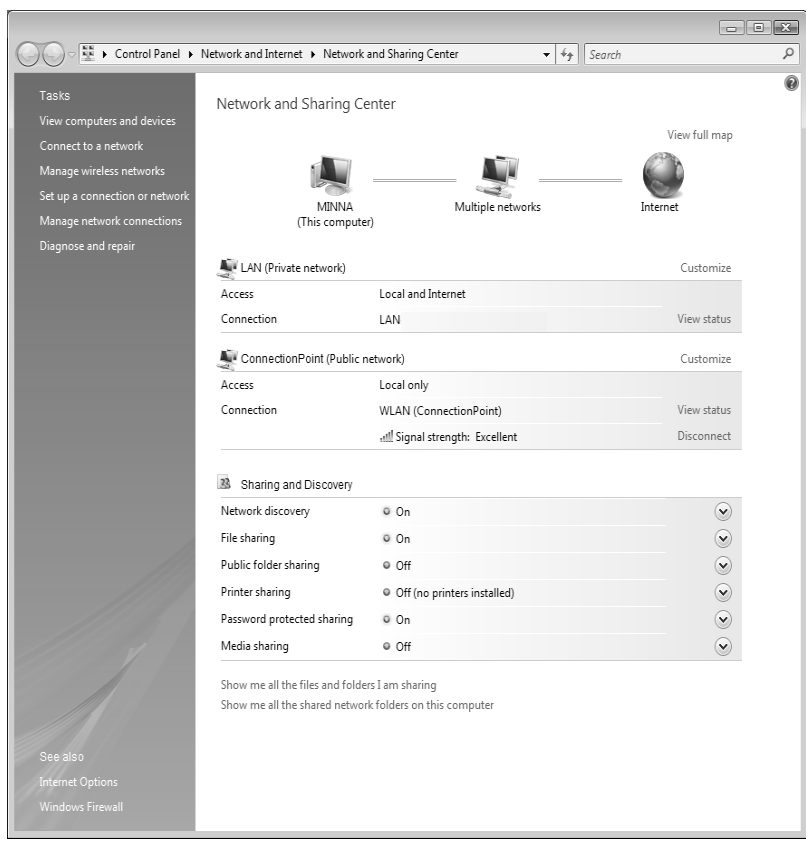
You can view the available networks by clicking the  icon on the taskbar.

➔ Click the icon.

Networks that are currently connected are displayed.



➔ Click **Network and Sharing Center**.



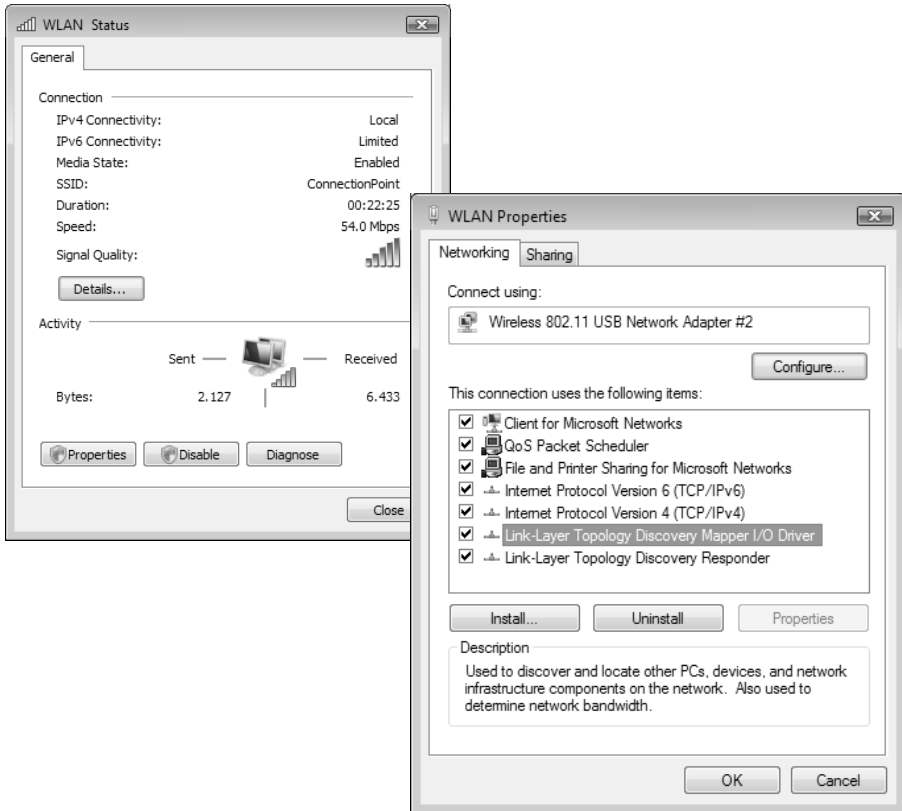
Local network configuration

An overview of your PC's network connections are displayed in the Network and Sharing Center. You can start all actions for your network configuration from here.

Changing the settings for IP addresses

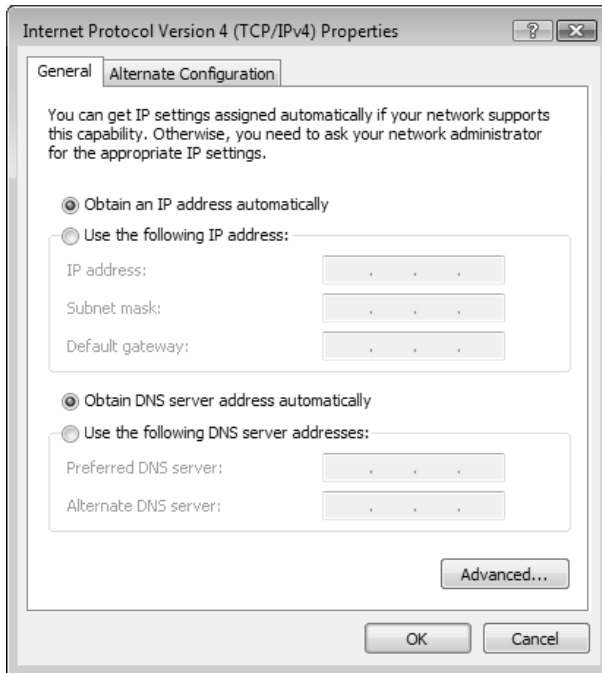
The IP addressing settings can be checked and modified as follows:

- ➔ Click **View status** next to the network connection used to connect your PC to the Gigaset SE587 WLAN dsl.
- ➔ Click **Properties**.



- ➔ Choose the entry **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties** again.

Local network configuration



Obtaining an IP address automatically

If the DHCP server of your router/access point is active and the PC is to obtain its IP address automatically, the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options must be activated.

- ➔ Check whether these options are selected and mark them if necessary.
- ➔ Click **OK** and close the following windows with **OK** to save your network configuration.

Assigning an IP address statically

If the DHCP server of your router/access point is not active or the PC is to be assigned a static IP address for other reasons, the following settings must be made:

- ➔ Select the option **Use the following IP address**.
- ➔ Enter the IP address for the PC in the **IP address** field.
- ➔ Enter the subnet mask to be used in your network in the **Subnet mask** field. You can check these settings if necessary in the LAN configuration for your router/access point.
- ➔ Enter the IP address for the router/access point in the **Default gateway** field.
- ➔ Select the option **Use the following DNS server addresses**.
- ➔ Enter the IP address for the router/access point in the **Preferred DNS server** field.
- ➔ Click **OK** and then **Close** to close all windows.

Selecting a computer name and workgroup

Your PC is assigned a name during installation and assigned to the default workgroup **WORKGROUP**. To change the name or the workgroup assignment, you have to:

- ➔ Click **Start - Control Panel - System and Maintenance**.
- ➔ Click the entry **Show computer name** under **System**.
The name of the PC and its workgroup are displayed in the window.
- ➔ Click **Change settings**.
- ➔ You can enter a description for the PC in the **Computer description** field on the **Computer Name** tab. You do not have to fill in this field however.
- ➔ Click **Change**.
- ➔ Enter the name the PC is to appear under in the network. This name must be unique within the network.
- ➔ Enter a name for the workgroup to which the PC is to be assigned. This name must be identical on all PCs for the same workgroup.
- ➔ Click **OK**.

Network configuration with Windows XP

Note:

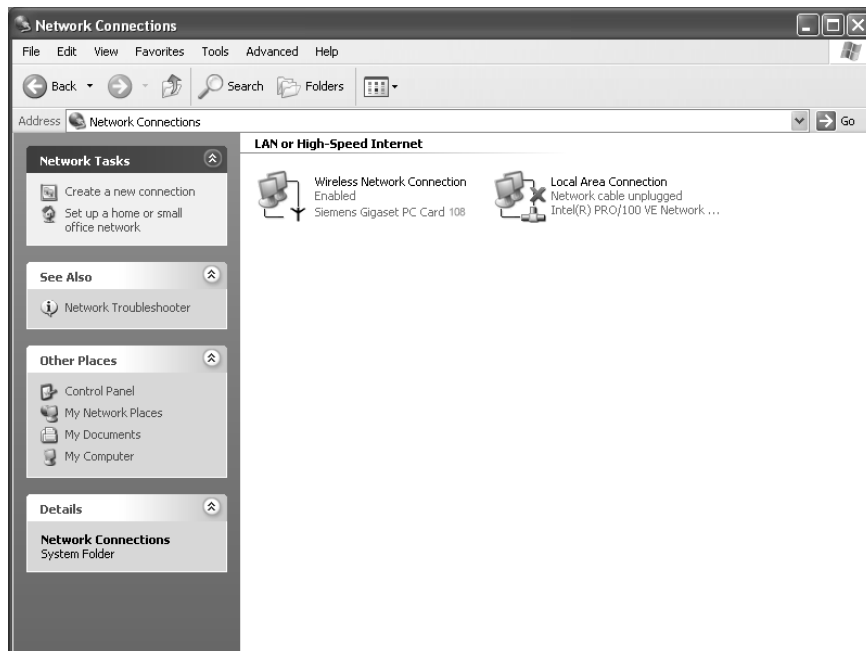
The names of the menu items may differ slightly from one version of Windows XP to another. However, the configuration settings described below generally apply.

Showing networks

- ➔ Click **Start - Control Panel** and select **Network Connections** or
- ➔ Click the network icon in the status area of the taskbar.

The configured networks are displayed.

Local network configuration



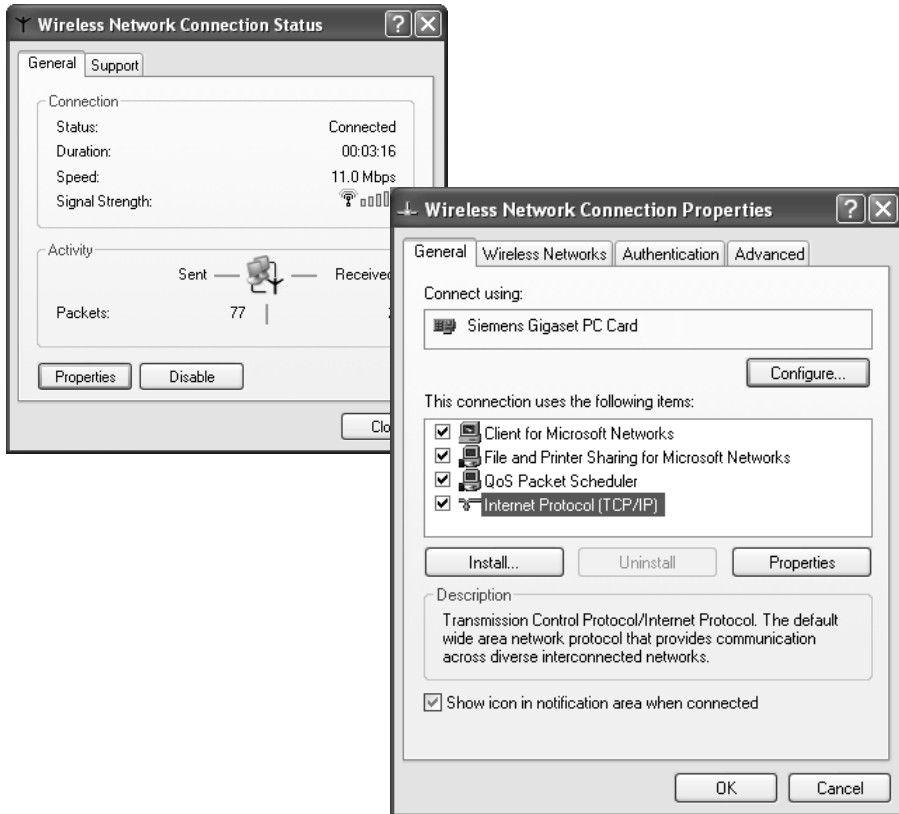
Changing the settings for IP addresses

The IP addressing settings can be checked and modified as follows:

- ➔ Double-click the wireless network or local area connection used to connect your PC to the Gigaset SE587 WLAN dsl.

The status window for the connection is opened.

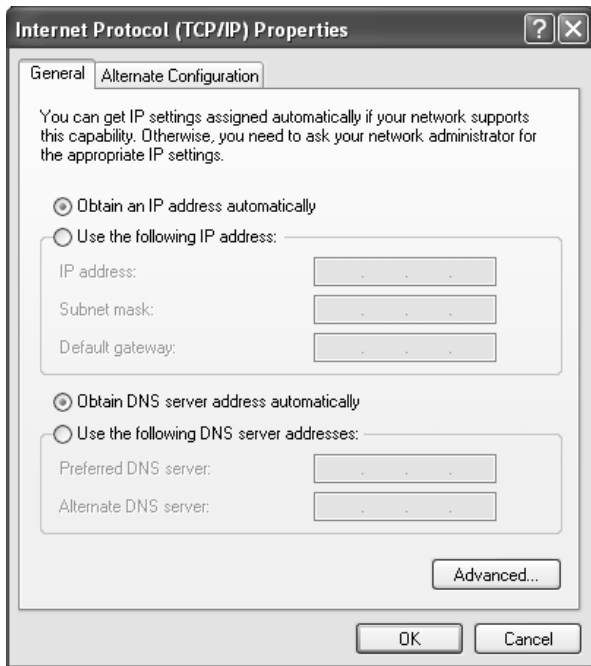
Local network configuration



➔ Click **Properties**.

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

Local network configuration



Obtaining an IP address automatically

If the DHCP server of your router/access point is active and the PC is to obtain its IP address automatically, the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options must be activated.

- ➔ Check whether these options are selected and mark them if necessary.
- ➔ Click **OK** and close the following windows with **OK** to save your network configuration.

Assigning an IP address statically

If the DHCP server of your router/access point is not active or the PC is to be assigned a static IP address for other reasons, the following settings must be made:

- ➔ Select the option **Use the following IP address**.
- ➔ Enter the IP address for the PC in the **IP address** field.
- ➔ Enter the subnet mask to be used in your network in the **Subnet mask** field. You can check these settings if necessary in the LAN configuration for your router/access point.
- ➔ Enter the IP address for the router/access point in the **Default gateway** field.
- ➔ Select the option **Use the following DNS server addresses**.
- ➔ Enter the IP address for the router/access point in the **Preferred DNS server** field.
- ➔ Click **OK** and then **Close** to close all windows.

Selecting a computer name and workgroup

Your PC is assigned a name during installation and assigned to the default workgroup **WORKGROUP**. To change the name or the workgroup assignment, you have to:

- ➔ Click **Start - Control Panel - System**.
- ➔ Select the **Computer Name** tab.

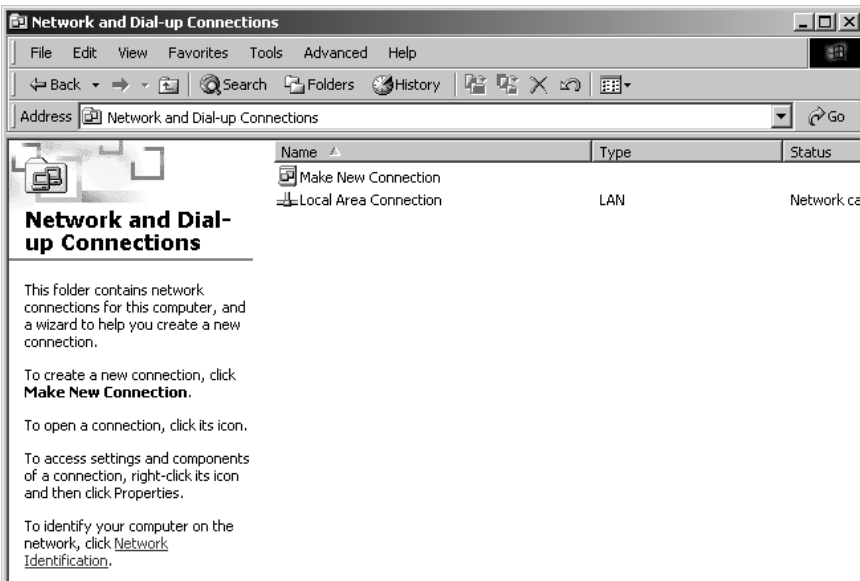
The name of the PC and its workgroup are displayed in the window.
- ➔ You can enter a description for the PC in the **Computer description** field on the **Computer Name** tab. You do not have to fill in this field however.
- ➔ Click **Change**.
- ➔ Enter the name the PC is to appear under in the network. This name must be unique within the network.
- ➔ Enter a name for the workgroup to which the PC is to be assigned. This name must be identical on all PCs for the same workgroup.
- ➔ Click **OK**.

Network configuration with Windows 2000

Showing networks

- ➔ Click **Start - Settings - Control Panel**.
- ➔ Double-click the **Network and Dial-up Connections** icon.

All available networks are displayed.

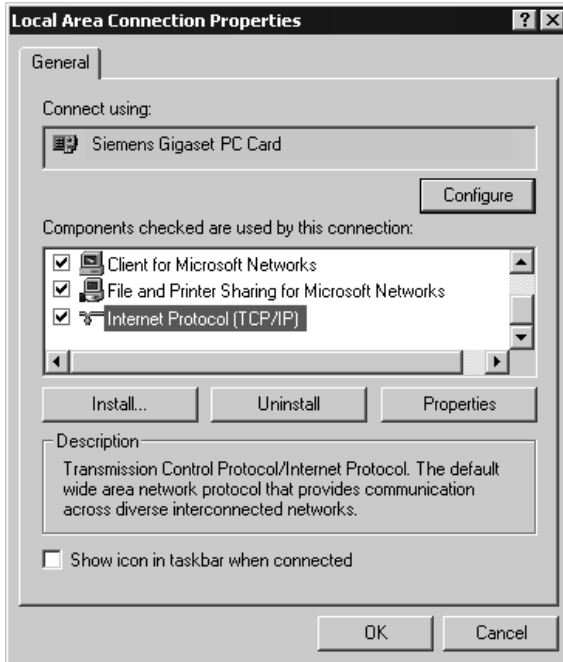


Local network configuration

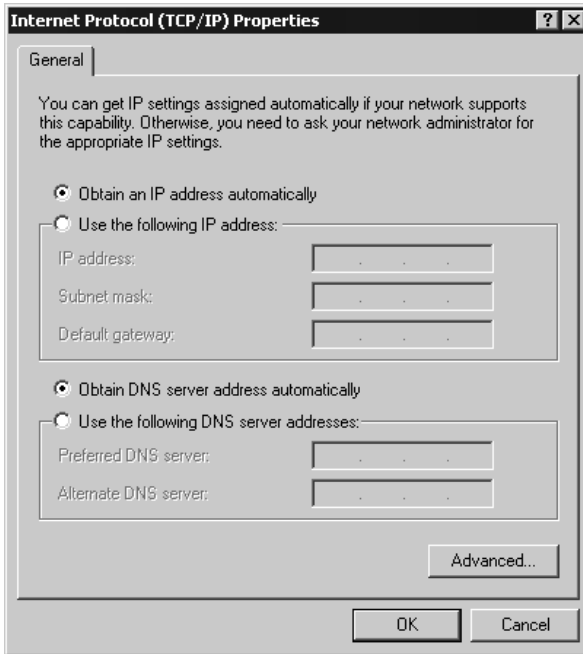
Changing the settings for IP addresses

The IP addressing settings can be checked and modified as follows:

- ➔ Double-click the wireless network or local area connection used to connect your PC to the Gigaset SE587 WLAN dsl.
 - The status window for the connection is opened.
- ➔ Click **Properties**.



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



Obtaining an IP address automatically

If the DHCP server of your router/access point is active and the PC is to obtain its IP address automatically, the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options must be activated.

- ➔ Check whether these options are selected and mark them if necessary.
- ➔ Click **OK** and close the following windows with **OK** to save your network configuration.

Assigning an IP address statically

If the DHCP server of your router/access point is not active or the PC is to be assigned a static IP address for other reasons, the following settings must be made:

- ➔ Select the option **Use the following IP address**.
- ➔ Enter the IP address for the PC in the **IP address** field.
- ➔ Enter the subnet mask to be used in your network in the **Subnet mask** field. You can check these settings if necessary in the LAN configuration for your router/access point.
- ➔ Enter the IP address for the router/access point in the **Default gateway** field.
- ➔ Select the option **Use the following DNS server addresses**.
- ➔ Enter the IP address for the router/access point in the **Preferred DNS server** field.
- ➔ Click **OK** and then **Close** to close all windows.

Local network configuration

Selecting a computer name and workgroup

Your PC is assigned a name during installation and assigned to the default workgroup **WORKGROUP**. To change the name or the workgroup assignment, you have to:

- ➔ Click **Start – Settings – Control Panel – System**.
- ➔ Select the **Network Identification** tab and click **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 the same for all the PCs in the network.
- ➔ Confirm this with **OK**.

Network configuration with Windows 98, SE, ME

To integrate a PC with Windows 98 SE or ME into a local network, you have to carry out the following steps:

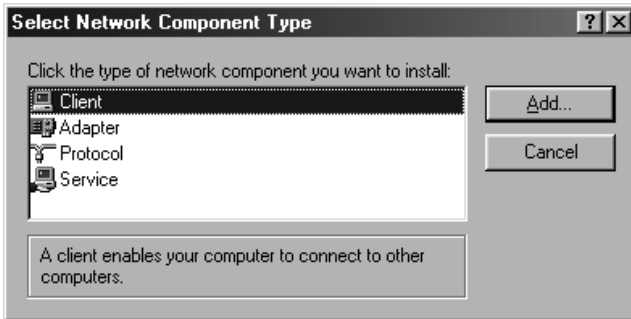
1. Set up the PC as a client for Microsoft networks (see below).
2. Select computer names and workgroup (see page 53).
3. Install the TCP/IP protocol (see page 54).
4. Make TCP/IP protocol settings (see page 55).
5. Synchronise the TCP/IP settings with the Gigaset SE587 WLAN dsl (see page 62).

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

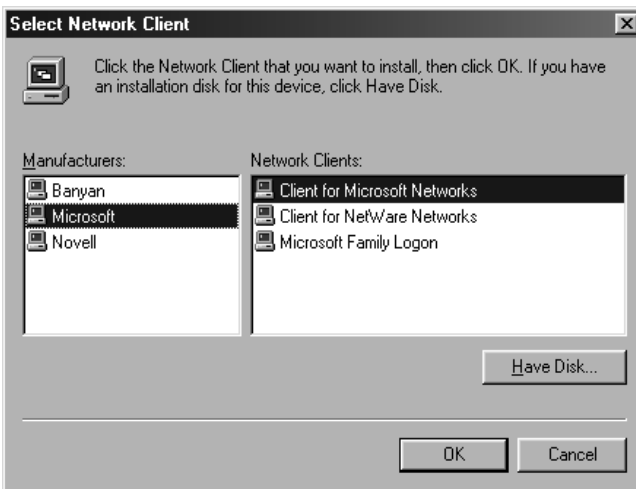
Setting up a PC as a client for Microsoft networks

Before the PCs in your network can work together, you have to configure them as clients of a Microsoft network. This is done as follows:

- ➔ Click **Start – Settings – Control Panel**.
- ➔ Double-click the **Network** icon and then open the **Configuration** tab in the **Network** window.
- ➔ Check whether the list of components contains the entry **Client for Microsoft Networks**.
- ➔ If it is not there click **Add**.



➔ Select **Client** as the network component type and click **Add**.



➔ Under **Manufacturers** select **Microsoft** and under **Network Clients** select **Client for Microsoft Networks**.

➔ Confirm this with **OK**.

Selecting a computer name and workgroup

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

➔ In the **Network** window, change from the **Configuration** tab to **Identification**.

➔ 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 the same for all the PCs in the network.

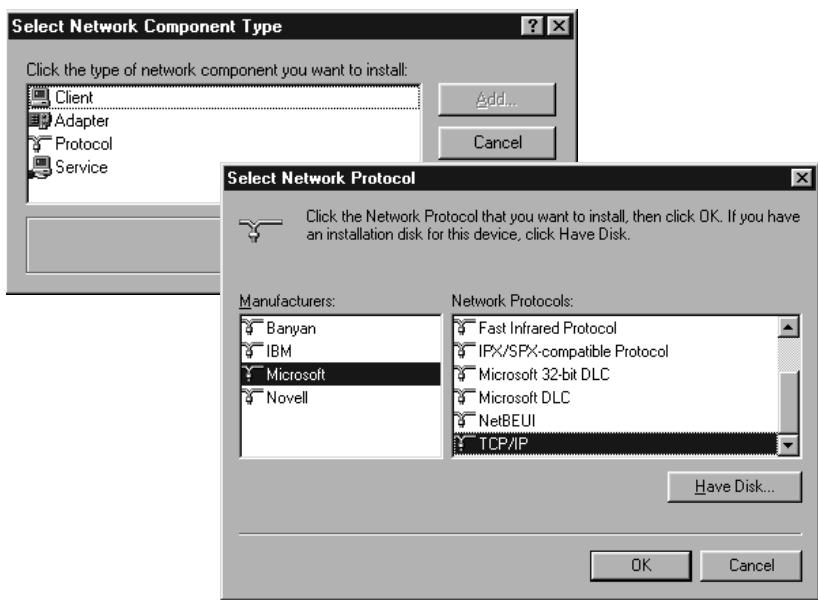
The **Computer Description** field can be left blank.

Local network configuration

Installing the TCP/IP protocol

The TCP/IP protocol ensures that the PCs in the network can communicate with each other. You must first install this protocol for the network adapter that establishes the connection with the Gigaset SE587 WLAN dsl.

- ➔ In the **Network** window, change from the **Identification** tab to **Configuration**.
- ➔ In the **Network** window, check that there is a TCP/IP -> entry for your network card or network adapter in the list of components. If, for example, you are using a Gigaset PC Card 108 as the wireless network adapter, the list must contain the entry **TCP/IP -> Siemens Gigaset PC Card 108**.
- ➔ If the entry does not exist, click **Add**.

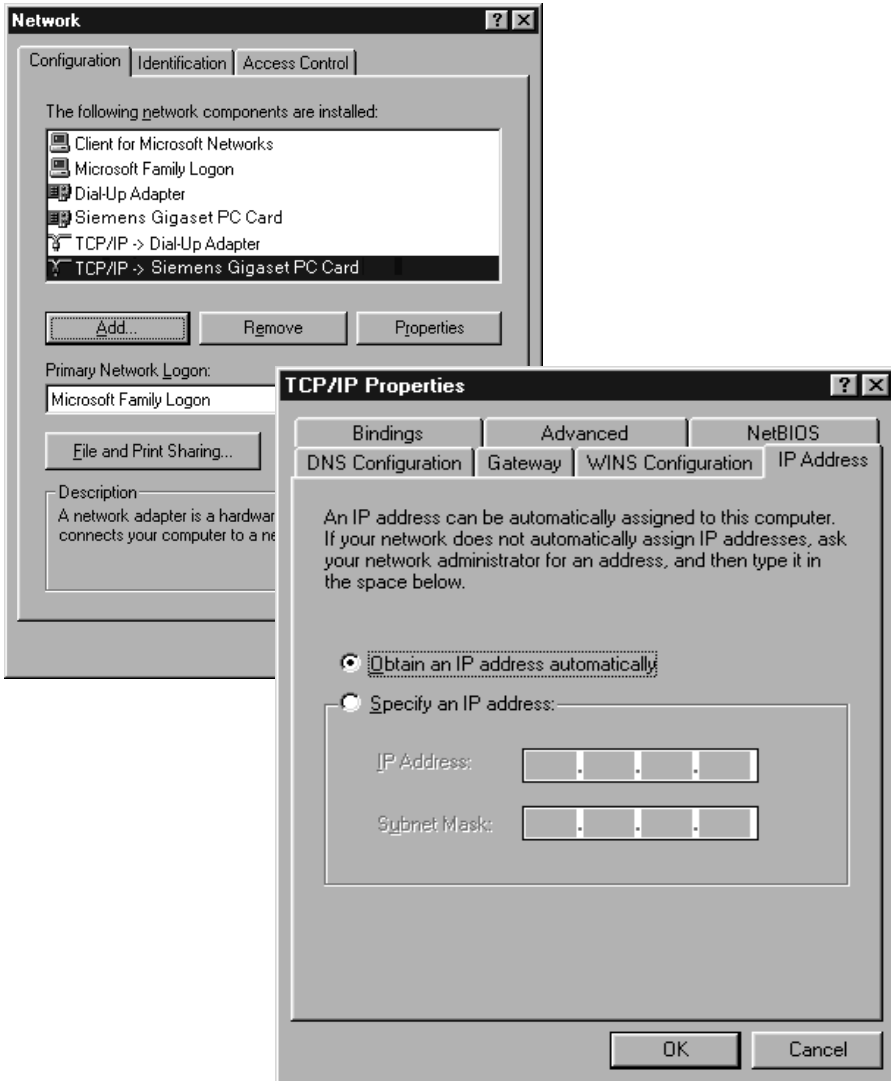


- ➔ Select **Protocol** as the network component type and click **Add**.
- ➔ Under **Manufacturers** select **Microsoft** and under **Network Protocols** select **TCP/IP**, and click **OK** to confirm.

Making TCP/IP settings

The TCP/IP protocol requires certain settings, which you should now make so that it can function smoothly.

- ➔ In the **Network** window, change to the **Configuration** tab.
- ➔ Select the **TCP/IP** entry for your network card.



- ➔ Click **Properties**.
- ➔ Open the **IP Address** tab.

Local network configuration

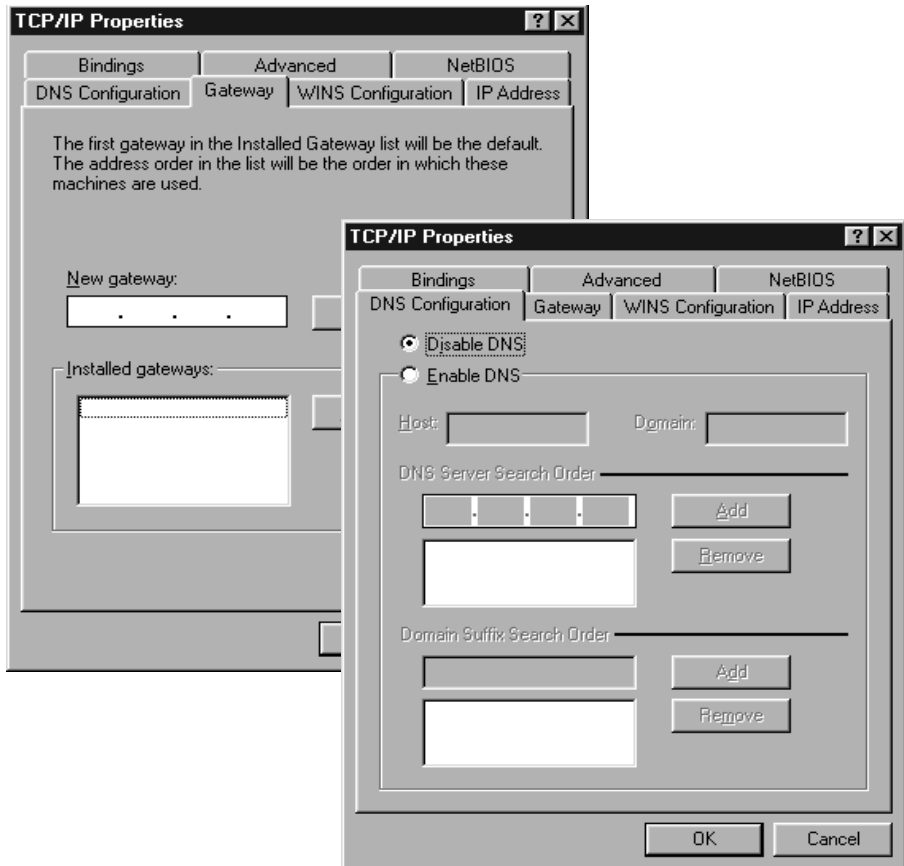
Obtaining an IP address automatically

➔ If **Obtain an IP address automatically** has been activated, your PC is already configured for DHCP. Click **Cancel** and close the following windows with **OK** to start your network configuration.

You may be prompted to insert your Windows installation CD. Follow the instructions in the installation procedure.

Once the copying procedure is completed, you will be prompted to reboot your system.

- ➔ Click **Yes**. The PC will then be shut down and rebooted.
- ➔ If **Obtain an IP address automatically** has not been activated, activate this option now.
- ➔ Open the **Gateway** tab and remove any entries in the **Installed gateways** list.
- ➔ Open the **DNS Configuration** tab.
- ➔ Select **Disable DNS**.



- ➔ Click **OK**.
- ➔ Finish the network configuration with **OK**.

You may be prompted to insert your Windows installation CD. Follow the instructions in the installation procedure.

Once the copying procedure is completed, you will be prompted to reboot your system.
- ➔ Click **Yes**. The PC will then be shut down and rebooted.

Assigning an IP address statically

If the DHCP server of your router/access point is not active or the PC is to be assigned a static IP address for other reasons, the following settings must be made:

- ➔ Select the option **Specify an IP address** on the **IP Address** tab.
- ➔ Enter the IP address for the PC in the **IP Address** field.
- ➔ Enter the subnet mask to be used in your network in the **Subnet Mask** field. You can check these settings if necessary in the LAN configuration for your router/access point.
- ➔ Open the **Gateway** tab and enter the IP address of the router/access point in the **New gateway** field or choose this, if available, from the **Installed gateways** list.
- ➔ Open the **DNS Configuration** tab.
- ➔ Select **Enable DNS**.
- ➔ Enter the IP address for the router/access point in the **DNS Server Search Order** field and click **Add**.
- ➔ Click **OK**.
- ➔ Finish the network configuration with **OK**.


You may be prompted to insert your Windows installation CD. Follow the instructions in the installation procedure.

Once the copying procedure is completed, you will be prompted to reboot your system.
- ➔ Click **Yes**. The PC will then be shut down and rebooted.

Local network configuration

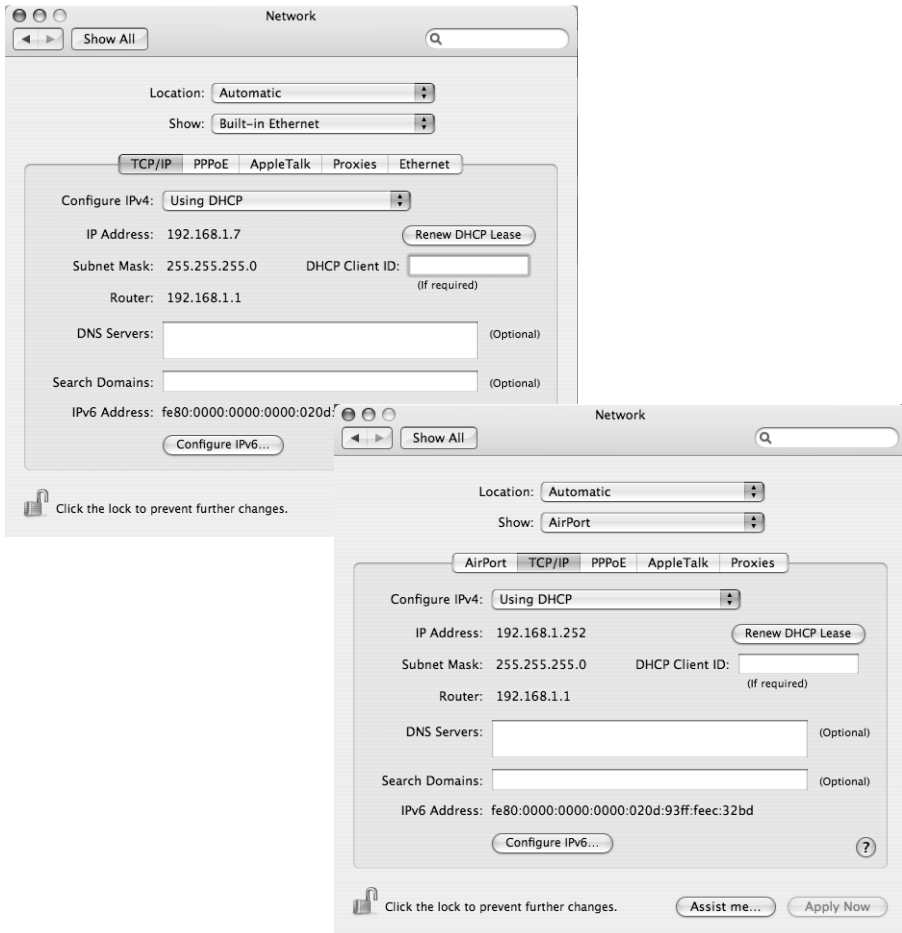
Network configuration with Mac OS X

Showing networks

To configure your network click the apple icon  on the left side of the menu bar and choose **System Preferences**.

➔ Choose **Network**.

➔ Choose from the list **Show** the option **AirPort**, if your Mac is connected wirelessly to the network and choose the option **Built-in Ethernet** if your Mac is connected via cable.



You can start all actions for your network configuration from here.

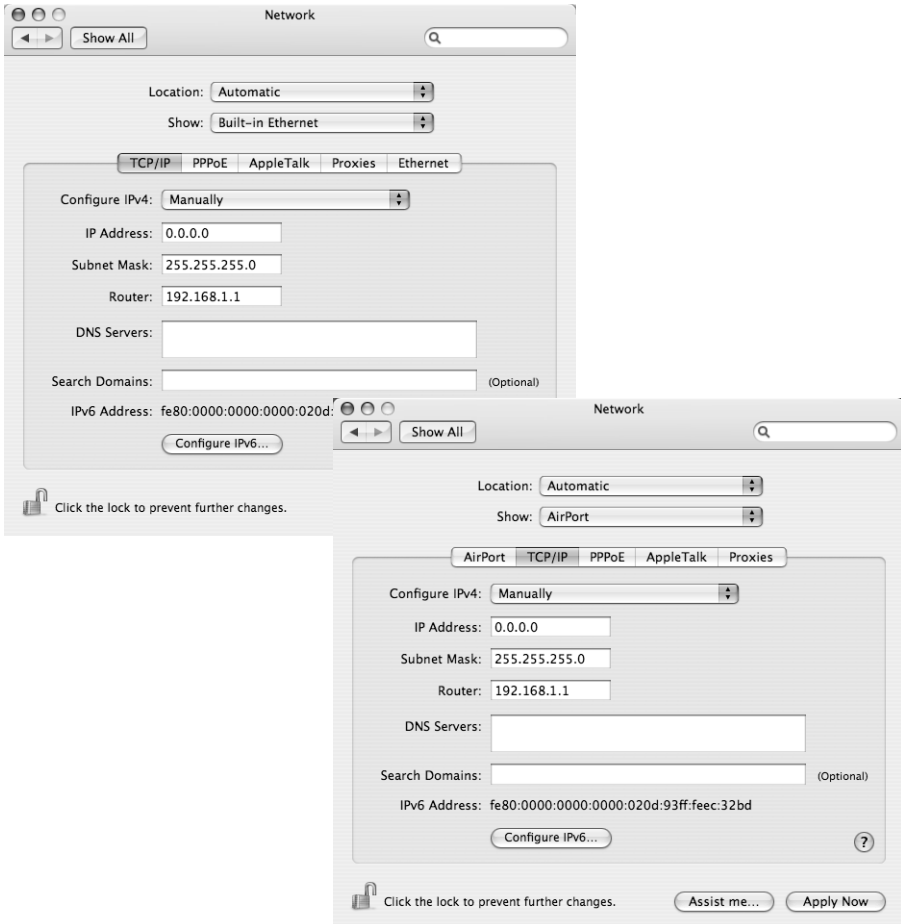
Changing the settings for IP addresses

The IP addressing settings can be checked and modified as follows:

Obtaining an IP address automatically

If the DHCP server of your router/access point is active and your Mac is to obtain its IP address automatically, you must choose the option **DHCP** from the **Configure IPv4** list.

- ➔ Check whether this option is selected and select it if necessary.
- ➔ Click **Apply Now** to save your network configuration.



Assigning an IP address statically


If the DHCP server of your router/access point is not active or your Mac is to be assigned a static IP address for other reasons, the following settings must be made:

Local network configuration

- ➔ Select the tab **TCP/IP**.
- ➔ Choose the option **Manually** from the **Configure IPv4** list.
- ➔ Enter the IP address for your Mac in the **IP Address** field.
- ➔ Enter the subnet mask to be used in your network in the **Subnet Mask** field. You can check these settings if necessary in the LAN configuration for your router/access point.
- ➔ Enter the IP address for the router/access point in the **Router** field.
- ➔ Select the option **Use the following DNS server addresses**.
- ➔ Enter the IP address for the router/access point in the **DNS Servers** field.
- ➔ Click **Apply Now**.

Selecting a computer name

Your Mac is assigned a name during installation. To change the name assignment, you have to:

- ➔ Click the Apple icon  on the left side of the menu bar and choose **System Preferences**.
- ➔ Click **Sharing**.
The name of your Mac is shown in the **Computer Name** field.
- ➔ Click **Edit**.
- ➔ Enter the name the Mac is to appear under in the network. This name must be unique within the network.
- ➔ Click **OK**.

Synchronising TCP/IP settings with the Gigaset SE587 WLAN dsl

If you have made changes to the network configuration on your computer or have connected it to a different Gigaset SE587 WLAN dsl, you may have to release the old TCP/IP settings and synchronise them with the settings for your router/access point. The software for your wireless adapter normally provides synchronisation functions. If this is not the case, you can use the following Windows operating system resources.

Windows Vista, Windows XP, Windows 2000

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

Local network configuration

```

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:\>

```

Information for Windows Vista:

Windows Vista requires more advanced rights to execute this command (even if your user account has administrator rights). Carry out the following steps:

- ➔ Click **Start**.
 - ➔ Enter **Command prompt** in the search box.
 - ➔ Right-click **Command Prompt** in the result list and select **Run as administrator**.
 - ➔ If prompted to enter the administrator password or a confirmation, then do this.
- The command prompt is opened and you can execute the command.

- ➔ 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. . . . .               : 192.168.1.100
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1

Ethernet adapter Local Area Connection:

    Media State . . . . .             : Media disconnected

C:\>

```

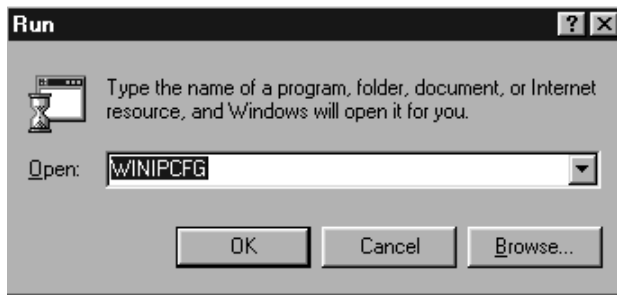
If the default IP address of the router/access point (192.168.1.1) was not changed, the IP address should now read 192.168.1.x (with x being a number between 2 and 254). The **Subnet Mask** must always be the same as that set on the Gigaset SE587 WLAN dsl (normally 255.255.255.0) and the **Default Gateway** must have the IP address of the router/access point (192.168.1.1). These values confirm that your Gigaset SE587 WLAN dsl is working.

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

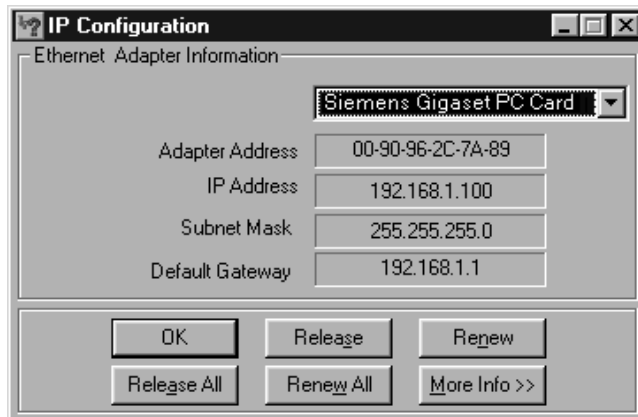
Local network configuration

Windows 98 SE, ME

- ➔ Click **Start – Run**.
- ➔ Enter **WINIPCFG** and click **OK**.



There may be a slight delay before the **IP Configuration** window appears.



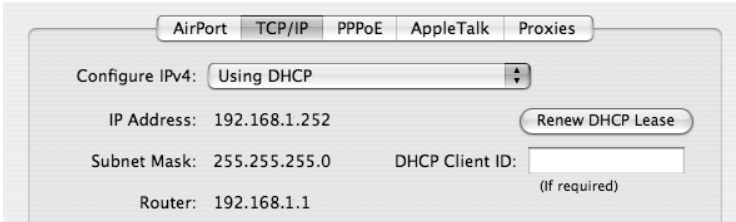
- ➔ Select your network adapter from the selection list.
- ➔ Click **Release** and then **Renew**.

If the default IP address of the router/access point (192.168.1.1) was not changed, the IP address should now read 192.168.1.x (with x being a number between 2 and 254). The **Subnet Mask** must always be the same as that set on the Gigaset SE587 WLAN dsl (normally 255.255.255.0) and the **Default Gateway** must have the IP address of the router/access point (192.168.1.1). These values confirm that your Gigaset SE587 WLAN dsl is working.

- ➔ Click **OK** to close the **IP Configuration** window.

Mac OS X

- ➔ Click the Apple icon on the left side of the menu bar and choose **System Preferences**.
- ➔ Choose **Network**.
- ➔ Choose from the list **Show** the option **AirPort**, if your Mac is connected wirelessly to the network and choose the option **Built-in Ethernet** if your Mac is connected via cable.
- ➔ Select the tab **TCP/IP**.
- ➔ Click the option **Renew DHCP Lease**.



If the default IP address of the router/access point (192.168.1.1) was not changed, the IP address should now read 192.168.1.x (with x being a number between 2 and 254). The **Subnet Mask** must always be the same as that set on the Gigaset SE587 WLAN dsl (normally 255.255.255.0) and the **Router** must have the IP address of the router/access point (192.168.1.1). These values confirm that your Gigaset SE587 WLAN dsl is working.

Checking the connection to the Gigaset SE587 WLAN dsl

Once the network has been set up on your computer, you can check whether the computer is correctly connected to the Gigaset SE587 WLAN dsl. This can be done as follows:

Windows operating systems

- ➔ Open **Command Prompt**. To do this click **Start – All Programs – Accessories – Command Prompt**.

Mac OS X

- ➔ Open the **Terminal**. Then open a Finder window and open **Applications**. Choose the folder **Utilities** and double-click the **Terminal**.

The ping command

- ➔ Enter the command **ping 192.168.1.1**.

Local network configuration

Please remember:

If the IP address of the router/access point has been changed, enter the new IP address.

The **ping** command sends data packets to the Gigaset SE587 WLAN dsl with the specified IP address and checks whether the router responds. If this is the case, the command shows statistics about the connection, for example 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 timeout, this means that the components cannot communicate with each other. Check the following points:

1. Is the Ethernet cable between the Gigaset SE587 WLAN dsl and the PC properly connected or is there a wireless connection via a wireless network adapter?

The LED display for the LAN connections on the Gigaset SE587 WLAN dsl and link display for the network card in your PC must be illuminated. For wireless connections, the WLAN monitor on your PC must display connection information.

2. Has TCP/IP been properly configured on your PC?

If the Gigaset SE587 WLAN dsl has the IP address 192.168.1.1, your PC's IP address must be between 192.168.1.2 and 192.168.1.254. The default gateway must have the address 192.168.1.1.

If you can successfully address the Gigaset SE587 WLAN dsl with the **ping** command, then the PC has been configured correctly.

Please remember:

If the command does not end with a timeout, press the key combination Ctrl-C.


Establishing the IP and MAC addresses in the network

You will need the IP address or the MAC address of the relevant computers for some of the settings.

The MAC address (Media Access Control) is used for the globally unique identification of a network adapter. It comprises six parts (hex digits), e. g. 00-90-96-34-00-1A. With many components, you will find the MAC address on the nameplate of the device.

Windows Vista

This is how you determine the IP and MAC address of PCs:

- ➔ Click the network icon in the taskbar  .
- ➔ Click **Network and Sharing Center**.
- ➔ Click **View status** next to the network connection used to connect your PC to the Gigaset SE587 WLAN dsl.
- ➔ Click **Details**.

Local network configuration

You will find the IP address next to **IPv4 IP Address** and the MAC address next to the entry **Physical Address**.

Windows XP SP2

This is how you determine the IP and MAC address of PCs:

- ➔ Click **Start – Control Panel – Network Connections** to view the current network connections.
- ➔ Double-click the network connection used to connect your PC to the Gigaset SE587 WLAN dsl.
- ➔ Open the **Support** tab in the **Local Area Connection Status** window.
- ➔ Click **Details**.

You will find the MAC address next to the entry **Physical Address**.

Windows XP, Windows 2000, Windows 98 SE/ME


If you are using older Windows systems, you can determine the IP and MAC address by entering the **ipconfig** command at the command prompt.

- ➔ Open **Command Prompt**. To do this click **Start – All Programs – Accessories – Command Prompt**.
- ➔ In the **Command Prompt** window, enter the **ipconfig /all** command and press the ENTER key.

You will find the MAC address next to the entry **Physical Address** under the network adapter used to connect your PC to the Gigaset SE587 WLAN dsl.

Mac OS X

This is how you determine the IP and MAC address of Macs:

- ➔ Click the Apple icon on the left side of the menu bar .
- ➔ Click **System Preferences**.
- ➔ Click **Network**.
- ➔ Choose from the list **Show** the option **Built-in Ethernet** if your Mac is connected to the network by wire. Select the tab **TCP/IP**. You will find the IP Address in the **IP Address** field. To identify the Mac Address select the tab **Ethernet**. You will find the Mac Address in the **Ethernet ID** field.
- ➔ Choose from the list **Show** the option **AirPort**, if your Mac is connected to the network wirelessly. Select the tab **TCP/IP**. You will find the IP Address in the **IP Address** field. To identify the Mac Address select the tab **AirPort**. You will find the Mac Address in the **AiPort ID** field.

Appendix

Appendix

Troubleshooting

This section describes common problems and their solutions. The Gigaset SE587 WLAN dsl 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 SE587 WLAN dsl and a power outlet. ➔ Check whether the power outlet and the mains adapter are working correctly. If the mains adapter is not working properly, contact Tiscali Customer care.
The LAN LED for 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.
You cannot connect to the Internet.	<ul style="list-style-type: none"> ➔ Make sure that you have entered the access data supplied by Tiscali correctly. This is done by performing the installation via set-up CD. ➔ There may be a problem at the service provider end. Get in touch with Tiscali.

Symptom	Possible cause and remedial actions
<p>You cannot open a connection from a wireless device to the Gigaset SE587 WLAN dsl.</p>	<p>The wireless network adapter is not using the correct SSID.</p> <ul style="list-style-type: none"> ➔ Connect the wireless clients to the wireless network with the correct SSID. The preset SSID is shown on the label on the bottom of the device. <p>Encryption is possibly enabled on the Gigaset SE587 WLAN dsl but not on the wireless network adapter, or it is not using the correct key, or it is using another type of encryption. The preset WPA pre-shared key is shown on the label on the bottom of the device.</p> <ul style="list-style-type: none"> ➔ Activate the same encryption on the network adapter with the correct key (see page 21). <p>If you do not know the key, you will have to reset the Gigaset SE587 WLAN dsl (see page 5).</p> <p>Warning: Please bear in mind that this will return all the configuration settings to the factory settings.</p> <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 20). <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.
<p>The Gigaset SE587 WLAN dsl or other PCs cannot be reached by a PC in the connected LAN with a ping command.</p>	<ul style="list-style-type: none"> ➔ Make sure that the network is configured correctly on all the PCs in the local network. ➔ Check that the IP addresses have been correctly configured. In most cases you can use the DHCP function of the Gigaset SE587 WLAN dsl 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 SE587 WLAN dsl must be identical. The device must also be configured as DNS server.</p> <p>Detailed information on network configuration can be found from page 36 onwards.</p>

Appendix

Symptom	Possible cause and remedial actions
No connection to the Gigaset SE587 WLAN dsl'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 SE587 WLAN dsl. ➔ Check the network cable between the PC you want to use to manage the device and the Gigaset SE587 WLAN dsl. ➔ If the PC you want to use is in the router's local network, make sure that you are using the correct IP address administration (see above). ➔ If the PC you want to use is not in the router's local network, it must be authorised via Remote Management.
Password forgotten or lost	<ul style="list-style-type: none"> ➔ Reset the Gigaset SE587 WLAN dsl (see page 5). <p>Warning: Please bear in mind that this will return all the configuration settings to the factory settings.</p>
You cannot access a resource (drive or printer) on another PC.	<ul style="list-style-type: none"> ➔ Make sure that the network is configured correctly on all the PCs in the local network and that the PCs all belong to the same workgroup. ➔ Check whether the resource has been released on the PC in question and whether you have the necessary access rights. ➔ Printing: Check whether the printer has been set up as a network printer.
The transmission rate is too low. For example, there are pixel errors with video streaming.	<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 wireless 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 DSL modem	RJ11, ITU G.992.5, Annex A
4 LAN	RJ45, 10Base-T/100Base-TX, Autosensing, MDI/MDIX
WLAN	IEEE 802.11g

Wireless properties

Frequency range	2,400 to 2,484 GHz ISM band
Number of channels	13
Transmission rate	IEEE 802.11b: up to 11 Mbps IEEE 802.11g: up to 54 Mbps
Range	approx. 50 m indoors, up to 300 m outdoors

Operating environment

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

LED displays

Power
Internet (activity, status)
WLAN (activity, wireless)
ADSL (ADSL connection, synchronisation)
LAN1... LAN4 (connection to PC or set-top box, activity, wired)

Compliance with security conditions and regulations

CE, EN60950

Software

Browser-based configuration environment
PPPoA, IPoEoA
DHCP server and client
NAT, Port Forwarding, DMZ
Firewall, prevention of hacker attacks
URL filtering,
WPA2-PSK/WPA-PSK encryption
WEP encryption

Appendix

Authorisation

This device is intended for operation in the United Kingdom with an analogue phone line and DSL via Annex A.

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/qigasetdocs>

CE 0682 

Glossary

Access point

An access point, such as the Gigaset SE587 WLAN dsl, is the centre of a wireless local network ([WLAN](#)). It handles the 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, for example an existing [Ethernet](#) LAN or via a modem to the [Internet](#). The operating mode of wireless networks with an access point is called [Infrastructure mode](#).

Ad-hoc mode

Ad-hoc mode describes wireless local networks ([WLANs](#)) in which the network components set up a spontaneous network without an [Access point](#), for example several Notebooks in a conference. All the network components are peers. They must have a wireless [Network adapter](#).

ADSL

Asymmetric Digital Subscriber Line (ADSL) and ADSL 2+ are special types of [DSL](#) data transfer technology.

AES

Advanced Encryption Standard

AES is an encryption system published as a standard in October 2000 by the National Institute of Standards and Technology (NIST). It is used for [WPA](#) encryption. A distinction is made between the three AES variants AES-128, AES-192 and AES-256 on the basis of the key length.

Auto connect

Auto connect means that applications such as Web browser, Messenger and E-mail automatically open an [Internet](#) connection when they are launched. This can lead to high charges if you are not using a [Flat rate](#). To avoid this, you can select the manual connection option on the Gigaset SE587 WLAN dsl.

Bridge

A bridge connects several network segments to form a joint network, for example to make a [TCP/IP](#) network. The segments can have different physical characteristics, for example different cabling as with [Ethernet](#) and wireless LANs. Linking individual segments via bridges allows local networks of practically unlimited size.

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

Broadcast

A broadcast is a data packet not directed to a particular recipient but to all the network components in the network. The Gigaset SE587 WLAN dsl does not pass on broadcast packets; they always remain within the local network ([LAN](#)) it administers.

Glossary

BSSID

Basic Service Set ID

BSSID permits unique differentiation of one wireless network (**WLAN**) from another. In **Infrastructure mode**, the BSSID is the **MAC address** of the **Access point**. In wireless networks in **Ad-hoc mode**, the BSSID is the MAC address of any one of the participants.

Client

A client is an application that requests a service from a **server**. For example, an HTTP client on a PC in a local network requests data, i.e. Web pages from an HTTP server on the **Internet**. Frequently the network component (e.g. the PC) on which the client application is running is also called a client.

DHCP

Dynamic Host Configuration Protocol

DHCP handles the automatic assignment of **IP addresses** to network components. It was developed because of the complexity involved in defining IP addresses in large networks – especially the **Internet** – as participants frequently move, drop out or new ones join. A DHCP server automatically assigns the connected network components (DHCP **Clients**) **Dynamic IP addresses** from a defined **IP pool range** thus saving a great deal of configuration work. In addition, the address blocks can be used more effectively: Since not all participants are on the network at the same time, the same IP address can be assigned to different network components in succession as and when required.

The Gigaset SE587 WLAN dsl includes a DHCP server and uses it to assign IP addresses automatically to PCs in the local network. You can specify that the IP addresses for certain PCs are never changed.

DHCP server

See **DHCP**

DMZ

Demilitarised Zone

DMZ describes a part of a network that is outside the **Firewall**. A DMZ is set up, as it were, between a network you want to protect (e.g. a **LAN**) and a non-secure network (e.g. the **Internet**). A DMZ is useful if you want to offer **Server** services on the Internet that are not to be run from behind the firewall for security reasons, or if Internet applications do not work 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.

DNS

Domain Name System

DNS permits the assignment of IP addresses to computers or [Domain names](#) that are easier to remember. A DNS server must administer this information for each [LAN](#) with an [Internet](#) connection. As soon as a page on the Internet is called up, the browser obtains the corresponding IP address from the DNS server so that it can establish the connection.

On the Internet, the assignment of domain names to IP addresses follows a hierarchical system. A local PC only knows the address of the local name server. This in turn knows all the addresses of the PCs in the local network and the superordinate name servers, which again know addresses of the next superordinate name servers.

DNS server

See [DNS](#)

Domain name

The domain name is the reference to one or more Web servers on the [Internet](#). The domain name is mapped via the [DNS](#) service to the corresponding [IP address](#).

DoS attack

Denial of Service

A DoS attack is a particular form of hacker attack directed at computers and networks with a connection to the [Internet](#). The aim is not so much to steal data but to paralyse the computer or network so severely that the network resources are no longer available. A typical hacker attack involves making a remote computer announce that it is acting for the paralysed computer, for example, and receive the data intended for you.

DSL

Digital Subscriber Line

DSL is a data transfer technique in which a connection to the [Internet](#) can be run at high speed over normal telephone lines. A DSL connection is provided by an [Internet service provider](#). It requires a DSL modem.

Dynamic IP address

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

See also: [Static IP address](#)

Glossary

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 SE587 WLAN dsl offers [WEP](#) encryption and [WPA](#) for secure data transfer over wireless networks.

Ethernet

Ethernet is a network technology for local networks ([LANs](#)) defined by the [IEEE](#) as standard IEEE 802.3. Ethernet uses a base-band cable with a transfer rate of 10 or 100 [Mbps](#) or 1 Gbps.

Firewall

Firewalls are used by network operators as protection against unauthorised external access. This involves a whole bundle of hardware and software actions and technologies that monitor and control the data flow between the private network to be protected and an unprotected network such as the [Internet](#).

See also: [NAT](#)

Flat rate

Flat rate is a particular billing system for [Internet](#) connections. The [Internet service provider](#) charges a monthly fee regardless of the duration and number of logins.

FTP (File Transfer Protocol)

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

Full duplex

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

See also: [Half duplex](#)

Gateway

A gateway is a device for connecting networks with completely different architectures (addressing, protocols, application interfaces etc.). Although it is not totally correct, the term is also used as a synonym for [Router](#).

Global IP address

See [Public IP address](#)

Half duplex

Operating mode for data transmission. Only one side can send and/or receive data at the same time.

See also: [Full duplex](#)

HTTP proxy

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

Hub

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

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

IEEE

Institute of Electrical and Electronic Engineers

The IEEE is an international body for defining network standards, especially for standardising [LAN](#) technologies, transfer protocols, data transfer speeds and wiring.

IEEE 802.11

[IEEE 802.11](#) is a standard for wireless LANs operating in the 2.4 GHz or 5 GHz band. In the 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](#).

Glossary

Internet

The Internet is a wide-area network ([WAN](#)) linking several million users around the world. A number of [Protocols](#) have been created for exchanging data, and these are known collectively as [TCP/IP](#) protocol stack. All participants on the Internet can be identified by an [IP address](#). Servers are addressed by [Domain names](#) (e.g. siemens.com). Domain names are assigned to IP addresses by the Domain Name Service ([DNS](#)).

These are some of the main Internet services:

- ◆ Electronic mail (e-mail)
- ◆ The World Wide Web (WWW)
- ◆ File transfer (FTP)
- ◆ Discussion forums (Usenet / Newsgroups)

Internet service provider

An Internet service provider, for example Tiscali, 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

The IP address is the unique network-wide address of a network component in a network based on the [TCP/IP](#) protocols (e.g. in a local area network ([LAN](#)) or on the [Internet](#)). The IP address has four parts (each with up to three-position digit sequences) separated by full stops (e.g. 192.168.1.1). The IP address comprises the network number and the computer number. Depending on the [Subnet mask](#), one, two or three parts form the network number; the remainder form the computer number. You can find out the IP address of your PC using the **ipconfig** command.

IP addresses can be assigned manually (see [Static IP address](#)) or automatically (see [Dynamic IP address](#)).

On the Internet [Domain names](#) are normally used instead of IP addresses. The [DNS](#) is used to assign domain names to IP addresses.

The Gigaset SE587 WLAN dsl has a [Private IP address](#) and a [Public IP address](#).

IPoA

IP over ATM

IP pool range

The Gigaset SE587 WLAN dsl's IP address pool defines a range of [IP addresses](#) that the router's [DHCP server](#) can use to assign [Dynamic IP addresses](#).

ISP

See [Internet service provider](#)

LAN

Local network

A local area network (or local network) links network components so that they can exchange data and share resources. The physical range is restricted to a particular area (a site). As a rule the users and operators are identical. A local network can be connected to other local networks or to a wide-area network ([WAN](#)) such as the [Internet](#).

With the Gigaset SE587 WLAN dsl you can set up a wired local [Ethernet](#) network and a wireless [IEEE 802.11g](#) standard network ([WLAN](#)).

Local IP address

See [Private IP address](#)

MAC address

Media Access Control

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

Mbps

Million bits per second

Specification of the transfer speed in a network.

MER

MAC Encapsulated Routing

MRU

Maximum Receive Unit

The MRU defines the maximum user data volume within a data packet.

MTU

Maximum Transmission Unit

The MTU defines the maximum length of a data packet that can be carried over the network at any one time.

Glossary

NAT

Network Address Translation

NAT is a method for converting IP addresses ([Private IP addresses](#)) within a network into one or several [Public IP addresses](#) on the [Internet](#). With NAT, several network components in a [LAN](#) can share the router's public IP address to connect to the Internet. The network components of the local network are hidden behind the router's IP address registered on the Internet. Because of this security function, NAT is frequently used as part of the [Firewall](#) of a network. If you want to make services on a PC in the local network available on the Internet despite NAT, you can configure the Gigaset SE587 WLAN dsl as a [Virtual server](#).

Network

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

Network adapter

The network adapter is the hardware device that creates the connection between a network component and a local network. The connection can be wired or wireless. An Ethernet network card is an example of a wired network adapter. The Gigaset PC Card 108 and the Gigaset USB Adapter 108 are examples of wireless network adapters.

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

Public IP address

The public [IP address](#) (also known as the global IP address) is a network component's address on the [Internet](#). It is assigned by the [Internet service provider](#). Devices that create a link from a LAN to the Internet, such as the Gigaset SE587 WLAN dsl, have a public and a [Private IP 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 SE587 WLAN dsl directs data packets from the [Internet](#) that are addressed to a particular [Port](#) to the corresponding port of the appropriate network component. This enables servers within the local network to offer services on the Internet without them needing a [Public IP address](#).

See also: [Virtual server](#)

PPPoA

Point-to-Point Protocol over ATM

PPPoA is a [Protocol](#) for connecting network components in a local Ethernet network to the [Internet](#) via an ATM network.

PPPoE

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

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

Private IP address

The private [IP address](#) (also known as the local IP address) is a network component's address within the local network ([LAN](#)). The network operator can assign any address he or she wants. Devices that act as a link from a local network, such as the Gigaset SE587 WLAN dsl, have a private and a [Public IP address](#).

Protocol

A protocol describes the agreements for communicating in a network. It contains rules for opening, administering and closing a connection, as well as in relation to data formats, time frames and possible troubleshooting. Communication between two applications requires different protocols at various levels, for example the [TCP/IP](#) protocols for the [Internet](#).

PVC

Permanent Virtual Circuit

A permanent virtual circuit is a logical connection in an ATM network. Multiple PVCs can share the same physical connection at the same time.

Radio network

See [WLAN](#)

Rekey interval

The rekey interval is the period after which new keys are automatically generated for data encryption with [WPA-PSK](#).

Remote management

Remote management refers to the ability to manage a network from a network component that is actually outside the local network ([LAN](#)).

Repeater

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

Glossary

Roaming

Roaming extends the range of a wireless LAN by using several [Access points](#) that use the same [SSID](#) and the same radio channel and are linked via [Ethernet](#). The PCs in the network can switch dynamically between several access points without losing the existing network connection.

Router

A router directs data packets from one local network ([LAN](#)) to another via the fastest route. A router makes it possible to connect networks that have different network technologies. For example, it can link a local network with [Ethernet](#) or [WLAN](#) technology to the [Internet](#).

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

Server

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

SMTP

Simple Mail Transfer Protocol

The [SMTP Protocol](#) is part of the [TCP/IP](#) protocol family. It governs the exchange of electronic mail on the [Internet](#). Your [Internet service provider](#) provides you with access to an SMTP server.

SNMP

Simple Network Management Protocol

The [SNMP Protocol](#) is part of the [TCP/IP](#) protocol family. It provides a simple procedure for administering the network based on a system of shared information for management data and network management messages (known as traps) and reports the occurrence of events within the monitored network (e.g. an alarm message or notification of configuration changes).

SSID

Service Set Identifier

The SSID is used to identify the stations in a wireless network ([WLAN](#)). All wireless network components with the same SSID form a common network. The SSID can be assigned by the network operator.

Static IP address

A static [IP address](#) is assigned to a network component manually during network configuration. Unlike the [Dynamic IP address](#), a static (fixed) IP address never changes.

Subnet

A subnet divides a network into smaller units.

Subnet mask

The subnet mask determines how many parts of [IP addresses](#) of a network represent the network number and how many parts the computer number.

If the subnet mask is in a network that is administered by the Gigaset SE587 WLAN dsl, for example 255.255.255.0, the first three parts of the IP address form the network number and only the final part can be used for assigning host numbers. The first three parts of the IP address of all network components are therefore always the same in this case.

Switch

A switch, like a [Hub](#), is an element used to link different network segments or components. Unlike a hub however, the switch has its own intelligence that enables it to forward packets to only the subnet or network component 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 transfer protocol, i.e. it sets up, monitors and terminates a connection for transferring data.

See also: [UDP](#)

TCP/IP

[Protocol](#) family on which the [Internet](#) is based. [IP](#) forms the basis for every computer-to-computer connection. [TCP](#) provides applications with a reliable transmission link in the form of a continuous data stream. TCP/IP is the basis on which services such as WWW, Mail and News are built. There are other protocols as well.

TKIP

Temporal Key Integrity Protocol

TKIP is a security protocol used for data [Encryption](#) in wireless networks. It is used for [WPA](#) encryption. It was designed to correct deficiencies in the older Wired Equivalent Privacy ([WEP](#)) standard. For this reason TKIP provides per-packet key mixing, a message integrity check, and a rekeying mechanism. TKIP ensures that every data packet is sent with its own unique encryption key.

UDP

User Datagram Protocol

UDP is a [Protocol](#) of the [TCP/IP](#) protocol family that handles data transport between two communication partners (applications). Unlike [TCP](#), UDP is a non-session based protocol. It does not establish a fixed connection. The recipient is responsible for making sure the data is received. The sender is not notified about whether it is received or not.

Glossary

UPnP

Universal Plug and Play

UPnP technology is used for the spontaneous linking of home or small office networks. Devices that support UPnP carry out their network configuration automatically once they are connected to a network. They also provide their own services or use services of other devices in the network automatically.

URL

Universal Resource Locator

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

VCI

Virtual Channel Identifier

Part of an address in an ATM network.

Virtual server

A virtual [Server](#) provides a service on the [Internet](#) that does not run on itself, but on another network component. The Gigaset SE587 WLAN dsl can be configured as a virtual server. It will then direct incoming calls for a service via [Port forwarding](#) directly to the appropriate [Port](#) of the network component in question.

VLAN

Virtual Local Area Network

A VLAN is a virtual local network within a physical network. A widely disseminated technical implementation of VLANs is defined partially in the Standard IEEE 802.1Q. VLAN allows preferred forwarding of voice data, for example. This functionality is important for VoIP (IP telephony). This also means that phone calls can be made without interruption within a restricted bandwidth.

VPI

Virtual Path Identifier

Part of an address in an ATM network.

WAN

Wide Area Network

A WAN is a wide area network that is not restricted physically to a particular area, for example the [Internet](#). A WAN is run by one or more public providers to enable private access. You access the Internet via an [Internet service provider](#).

Web server

See [Server](#)

WEP

Wired Equivalent Privacy

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

WLAN

Wireless LAN

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

WLAN is currently specified in Standard [IEEE 802.11](#). The Gigaset SE587 WLAN dsl complies with Standard 802.11g.

WPA

WPA is a new standard-conformant solution for greater security in wireless networks. WPA is meant to replace the existing WEP standard (Wired Equivalent Privacy) and offers more reliable encryption and authentication methods.

WPA-PSK

WPA Pre-shared Key

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

Index

Index

Numerics

10/100 Mbps switch port.	5
128-bit key	23
64-bit key	23
802.11b	38
802.11g	38

A

Access point	71
Access restriction	25
Address block for IP addresses . . .	18, 37
Ad-hoc mode.	71
Administration.	30
ADSL	4, 71
port	5
status.	12
ADSL modem, integrated.	4
AES	22, 71
Authentication	31
Authorisation	70
Auto connect.	71

B

Back panel.	5
Backing up configuration data.	34
Backup	34
Basic Setup	15
Bridge	71
Broadcast	21, 71
Browser see Internet browser	
BSSID.	72
Buttons	12

C

Channel.	21
Client	72
Command	
ipconfig	60
ping	63
Computer name	37
Configuration	10

Configuration data

backing up	34
restoring.	35
Configuration file.	34
Connection	
checking the connection to the	
router/access point	63
statistics	64
virtual.	16

D

data IPEoA	16
data PPOA.	16
Default settings	9
Defining a computer name	
Mac OS X	60
Windows 2000	52
Windows 98	53
Windows Vista	45
Windows XP	49
Defining a workgroup	
Windows 2000	52
Windows 98	53
Windows Vista	45
Windows XP	49
Device, status.	15
DHCP	36, 72
DHCP server	17, 36, 72
configuring.	18
Digital Subscriber Line see DSL	
Displaying wireless networks	
Mac OS X	41
Windows Vista	39
Windows XP	38
DMZ.	8, 29, 72
DNS	73
DNS configuration	
Windows 2000	51
Windows 98	56
Windows Vista	44
Windows XP	48
DNS server	73
Domain blocking	8
Domain name	73

- Domain Name Service see DNS
- DoS attack 73
- DSL 73
 - status 12
- Dynamic DNS see DynDNS
- Dynamic Host Configuration Protocol, see DHCP
- Dynamic IP address 73
- DynDNS 74

- E**
- Encryption 8, 21, 74
 - preset 9
 - WEP 23
 - WPA-PSK/WPA2-PSK 22, 23
- Entering the gateway
 - Mac OS X 60
 - Windows 2000 51
 - Windows 98 57
 - Windows Vista 44
 - Windows XP 48
- Entering the subnet mask
 - Mac OS X 60
 - Windows 2000 51
 - Windows 98 57
 - Windows Vista 44
 - Windows XP 48
- Ethernet 7, 36, 74
 - transmission speed 7

- F**
- Features 7
- Filter
 - IP 26
 - port 26
 - ULR 27
- Firewall 8, 74
 - enabling or disabling 24
- Firmware
 - upgrade 33
- Flat rate 74
- Front panel 5
- FTP, port number 26
- Full duplex 74

- G**
- Gateway 56, 74

- Global IP address see Public IP address

- H**
- H.323, port number 26
- Hacker attack 8, 73
- Half duplex 75
- Hexadecimal key 23
- HTTP proxy 75
- HTTP, port number 26
- HTTPS, port number 26
- Hub 75

- I**
- Idle time 11
- IEEE 75
- Infrastructure mode 75
- Installing TCP/IP protocol
 - Windows 98 54
- Institute of Electrical and Electronic Engineers see IEEE
- Internet 76
 - access 4
 - access restriction 25
 - configuring access 15
 - status 13
- Internet access 4
- Internet browser 8
- Internet connection
 - changing configuration 15
 - setting up 15
- Internet Explorer 10
- Internet protocol see IP protocol
- Internet service provider 76
- IP address 10, 36, 76
 - address block 18, 37
 - assigning automatically 17, 36
 - assigning static 19
 - assigning statically 18, 36
 - defining 17, 64
 - defining for the router 18
 - dynamic 73
 - private 37, 79
 - public 78
 - static 80
- IP address block for DHCP 19
- IP address pool 76

Index

- IP address, assigning statically
 - Mac OS X 60
 - Windows 2000 51
 - Windows 98 57
 - Windows Vista 44
 - Windows XP 48
- IP filter 26
- IP protocol 76
- ipconfig / release 60
- ipconfig /all 65
- ipconfig /renew 61
- IPoA 76
- IPTV 16

- K
- Key length
 - 128 bit 23
 - 64 bit 23

- L
- LAN 77
 - configuration 17
 - port 5
 - status 14
- LED displays 6
- Local area network see LAN
- Local IP address see Private IP address
- Logging 32
- Login screen 10

- M
- MAC address 64, 77
 - determining 64
- Mac computer, defining a name 60
- MAC Encapsulated Routing see MER
- Maximum Receive Unit see MRU
- Maximum Transmission Unit see MTU
- Mbps 77
- MER 77
- Mozilla Firefox 10
- MRU 77
- MTU 77

- N
- NAT 27, 78
 - DMZ 29
 - port forwarding 27
- Network 78
- Network adapter 78
- Network Address Translation . . . 8, 27, 78
- Network configuration 9
 - Mac OS X 58
 - Windows 2000 49
 - Windows 98 52
 - Windows Vista 42
 - Windows XP 45

- O
- Obtaining an IP address automatically
 - Mac OS X 59
 - Windows 2000 51
 - Windows 98 56
 - Windows Vista 44
 - Windows XP 48
- Opening the command prompt . . . 63, 65
- Operating state 6

- P
- Passphrase 23
- Password
 - of configuration user interface 10
 - of user ID 31
- PC
 - defining a name (Windows 2000) . . . 52
 - defining a name (Windows 98) 53
 - defining a name (Windows Vista) . . . 45
 - defining a name (Windows XP) 49
- Permanent Virtual Circuit see PVC
- Ping command 63, 64
- Point-to-Point Protocol over ATM
 - see PPPoA
- Point-to-Point Protocol over Ethernet
 - see PPPoE
- POP3, port number 26
- Port 78
 - ADSL modem 5
 - LAN 5
- Port filter 26
- Port forwarding 27, 78
 - configuring 28
- Port number 29, 78
 - mapping 28
- Port numbers of Internet services . . . 27
- Power supply unit 5

- PPPoA 79
- PPPoE 79
- Predefined application 28
- Pre-shared key 22, 40, 41
- Private IP address 79
- Problem solving 66
- Protocol 79
- Public IP address 78
- PVC 16, 79

- R**
- Radio network 83
- Radio settings 20
- Reboot. 5, 6
- Releasing TCP/IP settings 60
- Remote management 79
- Remote management 31
- Reset 5, 6
- Reset button 5
- Restore 35
- Roaming 80
- Router 80
 - IP address 17

- S**
- Security 8
 - firewall 24
 - wireless 21
- Server 80
 - virtual 82
- Service filtering 8
- Service Set Identifier see SSID
- Setting up a network client
 - (Windows 98) 53
- Setting up a WLAN connection 38
- Setup menu 15
- Showing networks
 - Mac OS X 58
 - Windows 2000 49
 - Windows Vista 42
 - Windows XP 45
- Simple Mail Transfer Protocol see SMTP
- Simple Network Management Protocol
 - see SNMP
- SMTP 80
- SMTP, port number 26
- SNMP 80

- SSID 40, 41, 80
 - concealed 21
 - pre-set 9
 - visible 21
- SSID broadcast 21
- Static IP address 80
- Status
 - device 15
 - DSL 12
 - Internet 13
 - local area network 14
 - wireless network 14
- Status information 12
- Subnet 80
- Subnet mask 37, 81
 - defining 18
- Summer time 19
- Switch 81
- System log 32
- System management 30

- T**
- TCP 81
- TCP/IP 81
- TCP/IP settings
 - Mac OS X 59
 - synchronising with router 60
 - Windows 2000 50
 - Windows 98 55
 - Windows Vista 43
 - Windows XP 46
- Telnet, port number 26
- Time server 19
- Time setting 19
- Tiscali standard connections 16
- TKIP 22, 81
- Trademarks 9
- Transmission Control Protocol see TCP
- Transmission speed 77
 - in the Ethernet LAN 7
 - in wireless LAN 7

- U**
- UDP 81
- Universal Plug and Play see UPnP
- Universal Resource Locator see URL
- UPnP 32, 82

Index

- URL 82
- URL filter 27
- User Datagram Protocol see UDP
- User ID
 - creating 31
 - editing 31
- User interface
 - elements 12
 - functions 11
 - idle time. 11
 - starting 10
- V
- VCI 82
- Virtual Channel Identifier see VCI
- Virtual connection
 - configuring 16
- Virtual Path Identifier see VPI
- Virtual server. 28, 82
- VPI. 82
- W
- WAN 82
- WEP 23, 83
- WEP key 40, 41
- Wide Area Network see WAN
- WINIPCFG. 62
- Wired Equivalent Privacy see WEP
- Wireless cell 83
- Wireless LAN see WLAN
- Wireless network mode 20
- Wireless security. 21
- Wireless settings 20
- WLAN. 7, 36, 83
 - status 14
 - transmission speed 7
- WLAN adapter 38
- Workgroup 37
- WPA 83
 - pre-shared key 83
- WPA2-PSK 22, 23
- WPA-PSK 22, 23

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 2007
All rights reserved. Subject to availability.
Rights of modification reserved.

www.siemens.com/gigaset

A31008-N1083-L171-1-7619