

# SIEMENS

Be inspired



# Gigaset SE 105

dsl/cable



# Contents

<b>Safety precautions</b> .....	<b>4</b>
<b>The Gigaset Router</b> .....	<b>5</b>
Features and Application .....	6
Procedure for installation and configuration .....	8
<b>First Steps</b> .....	<b>9</b>
System Requirements .....	9
Package Contents .....	9
Operating displays and connections .....	10
Front panel .....	10
Back panel .....	11
Setting up the Gigaset Router .....	12
Connecting the Gigaset Router .....	13
Connecting a DSL or cable modem to the router .....	13
Creating a LAN connection .....	14
Activation .....	16
<b>Configuring the local network</b> .....	<b>17</b>
Network configuration for Windows 98, 98 SE, ME .....	18
Setting up a PC as Client for Microsoft Networks .....	18
Selecting computer names and workgroup .....	19
Installing the TCP/IP protocol. ....	20
TCP/IP protocol settings .....	21
Deactivating the http proxy .....	25
Synchronising the TCP/IP settings with the Gigaset Router .....	26
Network configuration with Windows XP .....	27
Configuring the network .....	27
Selecting computer names and workgroup .....	29
Checking the network settings and completing the installation procedure .....	29
TCP/IP protocol settings .....	30
Deactivating the http proxy .....	33
Synchronising the TCP/IP settings with the Gigaset Router .....	34
Network configuration with Windows 2000 .....	35
Installing network services .....	35
Selecting computer names and workgroup .....	36
Installing the TCP/IP protocol. ....	37
TCP/IP protocol settings .....	39
Deactivating the http proxy .....	41
Synchronising the TCP/IP settings with the Gigaset Router .....	42
Checking the connection to the Gigaset Router .....	43

## **Gigaset Router User Interface . . . . . 44**

Launching the User Interface . . . . .	44
Language Selection . . . . .	46
UI elements . . . . .	47

## **General configuration with Basic Setup . . . . . 49**

Select Country . . . . .	49
Wireless Settings . . . . .	50
Configuring the WAN connection . . . . .	51
T-online . . . . .	51
Other Internet Service Provider . . . . .	53

## **Configuration with Advanced Setup . . . . . 59**

System Configuration . . . . .	60
Setting the Country . . . . .	60
Setting the Time Zone . . . . .	60
Assigning passwords . . . . .	62
Remote Management . . . . .	63
WAN Configuration . . . . .	64
Defining a DNS Server . . . . .	66
Configuring as a bridge . . . . .	67
LAN Configuration . . . . .	68
Configuring Wireless Connections . . . . .	70
Activating the wireless module . . . . .	70
Setting the Channel and SSID . . . . .	70
Setting the Encryption . . . . .	72
NAT Configuration . . . . .	73
Defining Address mapping . . . . .	74
Setting up the router as a virtual server . . . . .	75
Configuring Special Applications . . . . .	76
Firewall Configuration . . . . .	77
Activating the firewall . . . . .	77
Protection against hacker attacks . . . . .	78
Enabling only selected PCs to access your local network . . . . .	80
Restricting access of local PCs to the Internet . . . . .	81
Opening the firewall for particular PCs (DMZ) . . . . .	82
Activating dynamic DNS . . . . .	83
Using the universal plug and play function . . . . .	85

## **Gigaset Router Administration . . . . . 86**

Opening or closing an Internet connection manually . . . . .	86
Saving and restoring a configuration . . . . .	87
Firmware Upgrade . . . . .	88
Resetting the router . . . . .	89
Displaying the router's Status . . . . .	90
Router information . . . . .	90
Working with the security log . . . . .	91

**Appendix . . . . . 92**  
Fault tracing . . . . . 92  
Specifications . . . . . 95  
Service (Customer Care) . . . . . 97  
Guarantee certificate (United Kingdom) . . . . . 97  
Guarantee certificate (Ireland) . . . . . 98

**Glossary . . . . . 100**

**Index . . . . . 109**

# Safety precautions

- ◆ Only use the power supply unit provided with the Gigaset Router (9V-1A). Note the connection values and ratings when connecting the device to the mains.
- ◆ Protect the router from dampness.
- ◆ Never open the device. For electrical safety reasons it may only be opened by authorised service technicians.
- ◆ The device may affect the operation of medical equipment. Take account of the technical conditions in the relevant environment.
- ◆ Be sure to include the operating instructions if you pass your Gigaset Router on to someone else.
- ◆ Dispose of the Gigaset Router in an environmentally safe manner.

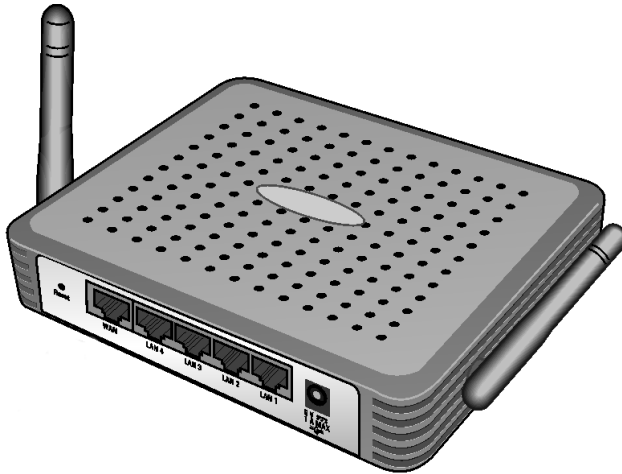
### Trademarks

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

Netscape, Netscape Navigator and Netscape Communicator are registered trademarks of the Netscape Communications Corporation.

## The Gigaset Router

The Siemens Gigaset Router (Gigaset SE105 dsl/cable) a powerful but simple communications device for connecting your PC or local network (LAN) to the Internet (WAN). If you want to surf the Internet at the lowest possible cost, the Gigaset Router is a comfortable and effective solution.



The Gigaset Router permits Internet access for several users. A single user account can be shared, if your Internet Service Provider permits this. You can connect either a DSL or cable modem to your Gigaset Router's WAN socket.

The Gigaset Router is programmed with numerous functions and is simple to handle. It can be configured and operational within a few minutes.

### Features and Application

---

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

#### ◆ **setting up a local network**

The Gigaset Router can accommodate

- four devices via **Ethernet** ports with a transmission speed of 10 or 100 **Mbps**.
- for up to 253 mobile end devices via a wireless interface with a transmission speed of 11 Mbps. Here it complies with Standard **IEEE 802.11b**– i.e. the router can be used together with products of several other manufacturers.

Using a Gigaset Router makes it easy to set up a network at home or small offices. For example, users can exchange data or share resources on the network, such as a file server or printer.

With the Gigaset devices for wireless networks you can operate a local network–as envisaged in Standard **IEEE 802.11** –in **Ad-hoc mode** and in **Infrastructure mode**.

The Gigaset Router supports **DHCP** for dynamic IP configuration of the local network and **DNS** for Domain name mapping.

#### ◆ **Internet access**

The Gigaset Router permits Internet access via a WAN socket with a transmission speed of 10 or 100 Mbps. You can connect a DSL or cable modem to this socket.

- Since many DSL providers permit communication with end users via the **PPPoE** protocol, the Gigaset Router has an integrated **Client** for this protocol, that means you no longer have to install this service on your computer.
- Shared IP address

If your Internet Service Provider permits this, the Gigaset Router can use a single **IP address** jointly for up to 253 users. Several users on your network can then surf the Internet at the same time using only one Internet Service Provider account.

#### ◆ **Virtual Private Network (VPN)**

The Gigaset Router supports three of the most common **Protocols** for setting up a Virtual Private Network: **PPTP**, **L2TP** and **IPSec**. This allows you to connect devices at different locations via the Internet securely, if your Internet Service Provider offers this service.

## ◆ Protection against unauthorised access from the Internet

The Gigaset Router offers comprehensive security measures such as:

- **Firewall** with prevention of hacker attacks (e. g. **SPI, DoS attacks**)  
Emails will be sent to notify you about any attacks on your network.
- **NAT** firewall  
If Network Address Translation (NAT) has been activated, all the PCs on the local network connect to the Internet using the router's **Public IP address** and as such are not visible on the Internet themselves. The router permits access from the Internet only if it has been requested from the local network.
- If you want to offer your own services on the Internet, you can configure the router as a virtual server without permitting further access to the local network.
- **DMZ**  
This allows you to release a PC on your local network for unrestricted access from the Internet without undermining the security of the other PCs.

## ◆ Protection for the users of the local network, e. g. parental control

You can configure the Gigaset Router so that Internet access is blocked or limited for various users. You can set time-based rules or specify that certain services or Internet pages cannot be requested.

### Important Information:



On the supplied CD you will find the file "Practical Tips and Configuration Examples" describing many of the uses of the Gigaset Router in full detail.



### Procedure for installation and configuration

1. First install an Ethernet network card or a wireless **Network adapter** such as the Gigaset USB Adapter 11 or Gigaset PC Card 11 in the PCs you want to connect with the Gigaset Router. The installation procedure can be found in the product's User Guide.



When installing wireless network adapters you should note the following:  
The factory-set **SSID** of the Gigaset SE105 dsl/cable is **ConnectionPoint**.

2. Then install the router (see page 13).
3. Before the PCs can communicate with the router and with each other in a local network, you have to change their network settings. Configure these network settings on **one** PC first so that it can establish a connection to the router. You can then use that PC to configure the router (see page 17).
4. In a wireless connection you establish the link from the PC's wireless network adapter to the router. This is described in the network adapter's operating instructions.
5. Configure the router so that the router's WAN socket can be used (see page 44). This will require the access data from your Internet Service Provider.
6. If you want to connect more PCs to the router, configure their network settings and set up the local network (see page 17).
7. If you want to use the router's other functions, , e. g. the comprehensive security functions, use the router's Advanced Setup (see page 59).

# First Steps

---

## System Requirements

---

To operate your Gigaset Router you will need

- ◆ a PC with
  - a **Ethernet** network card
  - or
  - a Gigaset USB Adapter 11, a Gigaset PC Card 11 or an 802.11b compatible wireless **Network adapter**.
- ◆ a Web browser, such as Microsoft Internet Explorer 5.5 or higher, Netscape Communicator 6.0 or higher for configuring your router.
- ◆ for Internet access: a DSL or cable modem and the access data of your **Internet Service Provider**.

## Package Contents

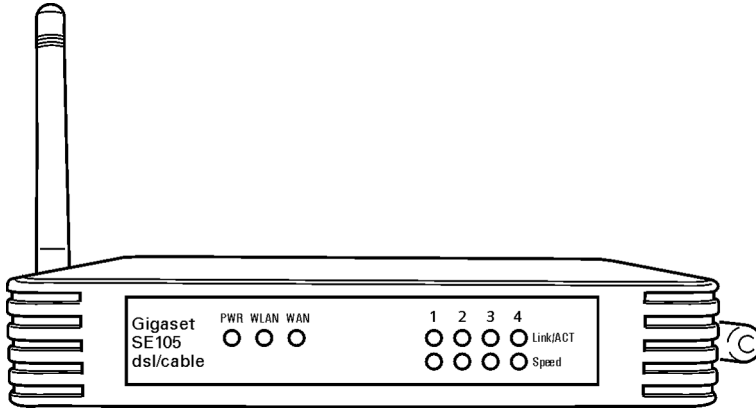
---

The package contains the following items:

- ◆ the Gigaset Router
- ◆ a power supply unit
- ◆ an Ethernet cable (CAT-5)
- ◆ the Installation CD including these operating instructions
- ◆ a quick guide

## Operating displays and connections

### Front panel



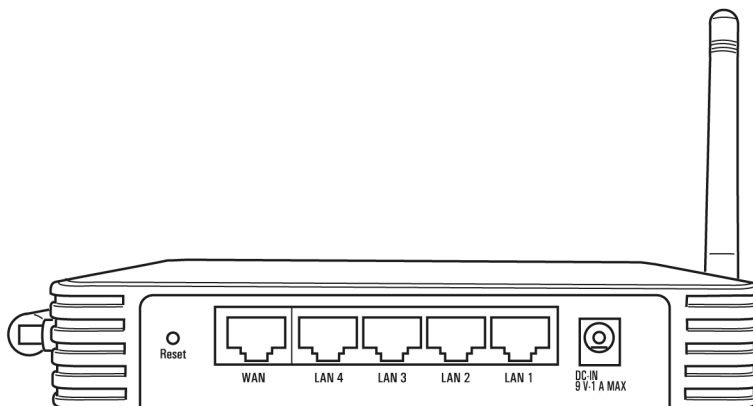
### LED displays

The front panel of the Gigaset Router contains LED displays that show the operating state and simplify installation and fault finding in the network.

The LEDs show the following:

LED	State	Status
PWR	On	The Gigaset Router has been switched on.
WLAN	On	The Gigaset Router is ready to open wireless connections.
WAN	On	The WAN connection has established a valid network connection.
	Flashing	The WAN connection is sending or receiving data (traffic).
Link/ACT	On	The LAN connection has established a valid network connection.
	Flashing	The LAN connection is sending or receiving data (traffic).
Speed	On	The LAN connection is running at 100 Mbps.
	Off	The LAN connection is running at 10 Mbps.

## Back panel



The back panel of the Gigaset Router houses the various sockets.

Element	Description
DC IN 9V-1A MAX	Socket for the supplied power unit. <b>Warning:</b> Using the wrong power supply unit may damage the router.
Reset	Reset function. Use this button to <ul style="list-style-type: none"> <li>◆ boot the router. Hold the button down for one second.</li> <li>◆ reset all the settings to the factory defaults. Hold the button down for five seconds.</li> </ul> <b>Warning:</b> This will clear all the configuration settings you have made. Updated firmware will not be affected.
WAN	WAN socket (RJ-45) for a DSL or cable modem.
LAN1-LAN4	Four 10/100 Mbps switch sockets with automatic recognition (RJ-45). You can connect up to four Ethernet devices (such as PCs, a Hub or Switch).

### Setting up the Gigaset Router

---

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

- ◆ Operate the Gigaset Router only indoors within a temperature range of +5 to +40 °C. Do not position the Gigaset Router near a heat source. Do not cover the ventilation slots.
- ◆ A mains socket for 220/230V~ and a connection socket for the DSL modem, cable modem or LAN must be available where you set up the Gigaset Router.
- ◆ Do not place the router in the immediate vicinity of stereo equipment, TV sets or microwave ovens. Otherwise this may cause interference.
- ◆ Position the Gigaset Router so that it is in the centre of your wireless network. In general: The higher you place the antenna, the better the performance. Make sure that where you position the Gigaset Router has optimum reception in the whole house or office.
- ◆ Position the Gigaset Router on a non-slip surface.  
The router feet do not normally leave any traces on the surface they are on. However, some furniture surfaces may contain substances that attack and soften the router's plastic feet. Then the feet may well mark the furniture surface.
- ◆ Position the Gigaset Router so that it cannot fall down and damage the antenna.
- ◆ Lay the cables so that nobody can trip over them. You should not cover the cables with anything.
- ◆ Protect the Gigaset Router from dampness.

## Connecting the Gigaset Router



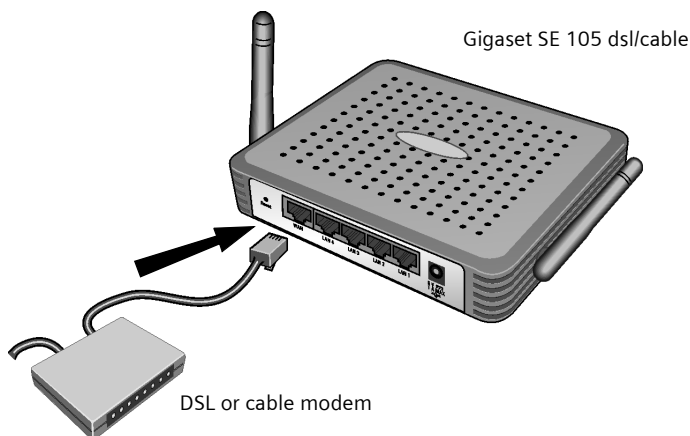
- ◆ Only use the (9V 1A) power supply unit supplied with the router.
- ◆ Do not plug any phone jack connectors into the router WAN and LAN sockets.
- ◆ Use standard network cables for all connections (CAT-5) for the WAN and LAN connections.
- ◆ An Ethernet cable must not be longer than 100 meters (328 feet).

Before you start connecting PCs to your Gigaset Router make sure that

- ◆ a wired or wireless **Network adapter** is connected to the PC. Please read the operating instructions that came with the adapter.
- ◆ ConnectionPoint has been entered as **SSID** on the network adapter.

### Connecting a DSL or cable modem to the router

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



Use a 100-Ohm shielded or unshielded 3, 4 or 5 category Ethernet cable with RJ-45 jacks on both ends for all connections. Please bear in mind that the cable you use must be the right one for the modem (straight or crossed wiring). Please consult your modem operating instructions. The Ethernet cable supplied has straight wiring.

### Creating a LAN connection

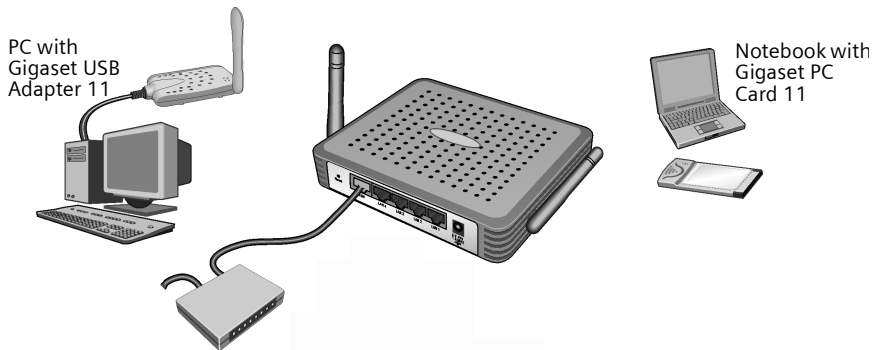
You can connect PCs to your router in wireless or wired mode and so set up a local network (LAN).

#### Wireless

A wireless connection is established via a wireless network adapter installed in your PC. This could be for example a Gigaset USB Adapter 11, a Gigaset PC Card 11 or an 802.11b compatible wireless network adapter.

You define a **Wireless network** by assigning all the devices an identical **SSID**. Assign the network adapters the router's SSID. The factory setting for the router's SSID is **ConnectionPoint**.

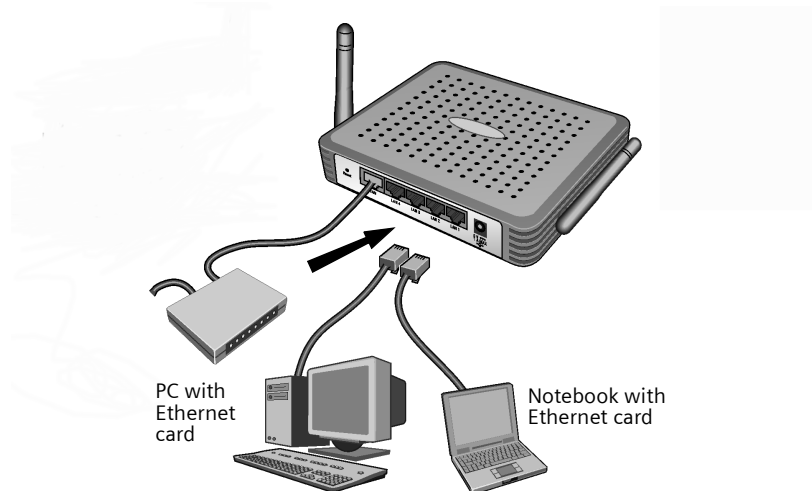
If the correct SSID has been entered in your PC's wireless network adapter, the wireless link will be established automatically once you connect your router to the mains power supply (see page 16).



Arrange the Gigaset Router's two antennas in an optimum position for reception from the network adapters. Coverage is more effective if you position one antenna vertically and the other horizontally.

## Wired

Insert one end of the supplied Ethernet cable in one of the LAN sockets (**LAN1 - LAN4**) on the back of the router and the other end in the PC's Ethernet network card, **Hub** or **Switch**. The four LAN ports can automatically set transmission speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet and the transmission mode to **Half duplex** or **Full duplex**.

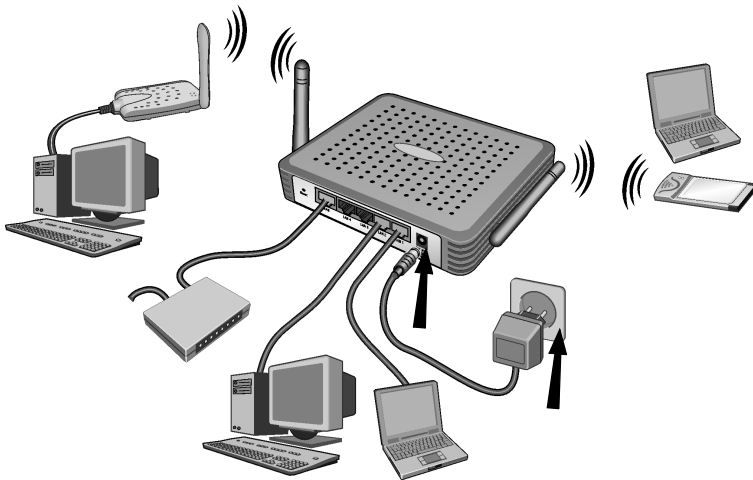




### Activation

---

Plug the power unit cable into the 9V 1A socket on the router. Plug the other end of the power unit cable into a power outlet.



This will activate the router. Check whether the LED display for the mains (PWR) on the front panel is lit up. If this is not the case, please turn to "Fault tracing" on page 92.

The wireless link to the PCs connected via a wireless network adapter will be established automatically if their network adapters have been configured with the same **SSID** as the router (see page 14). It can take a few seconds for the wireless connection to be established.

## Configuring the local network

Once you have set up the hardware and connected all the devices, you have to configure the network settings of all the PCs that will communicate with each other via the Gigaset Router.

The local network is set up as a **TCP/IP** network. You will have to make various choices during the configuration procedure. The most important decision is whether you want to use the router's **DHCP** service or not. The router uses DHCP (Dynamic Host Configuration Protocol) to assign **Dynamic IP addresses** for the network components, i.e. it automatically assigns a PC that logs in an IP address from a defined address block. The next time the PC logs on it may well be assigned a different IP address. How to configure the router's dynamic address assignment is described on page 68 of the section "LAN Configuration".

In this chapter we assume that you will use the router's DHCP service. This is also the router's default setting.

In some cases however it is better to assign **Static IP addresses**, e. g. when you want to use certain firewall functions. How to assign fixed IP addresses is described in "Practical Tips and Configuration Examples" on the supplied CD.

If your network has already been set up you can read on from page 44 in the chapter "Gigaset Router User Interface".

Network configuration differs depending on the Windows operating system you are using. Below you will find the procedure for Windows 98 from page 18, for Windows XP from page 27 and for Windows 2000 from page 35.

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



The Windows user interfaces depicted in this guide may differ from those on your screen because of the settings you have made. The illustrations always reflect the state after immediate installation.

### Network configuration for Windows 98, 98 SE, ME

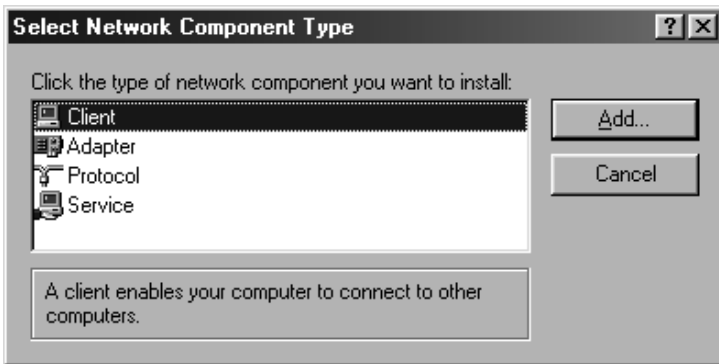
To integrate a PC with Windows 98, 98 SE or ME in a local network via a Gigaset Router:

1. Set up the PC as Client for Microsoft Networks (see below).
2. Select computer names and workgroup (see page 19).
3. Install the TCP/IP protocol (see page 20).
4. Make TCP/IP protocol settings (see page 21).
5. Deactivate the http proxy (see page 25).
6. Synchronise the TCP/IP settings with the Gigaset Router (see page 26).

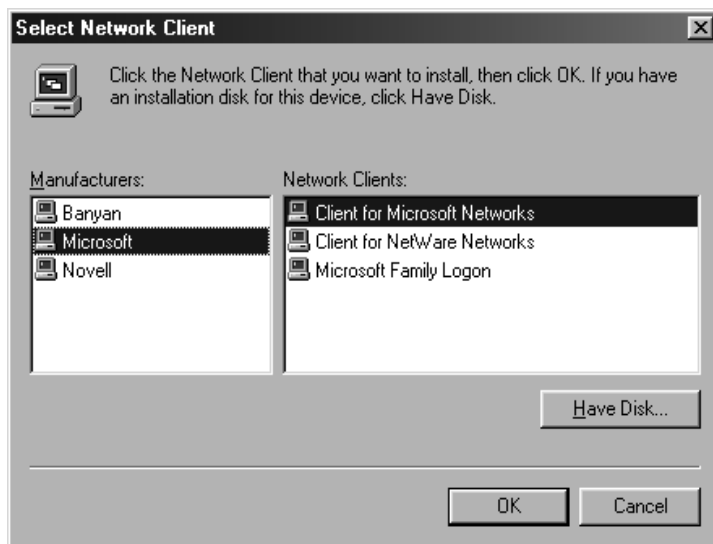
### Setting up a PC as Client for Microsoft Networks

Before the PCs on your network can work together, you have to configure them as Microsoft Network **Clients**. This can be done as follows:

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



- ◆ Select as network component type **Client** and click on **Add**.



- ◆ Select in **Manufacturer** the entry **Microsoft** and in **Network clients** the entry **Client for Microsoft Networks**.
- ◆ Confirm this with **OK**.

### Selecting computer names and workgroup

Now you have to specify a name for the PC and assign it to a workgroup.

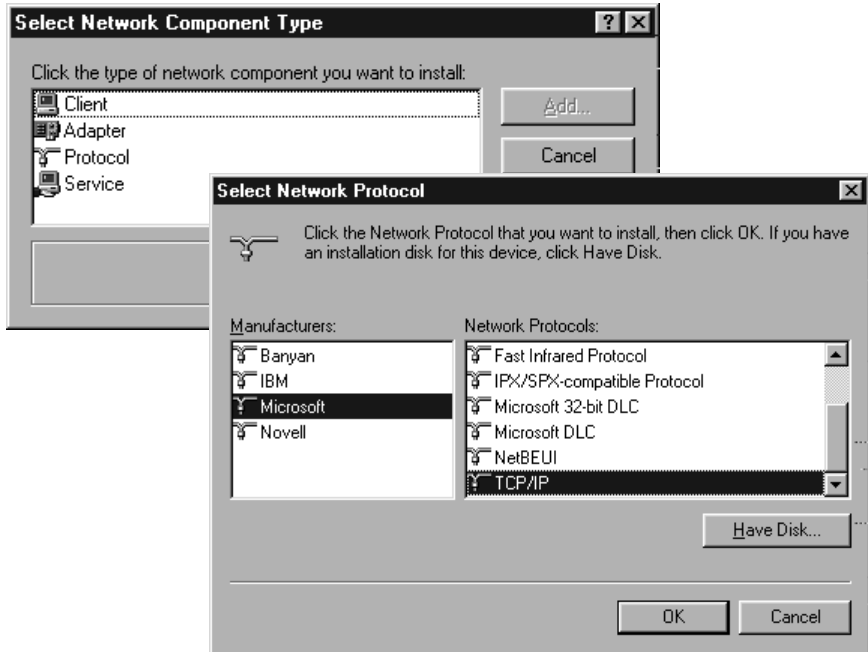
- ◆ In the **Network** window move from the **Configuration** to the **Identification** tab.
- ◆ In the **Computer name** box, enter the name the PC is to appear under in the network. This name must be unique within the network.
- ◆ In the **Workgroup** box, enter a name for the workgroup. This name must be the same for all the PCs in the network.
- ◆ The **Description** box can be left empty.

## Configuring the local network

### Installing the TCP/IP protocol.

The **TCP/IP** protocol ensures that the PCs in the network can communicate with each other. You first have to install this **Protocol** for the network adapter that establishes the connection to the Gigaset Router.

- ◆ In the **Network** window move from the **Identification** to the **Configuration** tab.
- ◆ 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 USB Adapter 11 as the wireless network adapter, the list must contain the entry **TCP/IP > Siemens Gigaset USB-Adapter 11**.
- ◆ If the entry does not exist, click on **Add**.

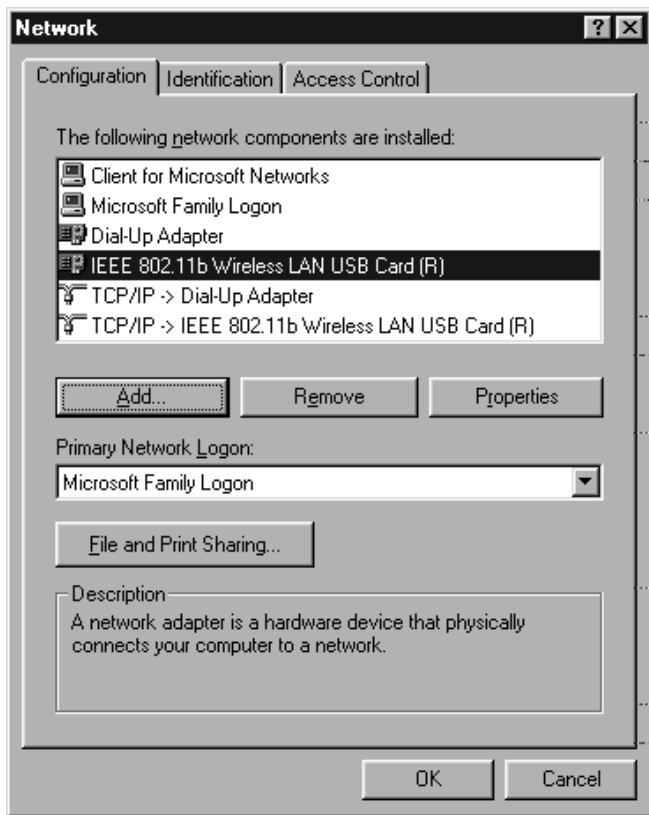


- ◆ Select as network component type **Protocol** and click on **Add**.
- ◆ Select in **Manufacturer** the entry **Microsoft** and in **Network protocol** the entry **TCP/IP** before confirming with **OK**.

## TCP/IP protocol settings

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

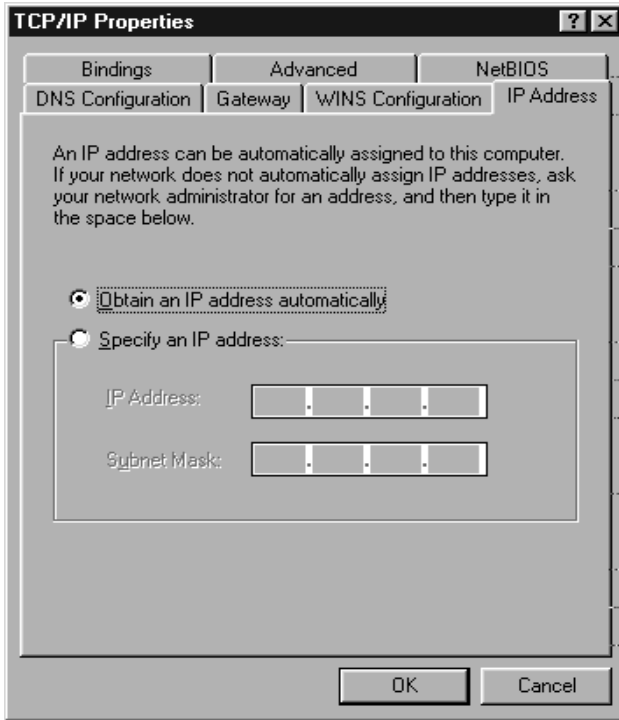
- ◆ To do this, in the **Network** window, switch to the **Configuration** tab.
- ◆ Select the **TCP/IP >** entry for your network card.



- ◆ Click on **Properties**.

## Configuring the local network

- ◆ Open the *IP address*.tab.



- ◆ If *Obtain an IP address automatically* has already been activated, your PC is already configured for **DHCP**. Click on **Cancel** and close the next windows with **OK** to run 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 on **Yes**. The computer will then be rebooted.  
Then read on from page 25.
- ◆ If *Obtain an IP address automatically* has not been activated, activate this option now.

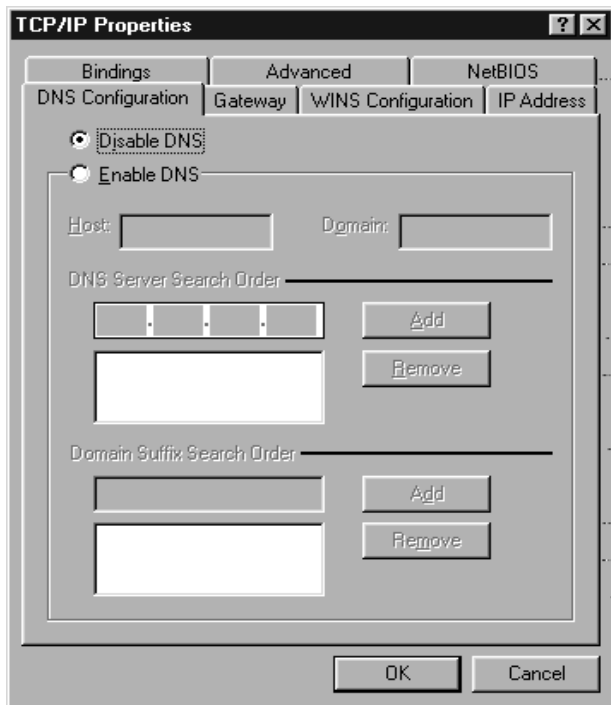
- ◆ Open the *Gateway* tab and remove any entries from the *Installed gateways* list.





## Configuring the local network

- ◆ Open the *DNS configuration* tab. Select *Disable DNS*.



- ◆ Click on **OK**.
- ◆ Complete 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 on **Yes**. The computer will then be rebooted.

## Deactivating the http proxy

---

Make sure that the **http proxy** in your Web browser is deactivated. This function must be deactivated so that your Web browser can access your Gigaset Router's configuration pages.

The following section describes the procedure for Internet Explorer and Netscape. Read the appropriate steps for the browser you are using.

### Internet Explorer

- ◆ Open Internet Explorer. Click on **Extras – Internet options**.
- ◆ In the **Internet options** window click on the **Connections** tab.
- ◆ Click on **LAN settings**.
- ◆ Deactivate all the check boxes in the **Settings for local network (LAN)** window and click on **OK**.
- ◆ Click on **OK** again to close the **Internet options** window.

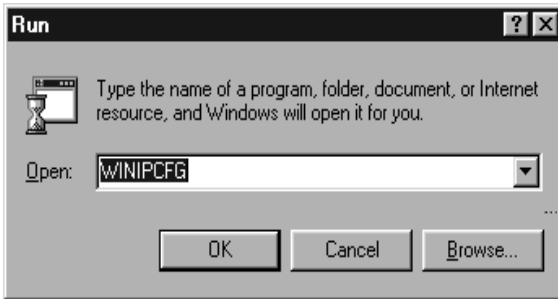
### Netscape

- ◆ Open Netscape. Click on **Edit** and then **Settings**.
- ◆ Double click on **Advanced Category** in the **Settings** windows and then click on **Proxies**.
- ◆ Select **Direct connection to the Internet**.
- ◆ Close the window with **OK**.

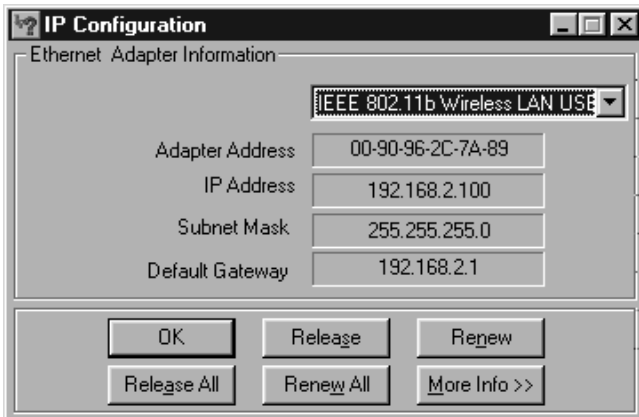
### Synchronising the TCP/IP settings with the Gigaset Router

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

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



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



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

If the router's default IP address (192.168.2.1) was not changed, the IP address should now read 192.168.2.x (with x being a number between 2 and 254). The **Subnet mask** must always be 255.255.255.0 and the **Default Gateway** must have the router's IP address (192.168. 2.1). These values confirm that your Gigaset Router is working.

- ◆ Click on **OK** to close the **IP configuration** window.

## Network configuration with Windows XP

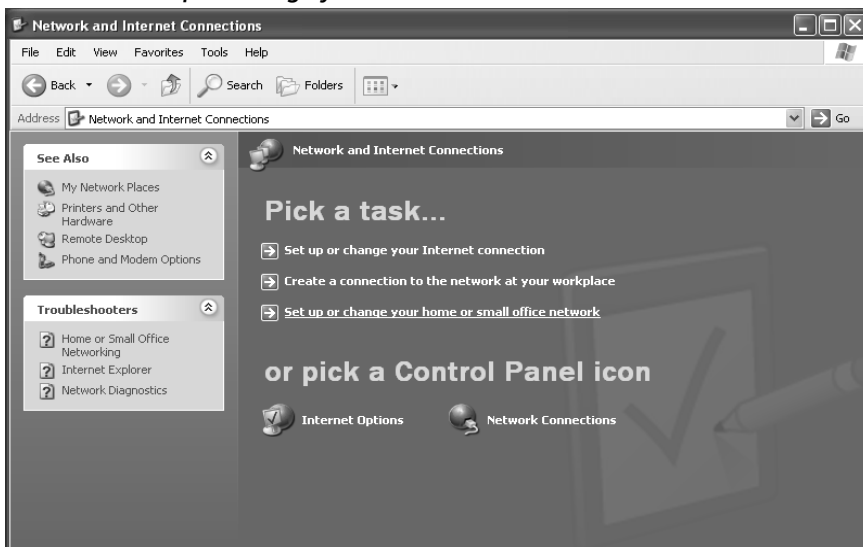
To integrate a PC in a network with Windows XP via a Gigaset Router:

1. Configure the network (see below).
2. Select computer names and workgroup (see page 29).
3. Check the network settings and complete the installation procedure (see page 29).
4. Make TCP/IP protocol settings (see page 30).
5. Deactivate the http proxy (see page 33).

### Configuring the network

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

- ◆ Select **Start – Control Panel**.
- ◆ Select **Network and Internet Connections**.
- ◆ Now select **Set up or change your home network or small office network**.



This launches the network wizard.

- ◆ Skip the welcome screen and the checklist by clicking on **next** each time.

## Configuring the local network

You will be prompted to select a connection method.

- ◆ Select **Other method** and confirm with **next**.

You will now see a screen listing various connection methods.



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

## Selecting computer names and workgroup

---

Now you have to specify a name for the PC and assign it to a workgroup.

- ◆ Enter the name the PC is to appear under in the network. This name must be unique within the network. You can complete the **Computer description** box or leave it empty. Then click on **next**.
- ◆ Enter a name for the workgroup the computer is to belong to. This name must be identical for all the PCs in the network. Continue with **next**.

## Checking the network settings and completing the installation procedure

---

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

- ◆ Click on **Back** if you want to make any changes or click on **next**, if you want to leave them unchanged.

If you do not want to install any more PCs:

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

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

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

After this your "home network" will have been installed.

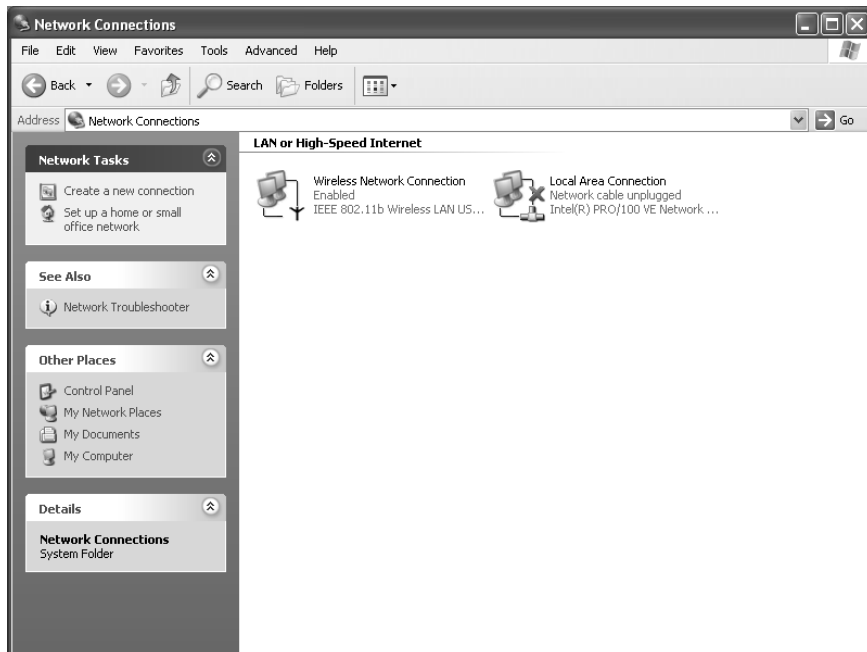
To set up the network on the other PCs with the same settings, insert the disk in the drive and run **Netsetup** with a double click.

## Configuring the local network

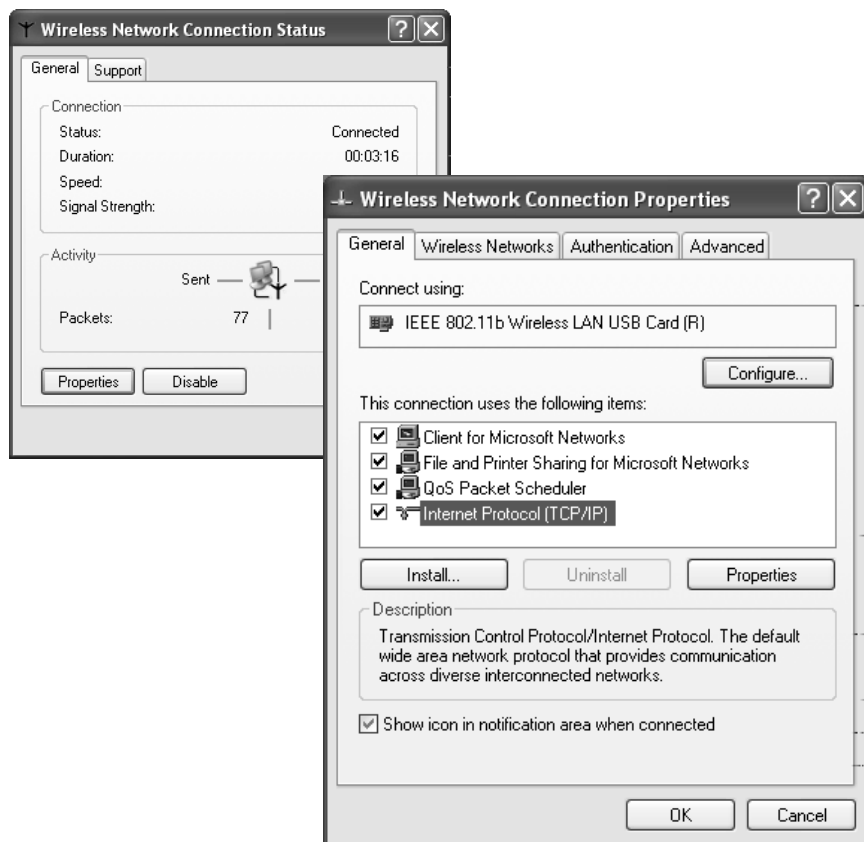
### TCP/IP protocol settings

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

- ◆ Click on **Start** and select **Control Panel**.
- ◆ Select **Network and Internet Connections** and then click on the **Network Connections** icon.



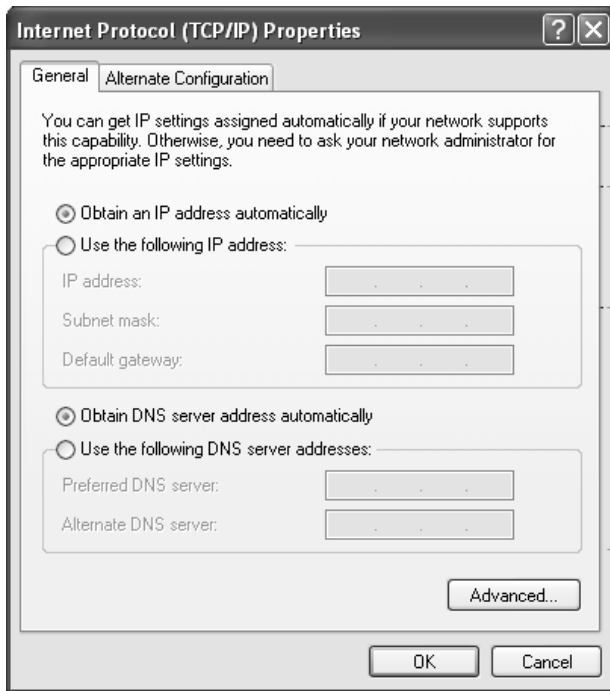
- ◆ Double click on the LAN connection with which you are connected to the router.



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



## Configuring the local network



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

## Deactivating the http proxy

---

Make sure that the **http proxy** in your Web browser is deactivated. This function must be deactivated so that your Web browser can access your Gigaset Router's configuration pages.

The following section describes the procedure for Internet Explorer and Netscape. Read the appropriate steps for the browser you are using.

### Internet Explorer

- ◆ Open Internet Explorer and click on **Stop**. Click on **Extras** and then **Internet options**.
- ◆ In the **Internet options** window click on the **Connections** tab.
- ◆ Click on **Settings**.
- ◆ Deactivate all the check boxes in the **Settings for local network (LAN)** window.
- ◆ Click on **OK** and then **OK** again to close the **Internet options** window.

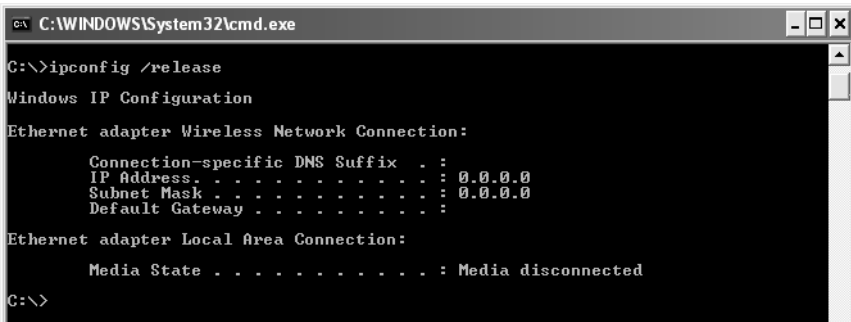
### Netscape

- ◆ Open Netscape. Click on **Edit** and then **Settings**.
- ◆ Double click on **Advanced Category** in the **Settings** windows and then click on **Proxies**.
- ◆ Select **Direct connection to the Internet**.
- ◆ Close the window with **OK**.

### Synchronising the TCP/IP settings with the Gigaset Router

You have now configured your computer so that it is ready to be connected to the Gigaset Router. You now have to release the old TCP/IP settings and update them with the settings of your Gigaset Router.

- ◆ Click on **Start** in Windows Desktop and then **Programs**, followed by **Accessoires** and finally **command prompt**.
- ◆ In the **command prompt** window enter the `ipconfig /release` command and press the ENTER KEY.



```
C:\WINDOWS\System32\cmd.exe

C:\>ipconfig /release

Windows IP Configuration

Ethernet adapter Wireless Network Connection:

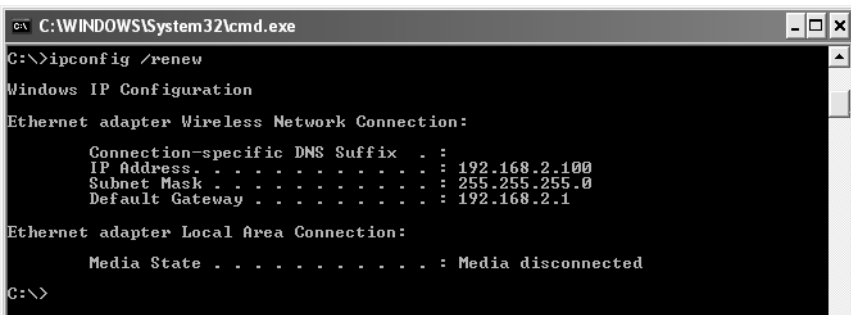
    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected

C:\>
```

- ◆ Then enter the `IPCONFIG /RENEW` command and press the ENTER KEY.



```
C:\WINDOWS\System32\cmd.exe

C:\>ipconfig /renew

Windows IP Configuration

Ethernet adapter Wireless Network Connection:

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

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected

C:\>
```

If the router's default IP address (192.168.2.1) was not changed, the IP address should now read 192.168.2.x (with x being a number between 2 and 254). The **Subnet mask** must always be 255.255.255.0 and the **Default Gateway** must have the router's IP address (192.168.2.1). These values confirm that your Gigaset Router is working.

- ◆ Enter `EXIT` and press the Enter Key to close the **command prompt** window.

## Network configuration with Windows 2000

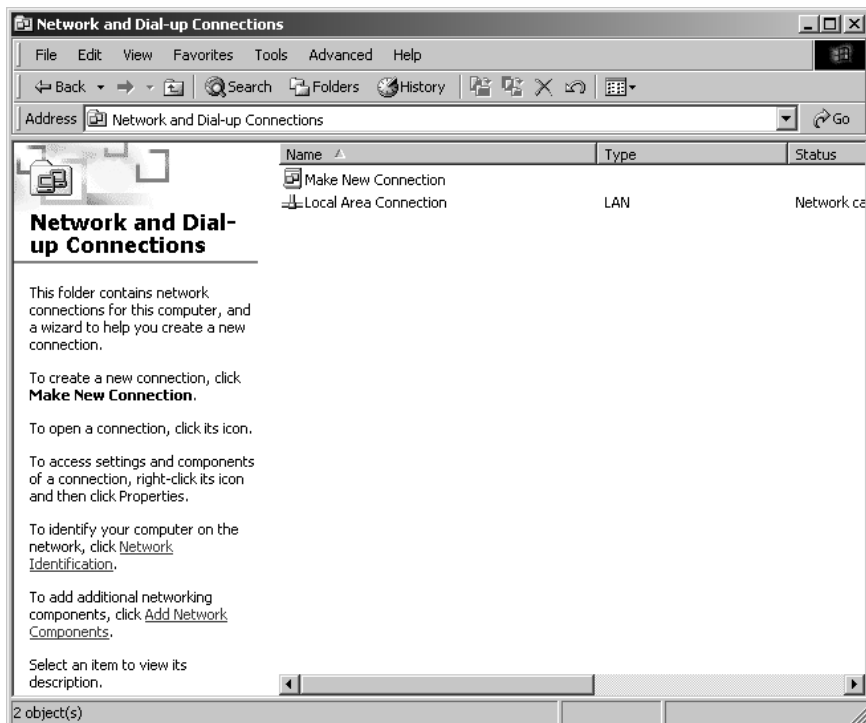
To integrate a PC in a network with Windows 2000 via a Gigaset Router:

1. Install the network services (see below).
2. Select computer names and workgroup (see page 36).
3. Install the TCP/IP protocol (see page 37).
4. Make TCP/IP protocol settings (see page 39).
5. Deactivate the http proxy (see page 41).
6. Synchronise the TCP/IP settings with the Gigaset Router (see page 42).

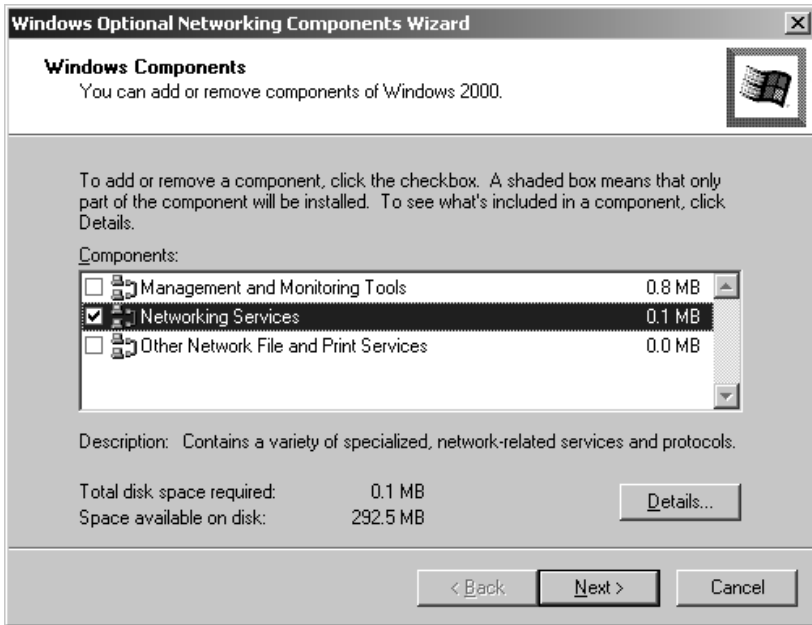
### Installing network services

You have to install the network services before the PCs in your network can access shared resources. This can be done as follows:

1. Click on **Start – Settings – Control Panel**.
- ◆ Double click on the **Network and Dial-up Connections** icon.



- ◆ In the left-hand pane click on **Add network components**.



- ◆ Select **Networking services** and click on **next**.
- ◆ You will now be prompted for the Windows installation CD. Insert the WIN2000 CD and click on the **OK** button to install all the required components.

### Selecting computer names and workgroup

---

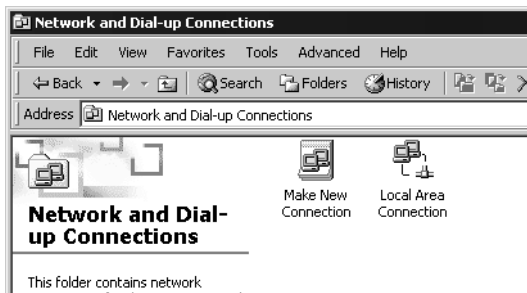
Now you have to specify a name for the PC and assign it to a workgroup.

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

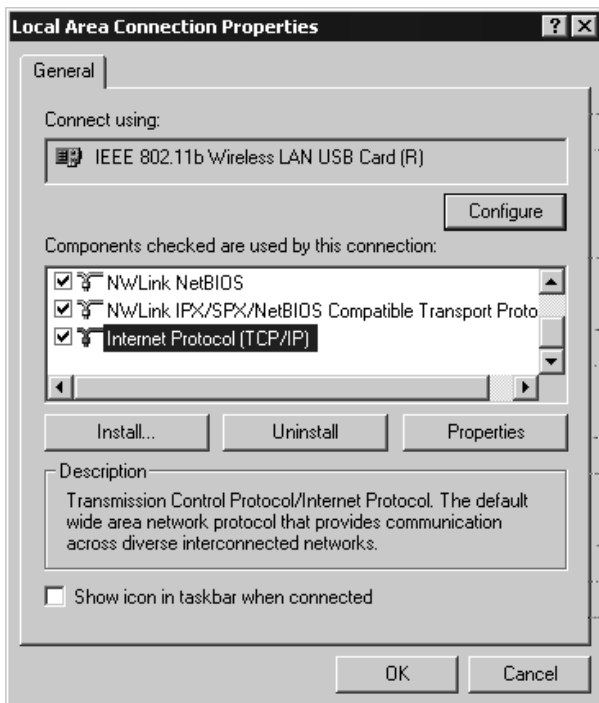
## Installing the TCP/IP protocol.

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

- ◆ Right click to open **Local Area Connection**.

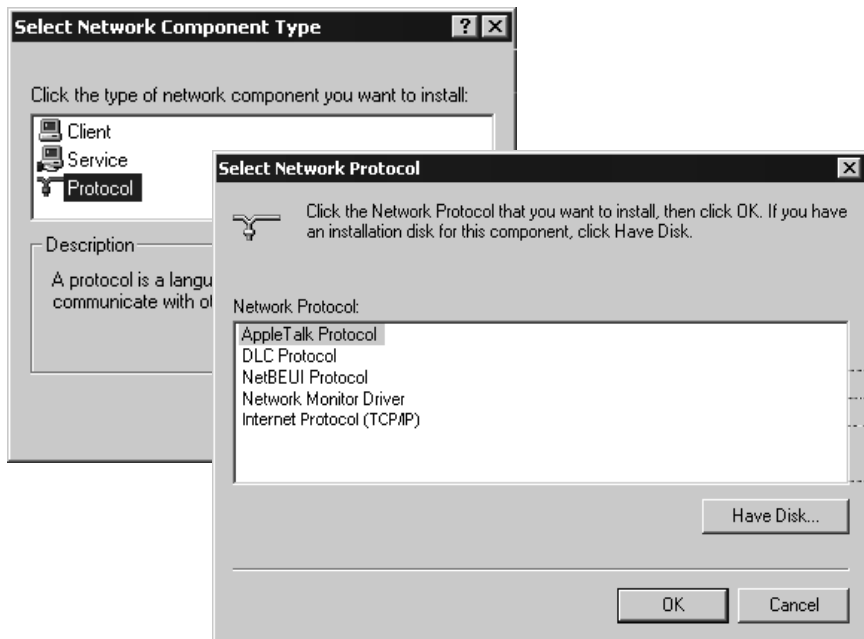


- ◆ In the next window click on **Properties**.



- ◆ Click on **Install**.

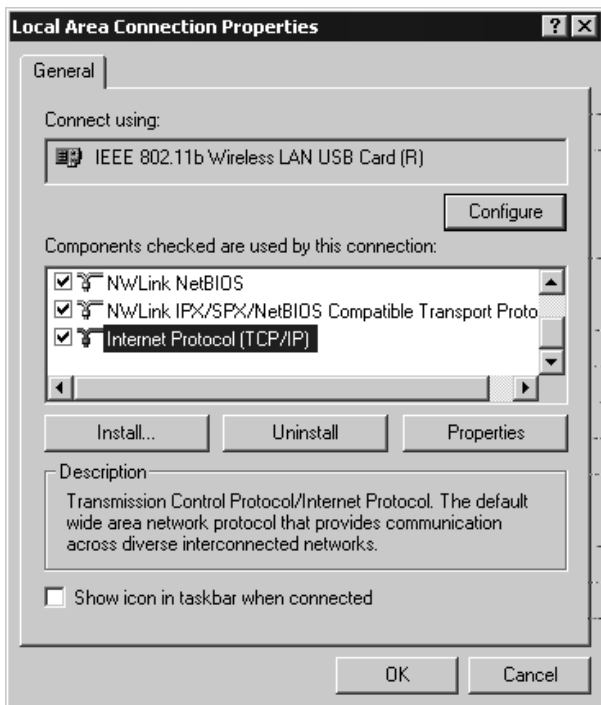
## Configuring the local network



- ◆ Select **Protocol** and click on **Add**.
  - ◆ In the **Network protocol** list, select the entry **Internet Protocol (TCP/IP)**.
  - ◆ Click on **OK**.
- You will now see the TCP/IP protocol in the **Local Area Connection Properties** window.

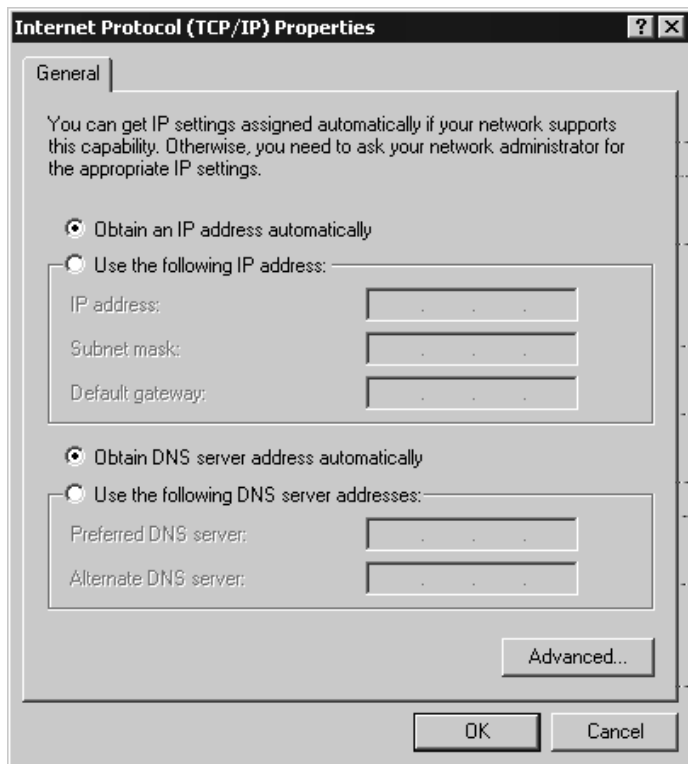
## TCP/IP protocol settings

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



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





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

## Deactivating the http proxy

---

Make sure that the **http proxy** in your Web browser is deactivated. This function must be deactivated so that your Web browser can read your Gigaset Router's configuration pages.

The following section describes the procedure for Internet Explorer and Netscape. Read the appropriate steps for the browser you are using.

### Internet Explorer

- ◆ Open Internet Explorer. Click on **Extras – Internet options**.
- ◆ In the **Internet options** window click on the **Connections** tab.
- ◆ Click on **LAN settings**.
- ◆ Deactivate all the check boxes in the **Settings for local network (LAN)** window.
- ◆ Click on **OK** and then **OK** again to close the **Internet options** window.

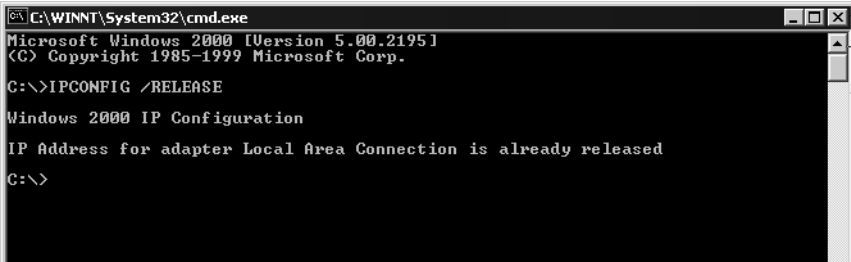
### Netscape

- ◆ Open Netscape. Click on **Edit** and then **Settings**.
- ◆ Double click on **Advanced Category** in the **Settings** windows and then click on **Proxies**.
- ◆ Select **Direct connection to the Internet**.
- ◆ Close the window with **OK**.

### Synchronising the TCP/IP settings with the Gigaset Router

You have now configured your computer so that it is ready to be connected to the Gigaset Router. You now have to release the old TCP/IP settings and update them with the settings of your Gigaset Router.

- ◆ Click on **Start – Programs – Accessoires – command prompt** in Windows Desktop.
- ◆ In the **command prompt** window enter the `ipconfig /release` command and press the ENTER KEY.



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

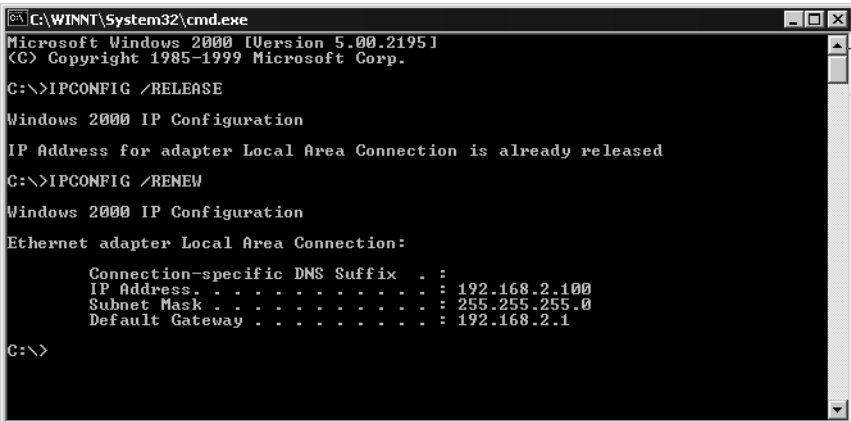
C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP Address for adapter Local Area Connection is already released

C:\>
```

- ◆ Then enter the `ipconfig /renew` command and press the ENTER KEY.



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

C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP Address for adapter Local Area Connection is already released

C:\>IPCONFIG /RENEW

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

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

C:\>
```

If the router's default IP address (192.168.2.1) was not changed, the IP address should now read 192.168.2.x (with x being a number between 2 and 254). The **Subnet mask** must always be 255.255.255.0 and the **Default Gateway** must have the router's IP address (192.168. 2.1). These values confirm that your Gigaset Router is working.

- ◆ Enter `exit` and press the ENTER KEY.

## Checking the connection to the Gigaset Router

Once the network has been set up on a PC, you can check whether the PC has been successfully connected to the Gigaset Router. This can be done as follows:

- ◆ Open **command prompt**. This can be done by clicking on **Start – Programs – command prompt**.
- ◆ Enter the command `ping 192.168.2.1`.



If the router's IP address was changed, enter the new IP address.

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

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

1. Has the Ethernet cable between the Gigaset Router and the PC been inserted properly or is there a wireless connection via a wireless network adapter?

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

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

If the Gigaset Router has IP address 192.168.2.1, your PC's IP-address must be between 192.168.2.2 and 192.168.2.254, the default gateway must have the address 192.168.2.1.

If you can reach the Gigaset Router with the `ping` command, then the PC has been configured properly.

# Gigaset Router User Interface

Once you have configured the network settings on a PC in your local network, you can then use that PC to configure the Gigaset Router with the user interface. The Gigaset Router can be configured using any browser that supports Java, e.g. Microsoft Internet Explorer 5.5 or higher, Netscape Communicator 6.0 or higher.

The Gigaset Router user interface includes Basic Setup and Advanced Setup.

**Basic Setup** Use Basic Setup for the settings required for connecting to the Internet via a DSL or cable modem. This is described from page 49 on.

**Advanced Setup** Advanced Setup provides additional functions. Here, for example, you can assign a password, configure and activate firewall functions, back up and restore the configuration data and much more besides. These configuration steps are optional and can be carried out at a later stage. This is described from page 59 on.

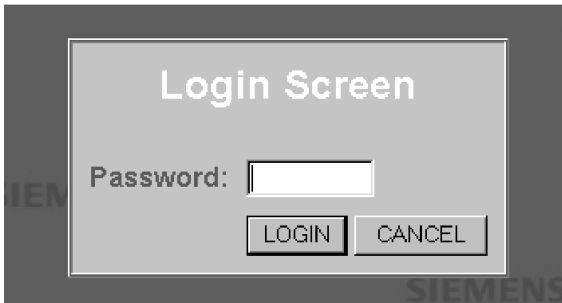
## Launching the User Interface

To access the Gigaset Router's user interface:

- ◆ Launch your Web browser.
- ◆ Enter the router IP address in the Web browser address bar.

`http://192.168.2.1`

You will then see a login window:



- ◆ Click on **LOGIN** (the default is no password).



For security reasons you should assign a password at a later stage (see page 62).

The opening screen is displayed.

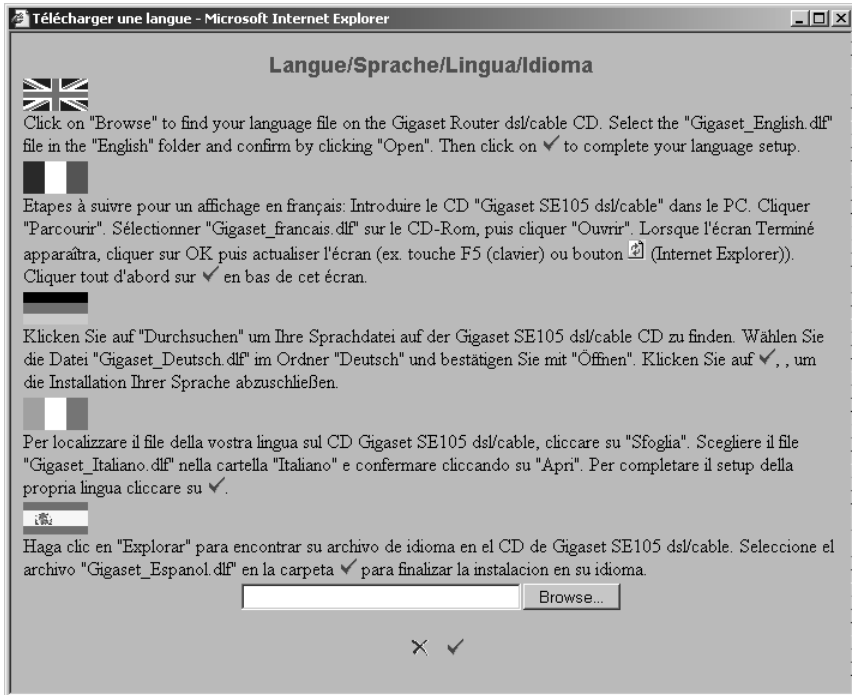


## Language Selection

The first time you launch the user interface it will appear in English. If you do not want to change the language, you can skip this section.

- ◆ If you want to work with the German, French, Italian or Spanish user interface, click on the flag of the respective country.

A new window is displayed where you can select the language.

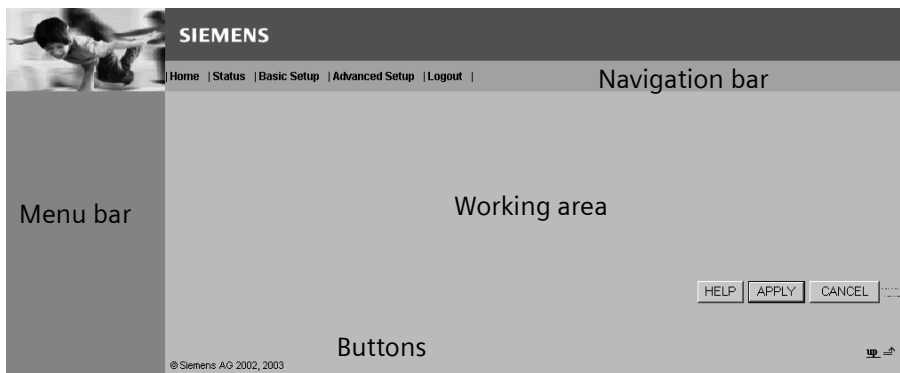


- ◆ Insert the installation CD into your CD ROM drive.
- ◆ Click on **Browse** and select your language file. You will find the file in the CD-ROM directory of the country in question; it has the file extension .dlf. For example you will find the language file for the English user interface under `\English\Gigaset_English.dlf`.
- ◆ Then click on  and in the following window click on **OK** to accept your selection.
- ◆ Now refresh the web page. This can be done by clicking on **Refresh** (Internet Explorer) or **Reload** (Netscape) the browser toolbar.

The user interface will now be displayed in the desired language.

## UI elements

The UI pages have the following elements:



### Navigation bar

<b>Home</b>	Takes you to the opening screen.
<b>Status</b>	Displays router status information. You can find detailed information about this page on page 90. You can also open and close an Internet connection manually here (see page 86).
<b>Basic Setup</b>	Launches Basic Setup.
<b>Advanced Setup</b>	Launches Advanced Setup.
<b>Logout</b>	Closes the current user's session and displays the login screen.

### Menu bar

The menu bar contains the functions that you can run.

- ◆ In Basic Setup you will see the steps you have to go through for configuration. You cannot make any selections. Configuration runs automatically.
- ◆ In Advanced Setup you will see a list of configuration options for the Gigaset Router. Clicking on an entry opens a menu in which you can select the function you want.



### Working area

Use the working area for configuration.

With configurable parameters you will see a dialogue box or selection list with default settings. There may be some limitations on the possible entries, e. g. entering special characters or certain value ranges. If your entry does not meet the rules for the box in question, you will see an error message. You can then repeat the input.

Once you have made any configuration changes on a page, you can activate the new setting by clicking on **APPLY** or **NEXT** at the bottom of the page.



Please read the following information if you are using Internet Explorer 5.0.

Once you have entered the command, the page will be properly updated if you have configured Internet Explorer as follows:

In **Extras – Internet options – General – Temporary Internet files – Settings** the setting for **Check for newer versions of the saved pages** should be set to **For every visit to the page**.

### Buttons

Basic Setup	<b>NEXT</b>	Opens the page for the next configuration step.
	<b>BACK</b>	Returns to the previous configuration step.
	<b>CANCEL</b>	Deletes all the entries on page since the last time it was opened.
	<b>FINISH</b>	Transfers the settings you have made to the router configuration.
Advanced Setup:	<b>HELP</b>	Displays help information about the current page.
	<b>APPLY</b>	Transfers the settings you have made to the router configuration.
	<b>CANCEL</b>	Deletes all the entries on page since the last time <b>APPLY</b> was run.
	<b>HELP</b>	Displays help information about the current page.

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

# General configuration with Basic Setup

Use Basic Setup for the general configuration of the Gigaset Router. This includes the settings for the WAN interface and wireless communication.

The router's **WAN** interface is used to provide a connection to the **Internet** for all the PCs connected to the router. You will need the access data you received from your **Internet Service Provider**. Please have it to hand.

*i*

Remember that configuration saves the access data in the router. Before passing your router on to somebody else or having your dealer replace it, you should first restore the factory settings. Otherwise unauthorised persons may use your Internet access data at your expense. To reset the router, press the reset button on the back for at least 5 seconds.

The router user interface guides you through configuration step by step. Once you have filled in a page, click on **NEXT**. If you want to make any changes or check your entries, click on **BACK**.

Click on **Basic Setup** in the opening screen or the navigation bar to start configuration.

## Select Country

**Select** In the first step of **Basic Setup** configuration choose your **Country**.

1. Country

<input type="radio"/> Austria	<input type="radio"/> Belgium	<input type="radio"/> Finland	<input type="radio"/> France
<input type="radio"/> Germany	<input type="radio"/> Greece	<input type="radio"/> Ireland	<input type="radio"/> Italy
<input type="radio"/> Netherlands	<input type="radio"/> Norway	<input type="radio"/> Portugal	<input type="radio"/> Spain
<input type="radio"/> Sweden	<input type="radio"/> Switzerland	<input type="radio"/> United_Kingdom	

NEXT

© Siemens AG 2002, 2003

- ◆ Check the box next to the appropriate country.

*i*

Selecting the country automatically selects the time zone as well. If necessary, you can set the time zone separately using Advanced Setup (see page 60).

- ◆ Click on **NEXT**.

### Wireless Settings

Use **Wireless Settings** to configure the router as an **Access point** of a wireless network (**WEP**). PCs that have a wireless network adapter can connect to the router. Accept the default settings. You can change them later on with Advanced Setup (see page 70).

#### 2. Wireless Settings

The Router can be quickly configured as a wireless access point for roaming clients by setting the access identifier. It also supports ..... data encryption and client filtering. ....

SSID :	<input type="text" value="ICMCPMVD BDP"/>
SSID Visible :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

- ◆ Click on **NEXT**.

## Configuring the WAN connection

In the next step you have to enter the access data for your WAN connection. You will have received the necessary information from your **Internet Service Provider (ISP)**.

If you have chosen Germany as your country, please read the next section. If you have chosen a different country, please turn to page 53.

### T-online

If you have chosen **Germany** as your country and use Internet services provided by T-online, enter the access data you have received from T-online in this page.

If you want to use the services from a different provider, select **Other Provider** from the list. Then read on from page 53.

**3a. Select ISP**


Set the parameter you got from your Internet Service Provider.

Select your Internet Service Provider :	T-DSL (T-Online) ▾
Connection identifier :	000123456789
T-Online number :	000123456789
Co-user number / suffix	0001
T-Online password	*****
Maximum Idle Time (0-60)	10 (minutes)
Auto-reconnect to the internet when a request is made.	<input type="checkbox"/> Auto-reconnect


© Siemens AG 2002, 2003 up ↗

## General configuration with Basic Setup

- ◆ Enter the required data.

	<ul style="list-style-type: none"><li>◆ <b>Maximum idle time</b> (Default setting: 0 minutes) This is the period of time after which the Internet connection is closed down automatically if no data is transmitted. Entering "0" deactivates the function. This means that the connection will remain open even if no data is transmitted. This can lead to high charges if you are using a time-based pricing system! In this case, you should enter a value other than "0".</li><li>◆ <b>Auto-reconnect</b> (Default setting: deactivated) Auto-reconnect means that applications such as Web browser, Messenger and Email can automatically open an Internet connection when they are launched. If you do not have <b>Flat rate</b>, this can lead to high charges being incurred. Therefore the default setting is deactivated. Please refer to page 86 for manually opening a connection.</li></ul>
---	---

- ◆ Once you have entered the data, click on **FINISH** to complete setup. Once you have completed configuration, the router will try to open an Internet connection. The router's Status page will appear with information about the connection.

	<ul style="list-style-type: none"><li>◆ You can change your settings later on with Advanced Setup. To do this open <b>WAN – PPPoE</b>.</li></ul>
---	--

## Other Internet Service Provider


First select the access type for your Internet connection. The options are:


- ◆ **DSL modem** (see page 54)
- ◆ **Cable modem** (see page 56)
- ◆ **DSL modem (alternative: PPTP)** (see page 57)


You will find information about the connection type and the access data you need for further configuration in the paperwork you received from your Internet Service Provider.


### 3. Broadband Type

Specify the WAN connection type required by your Internet Service Provider. Specify Cable modem, or xDSL modem.

 **DSL Modem**  
Generally used for DSL connections. May also be required by some cable suppliers who use PPPoE.

 **Cable Modem**  
Generally used for cable modems. Sometimes also used for a few ADSL modems with integrated router. The host name field is optional, but may be required by some Service Providers. If there is a Domain Name Server (DNS) that you would rather use, you need..... to specify the IP address in the "Advanced Setup | WAN | DNS" page.

 **DSL modem (alternative: PPTP)**  
The Point-to-Point Tunneling Protocol (PPTP) is also used for DSL connections in some European countries.

© Siemens AG 2002, 2003 

- ◆ Click on the connection type you are using.  
Depending on the connection type, you will see another page for entering the connection data.

## Configuring connection via DSL modem

Complete this page if you connect to the Internet via a DSL modem.

### 4. IP Address Information

This information is available from your Internet Service Provider; contact your provider if necessary. PPPoE is the latest access for ADSL modems without a separate router.

 **PPPoE: general case for ADSL (sometimes for specific cable providers)**

User Name (required):	<input type="text" value="000123456789000123456789"/>
Password :	<input type="password" value="*****"/>
Please retype your password:	<input type="password" value="*****"/>
Service Name (required):	<input type="text"/>
Inactivity time max. (0 to 60) (automatic connection clear-down if inactive for this length of time) :	<input type="text" value="10"/> (minutes) <input type="checkbox"/> Auto-reconnect

 **fixed IP: special case for ADSL**

IP Address	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>
Router IP Address	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>
DNS IP Address	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>
Subnet Mask	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>

- ◆ Select the connection type:
  - **PPPoE for DSL**  
Enter the **PPPoE** user name and password assigned by your Internet Service Provider.  
The Service Name is optional but may be required by some Internet Service Providers.

!	<ul style="list-style-type: none"> <li>◆ <b>Maximum idle time</b> (Default setting: 0 minutes) This is the period of time after which the Internet connection is closed down automatically if no data is transmitted. Entering "0" deactivates the function. This means that the connection will remain open even if no data is transmitted. This can lead to high charges if you are using a time-based pricing system! In this case, you should enter a value other than "0".</li> <li>◆ <b>Auto-reconnect</b> (Default setting: deactivated) Auto-reconnect means that applications such as Web browser, Messenger and Email can automatically open an Internet connection when they are launched. If you do not have <b>Flat rate</b>, this can lead to high charges being incurred. Therefore the default setting is deactivated. Please refer to page 86 for manually opening a connection.</li> </ul>
---	--

- **Fixed IP address Special case for DSL access**  
Some Internet Service Providers assign the router a **Static IP address**. If this is the case with your router, enter the assigned parameters in the dialog boxes, **IP address** is the address of the Gigaset Router and **Router's IP address** the router address of the Internet Service Provider.  
**DNS IP address** is the address of the Internet Service Provider's **DNS Server**.

- ◆ Click on **FINISH** to complete the setup.

Your WAN connection has now been configured.

Once you have completed configuration, the router will try to open an Internet connection. The router's Status page will appear with information about the connection.



### Configuring Connection via Cable modem

Complete this page if you connect to the Internet via a cable modem.

4. IP Address Information

**Cable Modem**

Host Name

MAC Address

"Cable modems" usually require minimal configuration. The connection between the Gigaset and the cable modem will be set up automatically when this type of configuration has been set. "Host name": This field is optional (you can leave it blank), but many service providers require it.

"Clone MAC address": Many service providers use your PC's MAC address (for identification) for connecting with the modem. As you have plugged your Gigaset between the two, you may need to generate a "Clone MAC address" for the PC so it can be assigned to the Gigaset. This will retain the process used by your service provider.

If there is a Domain Name Server (DNS) that you would rather use, you need to specify the IP address in the "Advanced Setup | WAN | DNS" page.

© Siemens AG 2002, 2003

- ◆ You may have been given a host name by your Internet Service Provider. If so, enter it in the box **Host name**.
- ◆ The **MAC address** is set by default to the router's physical WAN interface. Do not change this unless required to do so by your Internet Service Provider.



If your Internet Service Provider has used the MAC address of one of your PCs for registration when setting up your broadband account, connect **only** the PC with the registered MAC address to the router and click on **Clone MAC address**. Then the router's current MAC address will be replaced by the already registered MAC address of the PC. If you are not sure which PC was used as the identifier, have your Internet Service Provider register a new MAC address for your account. Then use this MAC address for the router.

- ◆ Click on **FINISH** to complete the setup.  
Your WAN connection has now been configured.

Once you have completed configuration, the router will try to open an Internet connection. If your configuration has been successful, a connection to your Internet Service Provider's home page will be opened.



In this connection type your router is assigned a **Dynamic IP address** by the Internet Service Provider.

- ◆ If you want to use a particular **DNS Server**, you will have to configure this in Advanced Setup. To do this, select **DNS** in the **WAN** menu (see page 66).
- ◆ If you want to use a PC in your network as a server, you can use the router's **DynDNS** service (see page 83).

## Configuring connection via DSL modem (alternative: PPTP)

Complete this page if you connect to the Internet via the Point-to-Point Tunneling Protocol (PPTP).

### 4. WAN Settings

**PPTP**

PPTP Account:

PPTP Password:

Please retype your password:

Host Name :

Service IP Address:

My IP Address:

My Subnet Mask:

Connection ID:  (Optional)

MTU (1400-1460):

Maximum Idle Time (0-60)  (minutes)

Auto-reconnect :

Enter the Account Name, Account Password, Host Name, Service IP Address, IP Address, Subnet Mask required by your ISP in the appropriate fields. If your ISP has provided you with a connection ID, enter it in the Connection ID field, otherwise, leave it as zero.

© Siemens AG 2002, 2003

- ◆ Enter the parameters assigned by your Internet Service Provider.

!

- ◆ **Maximum idle time** (Default setting: 10 minutes)  
This is the period of time after which the Internet connection is closed down automatically if no data is transmitted. Entering "0" deactivates the function. This means that the connection will remain open even if no data is transmitted. This can lead to high charges if you are using a time-based pricing system! In this case, you should leave the default setting or enter a value other than "0".
- ◆ **Auto-reconnect** (Default setting: deactivated)  
Auto-reconnect means that applications such as Web browser, Messenger and Email can automatically open an Internet connection when they are launched. If you do not have **Flat rate**, this can lead to high charges being incurred. Therefore the default setting is deactivated. Please refer to page 86 for manually opening a connection.

## General configuration with Basic Setup

- ◆ Click on ***FINISH*** to complete the setup.

Your WAN connection has now been configured.

Once you have completed configuration, the router will try to open an Internet connection. The router's Status page will appear with information about the connection.

## Configuration with Advanced Setup

In Advanced Setup you can configure all the Gigaset Router options. If you want, you can also make changes to the settings you made in Basic Setup. The following table shows the possibilities available in Advanced Setup.

Menu	Description
<b>System</b>	Here you can set the country and local time zone, assign a password for administrator access and define a PC that is permitted to carry out remote management of the Gigaset Router (see page 60).
<b>WAN</b>	Here you can check and change the configuration of your router's WAN connection (see page 64).
<b>LAN</b>	Here you can change the router's <b>Private IP address</b> and configure dynamic address assignment (see page 68).
<b>Wireless</b>	Here you can configure the options for wireless communication (channel, SSID and encryption) (see page 70).
<b>NAT</b>	Here you can configure the address mapping for using several public IP addresses, set up the router as a virtual server and configure special applications (see page 73).
<b>Firewall</b>	Here you can configure a number of security and special functions, e. g. access control for local PCs to the Internet or preventing hacker attacks (see page 77).
<b>DDNS</b>	Here you can carry out the <b>DynDNS</b> configuration (dynamic DNS) for the router (see page 83).
<b>UPnP</b>	Here you can activate and deactivate the router's universal plug and play function ( <b>UPnP</b> ) (see page 85).
<b>Tools</b>	Here you can back up and restore the current configuration for example, or restore the factory settings and update the system firmware (see page 87).

### System Configuration

---

You can use the Gigaset Router's system configuration

- ◆ to set or change the country (see below),
- ◆ to set or change the time zone (see page 60),
- ◆ to assign a password for accessing the router's user interface (see page 62),
- ◆ to enable access to the router user interface via a PC that is not on the local network (remote management) (see page 63).

### Setting the Country

---

You can use this page to set the country for the router. The country setting automatically sets the channel normally used for wireless connections in that country. You can change the channel on **Channel and SSID** (see page 70).

If you have configured your router with Basic Setup, this setting has already been made and can be changed here.

- ◆ In the **System** menu, select **Country**.

Country			
<input type="radio"/> Austria	<input type="radio"/> Belgium	<input type="radio"/> Finland	<input type="radio"/> France
<input type="radio"/> Germany	<input type="radio"/> Greece	<input type="radio"/> Ireland	<input type="radio"/> Italy
<input type="radio"/> Netherlands	<input type="radio"/> Norway	<input type="radio"/> Portugal	<input type="radio"/> Spain
<input type="radio"/> Sweden	<input type="radio"/> Switzerland	<input checked="" type="radio"/> United_Kingdom	

- ◆ If you want to change the setting, select the new country and click on **APPLY**.

### Setting the Time Zone

---

Information on the time zone is important for various time-dependent operations on the Internet. For example, the data packets sent in a particular country have to be sorted in the correct chronological order in the receiver's country. Access control to particular services can also be defined using time-based rules.

If you have configured your router with Basic Setup, the time zone was automatically defined appropriately for your setting for the **Country**. You can change the setting here.

- ◆ In the **System** menu, select **Time Zone**.

### Time Zone

Set the time zone of the Router. This information is used for log entries and client filtering.

#### Set Time Zone

(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾

Daylight Saving

Start from    End by

- ◆ Select your time zone from the selection list.
- ◆ If your time zone has summer and winter time, select **Daylight Saving** and use the selection list to specify the start and end of summer time.
- ◆ To apply the settings click on **APPLY**.

### Assigning passwords

After installation, your router configuration is not yet protected with a password. To prevent unauthorised changes to the configuration, you should assign a password and change this password from time to time.

- ◆ In the **System** menu, select **Password settings**.

#### Password Settings

Set a password to restrict management access to the Router.

- Current Password:
- New Password:
- Re-Enter Password for Verification:  
 (3-12 Characters)

- Idle Time Out:  Mins  
(Idle Time =0 : NO Time Out)

- ◆ Enter a password in the **New password** box and repeat it in the box underneath. The password must be between 3 and 12 characters long. It is not case sensitive. Avoid names and all too obvious words. Use a combination of letters, numbers and special characters.

*i*

If you ever forget the password you will have to reset your router. To do this, hold down the reset button on the back of the router for at least five seconds. Please bear in mind that this will restore **all** the settings to the factory configuration. No password will be active either.

- ◆ Check the value in **Idle time out**. Use the box to define when the configuration session should be automatically terminated if no more entries are made. The default entry is 10 minutes. For security reasons you should enter a smaller value.

**!**

If you enter 0 the session will **never** be cut automatically.

- ◆ To apply the settings click on **APPLY**.

## Remote Management

Remote management enables a PC that is not on your local network to be used to configure the Gigaset Router with a standard Web browser.

- ◆ In the **System** menu, select **Remote Management**.

**Remote Management**

Set the remote management of the Router. If you want to manage the Router from a remote location (outside of the local network), you must also specify the IP address of the remote PC.

Host Address	Enabled
<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	<input type="checkbox"/>

- ◆ In **Host address** enter the IP address of the PC that is to have access to the router's user interface from outside your local network.

i

- ◆ Remember that the Internet Service Provider may assign a dynamic IP address to the PC and so that it will change. Make sure that the PC always has the same IP address.
- ◆ If you use the IP address 0.0.0.0, any PC can be used to manage the Gigaset Router.

- ◆ Check the **Enabled** box.
- ◆ To apply the settings click on **APPLY**.



### WAN Configuration

If you have configured your router with Basic Setup, you have already configured your router's **WAN** connection. Use the WAN configuration option in Advanced Setup to check and change these settings.

You can use your Gigaset Router as a **Router** or **Bridge**. With the **Bridge** option, the WAN connection is configured as a link to other local networks.

The **WAN** menu offers the following entries:

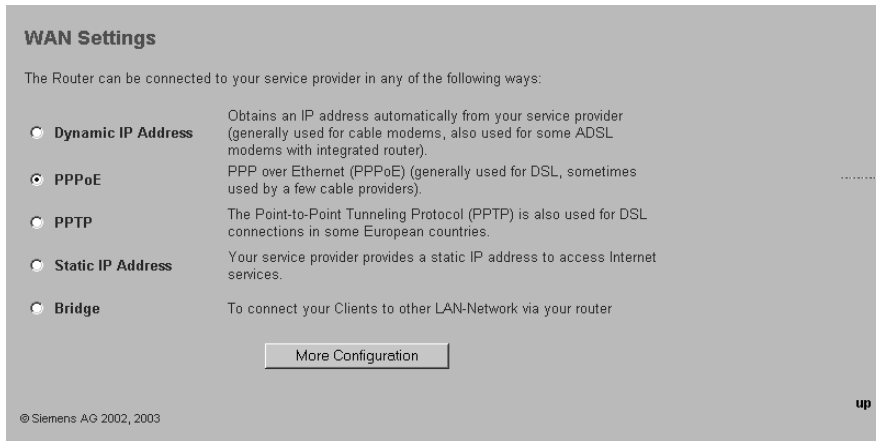
- ◆ Select **Dynamic IP**, if the router's WAN connection is assigned a **Dynamic IP address** by your Internet Service Provider. Configuration is similar to Basic Setup, as described on page 56.
- ◆ Select **PPPoE**, if you use PPP over Ethernet (**PPPoE**) for your WAN connection (e. g. for T-DSL (T-Online)). Configuration is similar to Basic Setup, as described on page 55.
- ◆ Select **PPTP**, if you use the Point-to-Point Tunneling Protocol (**PPTP**) for your WAN connection. Configuration is similar to Basic Setup, as described on page 57.
- ◆ Select **Static IP address**, if the router's WAN connection is assigned a **Static IP address** by your Internet Service Provider. Configuration is similar to Basic Setup, as described on page 55.
- ◆ Select **DNS**, if you want to use a particular **DNS Server** (see page 66).
- ◆ Select **Bridge**, if you want to use your router as a bridge (see page 67).

*i*

Remember that configuration saves the access data for your WAN connection in the router. Before passing your router on to somebody else or having your dealer replace it, you should first restore the factory settings. Otherwise unauthorised persons may use your Internet access data at your expense. To reset the router, press the reset button on the back for at least 5 seconds.

You can also open the page for WAN configuration via the **WAN Settings** window.

- ◆ Select **WAN in the menu bar**.



- ◆ Select the WAN connection type you use for your Internet connection.
- ◆ Click on **More configuration** to enter the configuration parameters for the selected connection type.

### Defining a DNS Server

The **DNS** service handles the mapping of domain names (Web addresses) to IP addresses. Most Internet Service Provider offer a **DNS Server**. In this case you do not need to enter anything here. If however you want to use a particular DNS server, you will have to enter the IP address of the DNS server on this page. You can enter a second DNS server in case the first one cannot be reached.


- ◆ In the **WAN** menu, select **DNS**.

**DNS**

A Domain Name System (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as `www.my-siemens.com`, a DNS server will find that name in its index and find the matching IP address e.g.: `192.147.25.20`. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.

Domain Name Server (DNS) Address:  .  .  .

Secondary DNS Address (optional):  .  .  .

© Siemens AG 2002, 2003 

- ◆ Enter the IP address of the DNS server(s) and click on **APPLY**.

## Configuring as a bridge

If you select **Bridge** for the router, it can be used as a link between its local network (**LAN**) and other LAN segments. In Bridge mode the router's WAN connection acts as a connection to another LAN.



The router's WAN connection can no longer be used for Internet access however.

- ◆ In the **WAN** menu, select **Bridge**.

### Bridge Settings

With bridging mode, the router acts as a network bridge. Network bridges connect two LANs or LAN segments. Because bridging disables NAT, you must have multiple IP addresses available (for example, as part of your account with your ISP) if you want to use bridging to connect multiple computers to the internet. In this case, when a computer on your network attempts to connect to the internet, it must be set up either to use a static (fixed) IP address or to obtain an address directly from the ISP.

**Bridge Mode :**  Enabled  Disabled

**LAN IP**

**IP Address:**  .  .  .

**IP Subnet Mask:**

© Siemens AG 2002, 2003

- ◆ Select **Bridge mode**.
- ◆ Enter the router's local **IP address** and click on **APPLY**.

## LAN Configuration

You can use LAN configuration to

- ◆ define an IP address for the router and
- ◆ define whether the router should automatically assign the IP addresses for the PCs in your local network or not.

The default IP address for the router is 192.186.2.1. This is the router's **Private IP address**. This is the address under which the router can be reached on the local network. It can be freely assigned from the block of available addresses. The IP address under which the router can be reached from outside is assigned by the Internet Service Provider.

The router has a **DHCP Server**, whose factory setting is active. Thus the PCs' IP addresses are automatically assigned by the router. If you want to assign static IP addresses for the PCs, you will have to deactivate the DHCP server.

*i*

- ◆ If the router's DHCP server is active, configure the PCs' network settings so that the **Obtain an IP address automatically** option is checked. To find out how to do this, please turn to page 17 in "Configuring the local network".
- ◆ If you deactivate the router's DHCP server, you will have to assign a static IP address for the PCs using the network settings. This is described in Practical Tips and Configuration Examples on the supplied CD.

- ◆ Select **LAN** in the menu bar.

### LAN Settings

You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on specific clients or protocols. The Router must have an IP address for the local network.

#### LAN IP

IP Address:	192 . 186 . 2 . 1
IP Subnet Mask:	255.255.255.0
DHCP Server:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Lease Time: Forever

#### IP Address Pool

Start IP:	192 . 186 . 2 . 2
End IP:	192 . 186 . 2 . 254
Domain Name:	<input type="text"/> (optional)

### LAN IP

- ◆ If you want to assign the router a different IP address, enter it in **IP address**.

*i*

We recommend using an address from the block that is reserved for private use. This is the address block 192.168.0.0 - 192.168.255.254.

- ◆ If the DHCP server is active, you will have to specify a **Lease time**. Lease Time defines the period of time in which the PCs retain the IP address assigned to them **without** changing them. For small networks you can set **Lease time to Forever**. This means that an IP address is assigned for an unlimited period of time.

### IP address pool

In **IP address pool** enter the range of IP addresses that the router is to use for automatically assigning IP addresses to the PCs.

- ◆ Enter the first and last addresses.

*i*

The first three fields of the beginning and end IP address always have as their default setting the first three fields of the router's IP address because the subnet mask is always 255.255.255.0. This means that the first three address segments for all network components must be identical.

- ◆ To apply the settings click on **APPLY**.

### Configuring Wireless Connections

If you want to connect PCs in wireless mode via the Gigaset SE105 dsl/cable, you will have to configure the router as an **Access point**. Use **Wireless Settings** for this configuration. Here you can

- ◆ activate the router's wireless module (see below),
- ◆ change the wireless channel and the Service Set ID (**SSID**) of the router (see below) and
- ◆ set **Encryption** for wireless transmissions (see page 72).

#### Activating the wireless module

Wireless devices can register with your router only if its wireless module has been activated.

- ◆ Open the **Wireless menu**.
- ◆ Activate the wireless module on **Wireless Settings**.
- ◆ Click on **APPLY**.

#### Setting the Channel and SSID

Before wireless network components can communicate with each other, you have to use a shared wireless channel and the same **SSID** (Service Set Identifier).

The Gigaset SE105 dsl/cable comes supplied with the SSID configured as **ConnectionPoint**. For security reasons, it is advisable to change this SSID and deactivate the broadcast function (**SSID visible**).

- ◆ In the **Wireless** menu, select **Channel and SSID**.

**Channel and SSID**

This page allows you to define SSID and Channel ID for the wireless connection. In the wireless environment, this Router can be acting as an wireless access point. These parameters are used for the mobile stations to connect to this access point.

SSID :	<input type="text" value="ICM CP M VD BDP"/>
Channel :	<input type="text" value="10"/>
SSID Visible :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

### ◆ **SSID**

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

*i*

- ◆ Remember that the connection to the wireless network adapters will be interrupted until you enter the new SSID on them as well.
- ◆ You will find a detailed example of how to change the SSID in "Practical Tips and Configuration Examples" on the supplied CD.

### ◆ **Channel**

Wireless channel used by the Gigaset Router to communicate with other wireless network components.

*i*

The available channel settings are governed by your country's regulations. They define the number of available channels. The default setting is determined by the country setting (see page 49). You should not change this setting unless you have a good reason to do so.

### ◆ **SSID visible**

If the option has been activated, the Gigaset Router includes the SSID in all data transmissions. In this case eavesdroppers could use the SSID to gain access to your network.

If the option is deactivated, wireless network components that want to connect to the local network must know the SSID. This offers a certain degree of protection against unauthorised access.

- ◆ To apply the settings click on **APPLY**.



### Setting the Encryption

---

If you are sending sensitive data over wireless channels, we recommend that you activate **WEP-Encryption** on your wireless network components.



Wired Equivalent Privacy (WEP) protects data transmitted between wireless nodes. However WEP does not protect transmission on your wired network or over the Internet.

To activate WEP encryption on your wireless network components:

1. Activate Web encryption on your Gigaset SE105 dsl/cable and generate a 64- or 128-bit key. Make a note of the generated key.
2. Activate Web encryption on wireless network adapters and enter the generated 64- or 128-bit key.

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

Keys can be generated automatically. You can also enter them manually. For automatic 64-bit encryption, you enter a passphrase that is used to generate four keys. For automatic 128-bit encryption, a single key is generated from the passphrase.



You will find a detailed example of how to set WEP encryption in "Practical Tips and Configuration Examples" on the supplied CD.

## NAT Configuration

---

Your Gigaset Router comes supplied with the NAT function (Network Address Translation). The NAT function acts as a firewall against unauthorised access from the Internet.

- ◆ All the local IP addresses of the PCs in the local network are mapped to the router's Public IP address. This means that each PC on the local network communicates with the Internet via the router's IP address. One advantage of this is that only one Internet access has to be bought from the Internet Service Provider even if you use several PCs. A further advantage is that the PCs' local IP addresses remain anonymous thus preventing any direct external access to the PCs on the local network. The router knows which PC has launched which Internet application and ensures that each local user receives the right data.
- ◆ No data from the Internet is allowed into your local network unless it has been explicitly requested by one of the PCs on that network.
- ◆ The router opens only **one** Port for each Internet application, e. g. for email, FTP or HTTP.

You can use the router's NAT settings to

- ◆ configure address mapping.  
If you have several public IP addresses, your PCs can use them as well as the router's IP address to connect to the Internet. This can be done by configuring the address mapping appropriately (see page 74).
- ◆ set up the router as a virtual server.  
If you want to offer files or Web services that are on a PC in your local network to other Internet users, you will have set the router up as a virtual server (see page 75).
- ◆ configure Special Applications  
Some applications, such as games, network conferences and voice over Internet, will not work if Network Address Translation (NAT) has been activated. If you want to use such applications nevertheless, then you will have to configure them as "Special Applications" (see page 76).

### Defining Address mapping

In the default setting, all the local PC IP address are mapped to your router's public IP address. If you have a large number of users on your local network, it may be advisable to order several IP addresses from your Internet Service Provider. Then use address mapping to define which local IP addresses will connect to the Internet via which public IP address.



Remember that connections via several IP addresses through the WAN port can lead to bottlenecks because all the connections have one hardware interface.

- ◆ In the **NAT** menu, select **Address mapping**.

#### Address Mapping

Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This feature limits the number of public IP addresses required from the ISP and also maintains the privacy and security of the local network. We allow one or more than one public IP address to be mapped to a pool of local addresses.

Address Mapping	
1. Global IP: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	is transformed as multiple virtual IPs
from <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	to <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
2. Global IP: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	is transformed as multiple virtual IPs
from <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	to <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
3. Global IP: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	is transformed as multiple virtual IPs

- ◆ Enter the public IP addresses you want to share in the **Global IP** boxes.
- ◆ Enter in the line underneath the range of local IP addresses that are to share this public IP address.
- ◆ To apply the settings click on **APPLY**.

## Setting up the router as a virtual server

---

If you want to offer files or Web services that are on a PC in your local network to other Internet users, set the PC up as a server (e. g. as FTP or HTTP server). However the router's NAT function does not normally allow "external" access to PCs on the local network. To make services available on the Internet from local PCs, you have to set up the router as a virtual server.

Externally the router takes on the role of the server. It receives the requests of remote users under its public IP address and automatically redirects them to the local PCs. The private IP addresses of the servers on the local network remain protected.

Internet services are addressed via defined port numbers. The router needs a mapping table of the port numbers to redirect the service requests to the server that actually makes the service available.

You have to set up this mapping table.



You will find a detailed example of how to set up the router as a virtual server in "Practical Tips and Configuration Examples" on the supplied CD.

### Configuring Special Applications

One property of NAT is that data from the Internet is not allowed into your local network unless it has been explicitly requested by one of the PCs on that network. Most Internet applications run behind the NAT **Firewall** without any problems. If you request Internet pages, for example, or send and receive emails, the request for data from the Internet comes from a PC on the local network and so the router allows the data through. The router opens exactly **one Port** for the application. If an external application tries to send a call to a PC within the local network, the router will block it. There is no open port via which the data could enter the local network.

Some applications, such as games, network conferences and voice over the Internet, require several links, i.e. several ports, so that the users can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to the user on the local network. These applications cannot work if Network Address Translation (NAT) has been activated. If you want to use such applications nevertheless, then you will have to configure them as **Special Applications**. This means:

- ◆ You define a so-called trigger port for the application and assign it the public ports that have to be opened for the application.
- ◆ The router checks all outgoing data for the port number. If it recognises a match with a defined Trigger Port, then it will open the assigned public ports and notes the IP address of the PC that sent the data. If data comes back from the Internet via one of these public ports, it allows the data through and directs it to the right PC. A trigger event always comes from a PC within the local network. If a Trigger Port is addressed from outside, it is simply ignored by the router.



You will find a detailed example of how to configure special applications in "Practical Tips and Configuration Examples" on the supplied CD.

## Firewall Configuration

The router's **Firewall** functions include various security functions for the local network. You can

- ◆ protect your network against hacker attacks (see page 78),
- ◆ enable only selected PCs to access your network (see page 80),
- ◆ restrict or totally block local users' access to the Internet (see page 81),
- ◆ exclude certain PCs from the firewall (see page 82).



Since the firewall has little impact on system performance, we recommend that you activate it.

### Activating the firewall

- ◆ Select the **Firewall** menu.



- ◆ Activate the firewall functions in the working area.
- ◆ Click on **APPLY**.

The firewall functions are now activated.

## Protection against hacker attacks

If you have activated your router's firewall functions, it will monitor and restrict the access of data arriving via the WAN connection with a function called Stateful Packet Inspection (SPI). This allows the router to identify and prevent certain types of attacks from the Internet, such as Denial-of-Service (DoS). DoS attacks are aimed at devices and networks with Internet connections. The aim is not so much to steal data but to paralyse the computer or network to such an extent 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 machine for example and receive the data meant for you.



The router prevents the following DoS attacks: Ping of Death (Ping Flood), SYN Flood, IP Fragment (Teardrop), Brute-Force, Land, IP Spoofing, IP with Zero Length, TCP Null Scan (Port Scan), UDP Port Loopback, Snork etc.

You can use the **Intrusion detection** page to change the standard firewall settings and arrange to be notified by email about any attempted hacker attacks.

- ◆ In the **Firewall** menu, select **Intrusion detection**.

### Intrusion Detection

When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the Router will support full operation as initiated from the local LAN.

The Router firewall can block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

- **Intrusion Detection Feature**

SPI and Anti-DoS firewall protection	<input checked="" type="checkbox"/>
RIP defect	<input checked="" type="checkbox"/>
Discard Ping From WAN	<input type="checkbox"/>
- **Stateful Packet Inspection**

FTP Service	<input checked="" type="checkbox"/>
H.323 Service	<input checked="" type="checkbox"/>
TFTP Service	<input checked="" type="checkbox"/>
- **When hackers attempt to enter your network, we can alert you by e-mail**

Your E-mail Address:

SMTP Server Address:

### Changing the standard firewall settings

You can activate or deactivate the following functions:

- ◆ ***SPI and anti-DoS firewall protection***

The router monitors incoming data traffic. If this option has been activated, the router will only let those data packets through that have requested by applications run by users on your local network. All other data packets will be rejected.

You can release applications for incoming traffic using ***Stateful Packet Inspection***. If for example you activate only ***FTP service***, all incoming traffic will be blocked apart from the data for FTP connections that have been initiated on the local network.

- ◆ ***RIP error***

RIP is a protocol used by routers to exchange information about their networks.

Faulty RIP packets slow down the data flow and can be provoked to paralyse a network. If this option has been activated, the firewall will identify and reject RIP errors.

- ◆ ***Reject Ping from WAN side***

A ping command can be used to tell whether a PC can be reached via the network.

If you activate this option, all attempts to contact a computer on the local network with a ping will be blocked.

### Notification of attempted hacker attacks

You can choose to be informed by email about a possible hacker attack.

- ◆ Enter in the dialog boxes in ***When hackers attempt to enter your network, we can alert you by e-mail***.
  - the email address to be used for notification about hacker attacks.
  - the address of the SMTP server (email server) of your Internet Service Provider, e. g. [mailto.t-online.de](mailto:t-online.de).
- ◆ To apply the settings click on ***APPLY***.



### Enabling only selected PCs to access your local network

In the **MAC filtering table** you can enter up to 32 PCs that are allowed to access your local network. All other computers will be denied access. Access control is based on the PCs' **MAC address**.

- ◆ In the **Firewall** menu, select **MAC filtering table**.

**MAC Filtering Table**

This function allows you to configure the MAC filter. When enabled, only configured MAC addresses will have access to your network. All other client devices will be denied access. This security feature can support up to 32 devices and applies to clients.

- MAC Address Control :  Yes  No
- MAC Filtering Table (up to 32 computers)

ID	Client PC MAC Address
1	00 : 01 : e3 : 00 : ef : b7
2	:  :  :  :  :  :
3	:  :  :  :  :  :
4	:  :  :  :  :  :
5	.  .  .  .  .  .

- ◆ Activate the **Yes** option next to **MAC Address Control** so that the MAC addresses of accessing PCs are checked.

There are two ways of making entries in the **MAC filtering table**:

- ◆ Enter the MAC addresses of those PCs you want to have access manually in **Client PC MAC address**.
- ◆ If you have activated **DHCP**, all the PCs that are currently logged in will appear in the **DHCP Client list** at the bottom of the page. Select a PC, decide in which row of the table the entry is to appear and click on **Copy to**. The MAC address of the selected PC will be transferred to the table.
- ◆ Once you have entered all the PCs you want, click on **APPLY**.



If you have activated the MAC address filter, you should enter at least one PC from which you can configure the router. Otherwise you will not have any access to the router's user interface. If you have accidentally denied router access for all the PCs, you will have to completely reset the router. To do this, hold down the reset button on the back of the router for at least five seconds.

## Restricting access of local PCs to the Internet

Under the general heading **Firewall** the Gigaset Router offers the following protection functions:

- ◆ Complete isolation of a PC
 

This allows you to prevent any access at all to Web pages from a given PC. To do this use the functions on the **Firewall – Access control** page.
- ◆ Blocking certain URLs
  - Keyword filtering
 

This allows you to prevent the opening of Web pages whose **URL** contains certain keywords that you have defined.

Example: Keyword *abcd*

This would block a website with the URL `http://www.abcd.com`
  - URL filtering
 

This allows you to prevent the displaying of a website with a particular URL address.

Example: URL `http://www.abcd.com/products`

This would block precisely the Web page `http://www.abcd.com/products`.
  - Domain blocking
 

This allows you to block a particular URL address and all the subsequent addresses that begin with the same sequence of characters.

Example: Domain `http://www.abcd.com`

All Web pages beginning with `http://www.abcd.com` would be blocked, e.g. `http://www.abcd.com` and also `http://www.abcd.com/products`, `http://www.abcd.com/service`, `http://www.abcd.com/products/product_graphics1.htm` etc.

To do this use the functions on the **Firewall – URL blocking** page.
- ◆ Time limits for blocks
 

You can define a particular block period or a schedule during which certain blocks become active. You can include the four block strategies described above in this schedule.

To do this use the functions on the **Firewall – Schedule Rule** page.



You will find a detailed example of how to set Internet blocks in "Practical Tips and Configuration Examples" on the supplied CD.

### Opening the firewall for particular PCs (DMZ)

Some applications do not work properly behind a firewall because they require unrestricted data flow in both directions. In this case you can define a so-called demilitarised zone (DMZ) for PCs running such applications.



When setting up DMZ PCs make sure that the PCs always have the same IP address. This means:

- ◆ the IP addresses must be static (see "Practical Tips and Configuration Examples") or
- ◆ the Lease time for dynamic address assignment must be set to **Forever** (see page 69).

- ◆ In the **Firewall** menu, select **DMZ**.

**DMZ(Demilitarized Zone)**

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.

Enable DMZ:  Yes  No

Multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To use the DMZ, you must set a static IP address for that PC.

Public IP Address	Client PC IP Address
1. 217.235.113.92	192.168.2.7
2. <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	192.168.2.0
3. <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	192.168.2.0
4. <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	192.168.2.0
5. <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	192.168.2.0

- ◆ The **Public IP address** has as the first entry the router's **Public IP address**. If you have other public IP addresses, enter them under the router address.
- ◆ In **Client PC IP address** enter the IP addresses of the PCs you want to exclude from the firewall functions.



Please bear in mind that these PCs are no longer protected against unauthorised access from the Internet and as such could be a security risk for your network. You should use this option only in emergency situations.

- ◆ To apply the settings click on **APPLY**.

## Activating dynamic DNS

---

A service you want to make available on the Internet is accessible via a **Domain name**. Your router's **Public IP address** is assigned to this Domain name. If your Internet Service Provider for your local network's WAN connection assigns the IP address dynamically, the IP address of the router can change. Then the assignment to the Domain name is no longer valid and your service will no longer be available.

In this case you must ensure that the assignment of the IP address to the Domain name is regularly updated. This is handled by the dynamic DNS Service (**DynDNS**). You can use the DynDNS service to assign your Gigaset Router an individual static Domain name on the Internet even if it does not have a static IP address.

There are various providers on the Internet offering free DynDNS Service. The Gigaset Router uses the DynDNS Service from **DynDNS.org** (<http://www.DynDNS.org>). If you use the service of this DynDNS provider, then your service can be reached on the Internet as a subdomain of one of the DynDNS.org domains.

If you have activated the router's DynDNS function, it will monitor its public IP address. When this changes, it will open a connection to DynDNS.org and update its IP address there.

You have to open an account with DynDNS.org before you can use the router's DynDNS function. Follow the instructions on the DynDNS.org website. Then enter the account user data when configuring the router.

## Configuration with Advanced Setup


- ◆ Select the **DDNS** menu.

**DDNS (Dynamic DNS) Settings**

Dynamic DNS provides users on the internet a method for tying their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

Dynamic DNS :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Server Provider:	WWW.DynDNS.ORG
Host Name :	<input type="text"/>
User :	<input type="text"/>
Password :	<input type="text"/>
Mail Exchanger (optional):	<input type="text"/>
Backup MX?	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Wildcard :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

HELP APPLY CANCEL ...

© Siemens AG 2002, 2003 

- ◆ You have to activate the **Dynamic DNS** option on **DDNS (Dynamic DNS) settings** so that the DynDNS service can be used.

**i**

The other entries have to match the entries you made when opening the account with DynDNS.org.

- ◆ To apply the settings click on **APPLY**.

## Using the universal plug and play function

PCs with UPnP (Universal Plug & Play) can run their network configuration themselves and automatically use services offered on the network.

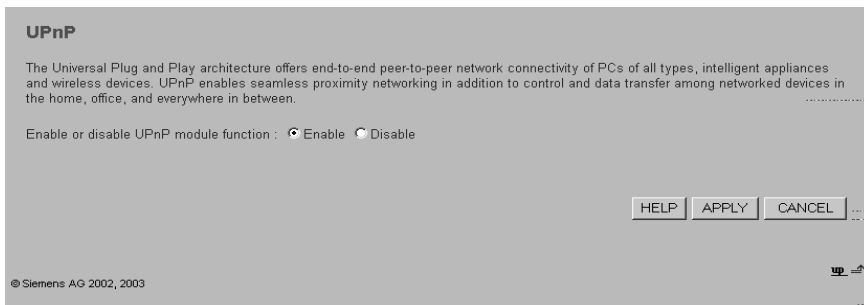
*i*

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

If you have installed UPnP on your PC's operating system and activated it on the router, an icon for your Gigaset Router will appear in the PC task bar. Windows XP systems will also include the icon under network connections. Clicking on this icon opens the Gigaset Router's configuration page.

To activate the router's UPnP function:

- ◆ Select **UPnP** in the menu bar.



- ◆ Activate UPnP.
- ◆ Click on **APPLY**.

# Gigaset Router Administration

The Gigaset Router user interface includes several helpful functions for administering your router. You can

- ◆ set up and close an Internet connection manually (see below),
- ◆ save and restore the router configuration data and, if required, reset the factory settings (see page 87),
- ◆ upgrade the router firmware (see page 88),
- ◆ re-boot the router (see page 89),
- ◆ view information about the router configuration and status (see page 90),
- ◆ check, save and clear the security log (see page 91).

## Opening or closing an Internet connection manually

You can open and close an Internet connection manually. If for example you deactivated **Auto-reconnect** when you configured the WAN interface, Internet applications (such as your browser or email application) will not automatically open a connection when they are launched. In this case, you will have to open the connection manually when it is required and also close it again when you are finished with it.

Opening and closing an Internet connection manually:

- ◆ Click on **Status** in the navigation bar.

Below the status information for the **INTERNET** you will see two buttons.

For PPPoE or PPTP connections:

**Disconnect** Cuts an open connection to the Internet.

**Connect** Opens a connection to the Internet.

For connections with a dynamic router IP address:

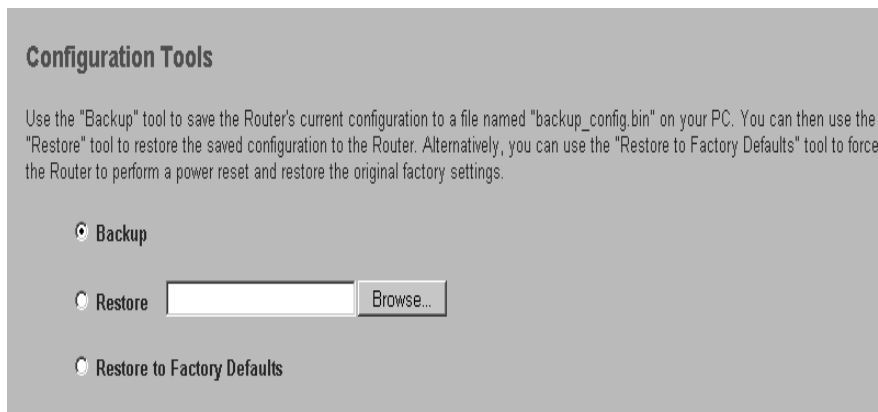
**Release** Cuts an open connection to the Internet and releases the IP address.

**Renew** Opens a connection to the Internet and forces the DHCP server to assign a new IP address.

## Saving and restoring a configuration

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

- ◆ In the **Tools** menu, select **Configuration tools**.



### Saving the configuration data

- ◆ Select the option **Backup**.
- ◆ Click on **APPLY**.
- ◆ Your browser opens a window in which you can run the backup routine for the router configuration file. Confirm this with **OK**. Then select a directory on your local PC to which the configuration file is to be backed up and give it a name (default name: `config.bin`). Confirm this once again with **OK**.

Once the procedure has been completed, the current configuration data of your router will have been backed up in the specified file.

### Restoring the back-up

- ◆ Select the option **Restore**.
- ◆ Click on **Browse** and select the configuration file (`config.bin`) you want to restore.
- ◆ Click on **APPLY**.

### Restoring Factory Defaults

- ◆ You can restore the original factory settings by activating **Restore to factory defaults** and clicking on **APPLY**.



You can also restore the factory settings by pressing the reset button on the back of the Gigaset Router for at least 5 seconds (see page 11). This option is always available even if you cannot access the router's user interface.



## Firmware Upgrade

You can load the latest firmware for the router. First you will have to obtain the latest firmware version. This is available on the Siemens website [www.my-siemens.com/se105](http://www.my-siemens.com/se105). Then carry out the following steps:

- ◆ Download the new firmware from the Siemens website and save it on your PC.
- ◆ Close down all network activities on your local network.
- ◆ In the **Tools** menu, select **Firmware Upgrade**.


### Firmware Upgrade

This tool allows you to upgrade the Router system firmware using a file provided by Siemens.


Enter the path and name of the upgrade file then click the APPLY button below. You will be prompted to confirm the upgrade.

Upgrade Target


- ◆ Click on **Browse** and select the file you downloaded from the Internet.
- ◆ Click on **APPLY**.
- ◆ A window will appear prompting you to confirm that you want to update the firmware. Click on **OK**.
- ◆ The next window will warn you that the router will not be available for about a minute during the upgrade procedure. Acknowledge this message **promptly** with **OK**.

 Some browsers abort the upgrade process if you do not click on **OK** immediately.

The firmware will now be updated.

 Do not switch the router off during the upgrade procedure.

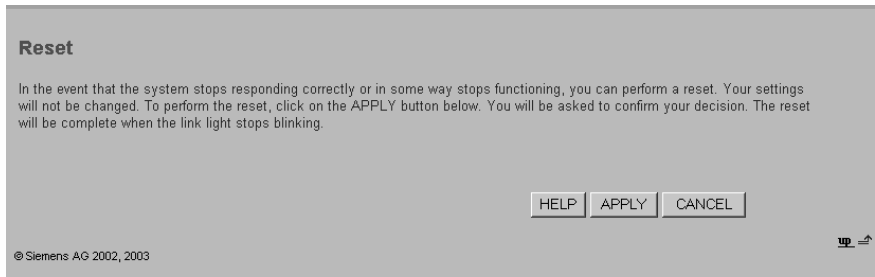
After successful upgrading, the router is automatically rebooted. All the LEDs will go out. Once the process has been completed, the PWR LED will light up again. The browser will show the router login screen.

 Use the **Status** tab in **INFORMATION** to check whether the upgrade process was in fact successful (see page 90). Here you should see the latest firmware version for your router.

## Resetting the router

You can reset the router if it no longer functions properly. The router will be rebooted and should then work properly.

- ◆ In the **Tools** menu, select **Reset**.



- ◆ Click on **APPLY**. You will see a dialog window prompting you for further confirmation.

The reboot procedure takes a few moments. Then you have to log on again before you can make any changes to the configuration.



You can also reboot the router by briefly pressing the reset button on the back or switching the router off and on again (see page 11).

## Displaying the router's Status

The **Status** tab shows information about the router's configuration and connection status. In addition, you can open and close an Internet connection manually, and also check, save and clear the security log.

- ◆ Click on **Status** in the navigation bar.

**Status**

You can use the Status screen to see the connection status for the router's WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your network.

Current Time: Mon May 5 13:04:19 2003

**INTERNET**  
Cable/DSL: CONNECTED  
WAN IP: 217.235.113.92  
Subnet Mask: 255.0.0.0  
Router: 217.5.98.8  
Primary DNS: 212.185.252.201  
Secondary DNS: 194.25.2.129

**Router**  
IP Address: 192.168.2.1  
Subnet Mask: 255.255.255.0  
DHCP Server: Enabled  
Firewall: Enabled

**INFORMATION**  
Numbers of DHCP Clients: 3  
Runtime Code Version: V1.00.0237  
Boot Code Version: V1.00.0023  
LAN MAC Address: 00-01-E3-01-91-A2  
WAN MAC Address: 00-01-E3-01-91-A3  
Hardware Version: 01  
Serial Num.: A242105052

Disconnect Connect

---

**Security Log**  
View any attempts that have been made to gain access to your network.

Mon May 05 12:31:33 2003	:	192.1.1	▲
Mon May 05 12:30:10 2003	:	192.1.1	
Mon May 05 12:29:06 2003	:	192.1.1	
Mon May 05 11:56:47 2003	:	Seco	n
Mon May 05 11:56:47 2003	:	Prima	
Mon May 05 11:56:47 2003	:	local	
Mon May 05 11:56:47 2003	:	local	
Mon May 05 11:56:47 2003	:	local	
Mon May 05 11:56:47 2003	:	PPPoE	▼

Save Clear Refresh

**DHCP Client Log**  
View information on LAN DHCP clients currently linked to the Router.

ip=192.168.2.158	mac=00-90-96-
ip=192.168.2.33	mac=00-90-96-3
ip=192.168.2.66	mac=00-01-E3-0

HELP BACK

© Siemens AG 2002, 2003

## Router information

The following information is displayed:

**Current time**

Shows the current time.

**INTERNET**

Shows the connection type of the WAN connection and whether it is active or not. If it is, you will see further information about the connection.

**ROUTER**

Shows the private IP address of the router and the subnet mask of the local network.

Shows whether the DHCP server of the router and the firewall are active.

**INFORMATION**

Provides the following information:

- ◆ The number of connected PCs,
- ◆ The firmware versions,
- ◆ The MAC address of the LAN side of the router,
- ◆ The MAC address of the WAN connection,
- ◆ The hardware version number,
- ◆ The product serial number,

**DHCP Client Protocol**

Displays information about all the DHCP clients in your network.

**Working with the security log**

---

The **Security log** lists all the accesses and attempted accesses to your network. It contains the following information:

- ◆ Date and time of access
- ◆ IP address of the accessing PC
- ◆ Nature of the access

You can do the following:

- |                |  |
|----------------|--|
| <b>Save</b>    | Saves a security log. You will see a dialog window asking you where you want to save the log file. |
| <b>Clear</b>   | Clears the content of the security log.  |
| <b>Refresh</b> | Updates the security log.  |

# Appendix

## Fault tracing

This chapter describes common problems and their solution. The Gigaset Router is easy to monitor thanks to its LED displays. Problems can be quickly identified. If you cannot solve the connection problem after checking the LED displays, please consult the other sections of the following table.

Symptom	Possible cause and solutions
PWR lamp does not light up.	No power supply. <ul style="list-style-type: none"> <li>◆ Check whether the mains unit is connected to the Gigaset Router and a power outlet.</li> <li>◆ Check whether the power outlet and the mains unit are working properly. If the mains unit is not working properly, please get in touch with our customer service unit (see page 97).</li> </ul>
(LINK/ACT) display of a connected device does not light up.	No LAN connection <ul style="list-style-type: none"> <li>◆ Make sure that the connected device is switched on.</li> <li>◆ Check whether the Ethernet cable is plugged in.</li> <li>◆ Check that you are using the right cable type (CAT 3, 4 or 5) and that the cable is not too long (100 m).</li> <li>◆ Check that the network card on the connected device and the cables are not defective. If necessary, replace a defective network card or cable.</li> <li>◆ 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.</li> </ul>
WLAN display does not light up.	<ul style="list-style-type: none"> <li>◆ Activate the router's wireless module (menu <b>Wireless</b>).</li> </ul>

Symptom	Possible cause and solutions
You cannot connect to the Internet.	<ul style="list-style-type: none"> <li>◆ Check that you are using the right cable to connect to the modem. Depending on the modem you are using, the cable must have either straight or cross wiring. Please consult your modem operating instructions. The Ethernet cable supplied has straight wiring.</li> <li>◆ Check whether the <b>Auto-reconnect</b> option has been deactivated (for PPPoE or PPTP connections). In this case, connections cannot be opened automatically. Select <b>Auto-reconnect</b>. Remember that this setting may lead to higher costs if you are billed on the time used.</li> <li>◆ If the <b>Auto-reconnect</b> option has been activated, perhaps the connection was terminated manually on the <b>Status</b> tab using the <b>Disconnect</b> button. <ul style="list-style-type: none"> <li>– Open the connection manually using the <b>Connect</b> button again or</li> <li>– restart your router.</li> </ul>           In both cases, the <b>Auto-reconnect</b> setting will be active again. </li> </ul>
You cannot open a connection from a wireless device to the Gigaset Router.	<p>The wireless network adapter is not using the correct SSID.</p> <ul style="list-style-type: none"> <li>◆ Change the SSID on the network adapter.</li> </ul> <p>WEP encryption has been activated on the Gigaset Router but not on the wireless network adapter or it is using the wrong WEP key.</p> <ul style="list-style-type: none"> <li>◆ Activate WEP encryption on the network adapter with the correct key.</li> </ul> <p>If you do not know the key, you will have to reset your router. To do this, hold down the reset button on the back of the router for at least five seconds.</p> <p><b>Warning:</b> Please bear in mind that this will restore <b>all</b> configuration settings to the factory settings.</p>

Symptom	Possible cause and solutions
The Gigaset Router or other PCs cannot be reached by a PC in the connected LAN with a ping command.	<ul style="list-style-type: none"> <li>◆ Make sure that TCP/IP has been installed and configured on all the PCs on the local network.</li> <li>◆ Check that the IP addresses have been properly configured. In most cases, you can use the Gigaset Router's DHCP function to assign dynamic addresses to the PCs in the LAN. In this case, you have to configure the TCP/IP settings of all the PCs so that they obtain the IP address automatically.</li> </ul> <p>If you configure the IP addresses in the LAN manually, remember to use the subnet mask 255.255.255.0. This means that the first three parts of the IP address on each PC and the router have to be identical. The router also has to be configured as DNS server and as default router.</p>
No connection to the router's configuration interface	<ul style="list-style-type: none"> <li>◆ Use the ping command to check whether you can establish a network connection to the Gigaset Router.</li> <li>◆ Check the network cable between the PC you want to use to administer the router and the Gigaset Router.</li> <li>◆ If the PC you want to use is on the router's local network, make sure that you are using the correct IP address administration (see above).</li> <li>◆ If the PC you want to use is not on the router's local network it must be authorised via Remote Management.</li> </ul>
Password forgotten or lost	<ul style="list-style-type: none"> <li>◆ Hold down the reset button on the back of the router for at least five seconds to restore the factory settings.</li> </ul> <p><b>Warning:</b> Please bear in mind that this will restore <b>all</b> configuration settings to the factory settings.</p>
You cannot access a resource (drive or printer) on a different PC	<ul style="list-style-type: none"> <li>◆ Make sure that TCP/IP has been installed and configured on all the PCs on the local network and that the PCs all belong to the same workgroup.</li> <li>◆ Check whether the resource has been released on the PC in question and whether you have the necessary access rights.</li> <li>◆ Printing: Check whether the printer has been set up as a network printer.</li> </ul>

## Specifications

---

Standards	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX FastEthernet 802.11b
WAN interface	10Base-T/100Base-TX
LAN interface	10Base-T/100Base-TX 4 RJ-45 Ports LAN data transmission rate up to 10/20Mbps (10Base-T half/full duplex) or 100/200Mbps (100Base-TX with half/full duplex)
Management	Browser-based management Both DHCP server and also client available
Advanced performance features	Dynamic configuration of IP addresses – DHCP, DNS Firewall – Client privileges, protection against hacker attacks, log file Virtual server via NAT & NAPT Virtual Private Network – PPTP, L2TP, IPSec Pass-Through Identification of intruders, email warnings, parental control
LED displays	LAN (Connection/Link, Activity/ACT), WAN (Connection/Link, Activity/ACT), power (PWR)
Dimensions	156 mm x 129 mm x 30 mm
Weight	470 g
Input power	9 V 1A
Maximum current	0.04A RMS max. at 110V/240V
Power consumption	5 Watt max. with 100-240 V AC
Internet Standards	RFC 826 ARP, RFC 791 IP, RFC 792 ICMP, RFC 768 UDP, RFC 793 TCP, RFC 854-859 TELNET, RFC 1321 MD5, RFC 1497 BOOTP Extension, RFC 1570 PPP LCP Extension, RFC 1631 NAT, RFC1661 PPP, RFC 1700 Assigned Numbers, RFC 1866 HTML, RFC 1945 HTTP, RFC 1994 CHAP, RFC 2131 DHCP, RFC 2637 PPTP
Temperature	Operating temperature from 5 to 40° C Storage temperature from -40 to 70 °C
Humidity	5 % to 95 % (non condensing)
Safety	EN60950 IEC60950
as per	Immunity: EN 61000-3-2/3, EN 61000-4-02.03.04/05.06.08/11



Special conditions prevailing in your country have been taken into consideration.  
The router complies with the R&TTE Guidelines, as shown by the CE mark.

# SIEMENS

Information and Communication Mobile

### Declaration of Conformity

We, Siemens AG  
Information and Communication Mobile  
Cordless Products  
ICM CP

Frankenstrasse 2  
46395 Bocholt  
Germany

declare, that the hereinafter mentioned product is manufactured according to our Full Quality Assurance System certified by CETECOM ICT Services GmbH with the registration number "Q810820M" in compliance with

#### ANNEX V of the R&TTE-Directive 1999/5/EC

**Product:** „Gigaset SE 105 dsl/cable“ EU\* Version  
Wireless Router according IEEE 802.11b

The presumption of conformity with the essential requirements regarding Council Directive 99/05/EC is ensured according to

Art. 3.1 a)	Safety:	<b>EN60950</b> <i>(equivalent to 73/23/EC)</i>
Art. 3.1 a)	EMF/SAR:	<b>99/519/EC (EU-Council Recommendation)</b> <b>EN 50360</b> <i>ICNIRP Guideline</i>
Art. 3.1 a)	Acoustic Shock:	<b>Not applicable</b>
Art. 3.1 b)	EMC:	<b>ETS 301 489-1/17</b> <i>(equivalent to 89/336/EC)</i>
Art. 3.2	Radio:	<b>EN 301 328-2</b>

The product is labelled with the European Approvals Marking CE 0682 0 including notified Body and Equipment Class Identifier.  
Any unauthorized modification of the product voids this Declaration.

\*This Product is also intended for use in the European Economic Area (EEA) and Switzerland  
National Authorities were informed according to Article 6.4 of Frequency Notification.

Special national Requirements are considered.

Bocholt, 17 January 2003  
Place and Date

  
.....  
Mr. Leiblich  
Senior Approvals Manager

## Service (Customer Care)

---

You have access to straightforward support concerning with technical aspects of your device and how to operate it through our Online Support on the Internet:

[www.my-siemens.com/customer-care](http://www.my-siemens.com/customer-care)

or you can refer to the section "Fault tracing" on page 92.

If you have any trouble with the equipment, please contact the **Siemens telephone service**:

**United Kingdom**      0 87 05 33 44 11

**Ireland**                18 50 77 72 77

The Siemens Service is only available to deal with device faults only. Your specialist dealer will be able to help you with any questions about operating your device.

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

## Guarantee certificate (United Kingdom)

---

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

- ◆ In the case of new devices and their components exhibiting defects resulting from manufacturing and/or material faults within 24 months of purchase, Siemens shall, at its own option and free of charge, either replace the device with another device reflecting the current state of the art, or repair the said device. In respect of parts subject to wear and tear (including but not limited to, batteries, keypads, casing), this warranty shall be valid for six months from the date of purchase.
- ◆ This Guarantee shall be invalid if the device defect is attributable to improper treatment and/or failure to comply with information contained in the user manuals.
- ◆ This Guarantee shall not apply to or extend to services performed by the authorised dealer or the customer themselves (e.g. installation, configuration, software downloads). User manuals and any software supplied on a separate data medium shall be excluded from the Guarantee.
- ◆ The purchase receipt, together with the date of purchase, shall be required as evidence for invoking the Guarantee. Claims under the Guarantee must be submitted within two months of the Guarantee default becoming evident.

- ◆ Ownership of devices or components replaced by and returned to Siemens shall vest in Siemens.
- ◆ This Guarantee shall apply to new devices purchased in the European Union. The Guarantee is issued by Siemens plc, Siemens House, Oldbury, Bracknell, Berkshire, RG12 8FZ.
- ◆ Any other claims resulting out of or in connection with the device shall be excluded from this Guarantee. Nothing in this Guarantee shall attempt to limit or exclude a Customers Statutory Rights, nor the manufacturer's liability for death or personal injury resulting from its negligence.
- ◆ The duration of the Guarantee shall not be extended by services rendered under the terms of the Guarantee.
- ◆ Insofar as no Guarantee default exists, Siemens reserves the right to charge the customer for replacement or repair.
- ◆ The above provisions does not imply a change in the burden of proof to the detriment of the customer.

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

## Guarantee certificate (Ireland)

---

### Scope

- ◆ This equipment guarantee applies to end users ("customers"). This guarantee does not in any way affect the customer's statutory rights.
- ◆ The guarantee applies to the supplied devices and all their components but not to their installation or configuration or to the services provided by the dealer. Manuals and any software supplied on a separate data medium are excluded from the guarantee. This guarantee does not apply to decorative covers or any other personalised parts or software not included in the scope of supply. The guarantee also does not apply to decorative top or bottom shells for special editions.
- ◆ The guarantee provides for devices or components that, despite proper care and use, have demonstrably developed defects due to faulty workmanship and/or faulty materials to be replaced or repaired at our discretion free of charge. The guarantee does not cover normal wear and tear. Alternatively, we reserve the right to replace the defective device with a successor model or reimburse the original purchase price on return of the defective device. Our decision is final. Any legal claims are excluded.

- ◆ Claims under the guarantee cannot be made if the defect or damage was caused by improper care or use. Improper care or use includes the following:
  - Opening the device (this is classed as third-party intervention)
  - Manipulating components on the printed circuit board
  - Manipulating the software
  - Defects or damage caused by dropping, breaking, lightning or ingress of moisture. This also applies if defects or damage were caused by mechanical, chemical, radio interference or thermal factors (e.g. microwave, sauna, etc.).
  - Repairs or other work done by persons not authorised by us.
  - Devices fitted with accessories not authorised by Siemens.
- ◆ Any further claims due to damage are excluded, such as damage arising outside the device, provided this was not due to gross negligence and/or intent on our part.
- ◆ Claims under the guarantee must be made as soon as the defect is noticed.
- ◆ A till receipt showing the date of purchase must be presented as proof. Each claim under the guarantee is accepted with the express reservation that subsequent investigations confirm the validity of the claim.
- ◆ Any devices or components that are replaced become our property.
- ◆ The costs of materials and labour will be borne by us, but not the costs of transport, postage or freight.
- ◆ We are entitled, at our discretion, to make technical changes (such as firmware updates) beyond repair or replacement in order to upgrade the device to the latest state of the art. There is no additional charge to the customer for this work. Our decision is final. Any legal claims are excluded.
- ◆ The guarantee is valid in the country of purchase. It applies only if the device is operated in the relevant geographical area in accordance with the information on the packaging and in the operating instructions.
- ◆ Any further claims are excluded. Siemens is not liable in any circumstances for downtime, loss of profits, loss of data or loss of any other information. The customer alone is responsible for safeguarding such data and information.
- ◆ Changes to this guarantee require prior approval by Siemens in writing.

### **Guarantee period**

- ◆ The guarantee applies in countries in the EU from 1 January 2002 for a period of 24 months.
- ◆ In all other countries the guarantee period shall be the relevant minimum statutory guarantee period, but no longer than 24 months.
- ◆ The guarantee period starts on the day of purchase by the customer.
- ◆ A successful claim under the guarantee does not extend the guarantee period.
- ◆ Work under the guarantee is handled by our Customer Care Centres.

# Glossary

### Access point

An Access Point, such as the Gigaset SE105 dsl/cable, is the centre of a wireless local network (**WEP**). It handles the connection of the wireless linked network components and regulates the data traffic in the wireless network. The Access Point also serves as an interface to other networks, e. g. an already 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 modus describes wireless local networks (**WEP**) in which the network components set up a spontaneous network without an **Access point**, e. g. several Notebooks in a conference. All the network components are peers. They must have a wireless **Network adapter**.

### Auto-reconnect

Auto-reconnect means that applications such as Web browser, Messenger and Email can automatically open an **Internet** connection when they are launched. This can lead to high charges if you are not using **Flat rate**. Auto-reconnect can be deactivated at the Gigaset Router to save call charges.

### Bridge

A Bridge connects several network segments to form a joint network, e. g. to make a **TCP/IP** network. The segments can have different physical characteristics, e. g. different connections such as **Ethernet** and wireless LANs. Linking individual segments via Bridges 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 on the network. The Gigaset Router does not pass broadcast packets on; they always remain within the local network (**LAN**) it administers.

### BSSID

Basic Service Set ID

BSSID permits unique differentiation of one wireless network (**WEP**) 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 in large networks – especially the **Internet** – the defining of IP addresses is very complex as participants frequently move, drop out or new ones join.

A DHCP Server automatically assigns the connected network components (DHCP Clients) Dynamic IP addresses from a defined IP address pool thus saving a great deal of configuration work. It also allows address pools to be used more effectively: Since not all participants are on the network at the same time, the same IP address can be assigned to different network components in succession as and when required.

The Gigaset Router includes a DHCP Server and so it can automatically assign IP addresses for the PCs on its local network. You can configure the Lease time so that once an IP address has been assigned it will never change.

### **DHCP Server**

See DHCP

### **DMZ**

Demilitarised Zone

DMZ describes a part of a network that is outside the Firewall. A DMZ is so to speak set up between a network you want to protect (e. g. a LAN) and an insecure network (e. g. the Internet). A DMZ is useful if you want to offer Server services on the Internet which for security reasons are not to be run from behind the firewall or if Internet applications do not work properly behind a firewall. A DMZ permits unrestricted access from the Internet to only one or a few network components, while the other network components remain secure behind the firewall.

### **DNS**

Domain Name System

DNS permits the assignment of IP addresses to computer or Domain names that are easier to remember. A DNS Server has to 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 computers in the local network and the next higher Name Server, which again knows addresses in its network and that of the next Name Server.

### **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 to such an extent 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 machine for example and receive the data meant for you.

### **DSL**

Digital Subscriber Line

## Glossary

DSL is a data transmission technique in which a connection to the **Internet** can be run at 1.5 **Mbps** over normal telephone lines. A DSL connection is provided by an **Internet Service Provider**. It requires a DSL modem.

### Dynamic IP address

A dynamic **IP address** is assigned to a network component automatically via **DHCP**. Depending on the setting for the **Lease time** the IP address of a network component can change every time it logs on or in certain time intervals.

See also: **Static IP address**

### DynDNS

Dynamic DNS

Domain Name Service (**DNS**) is used to assign **Domain names** and **IP addresses**. For **Dynamic IP addresses** this service is now enhanced with so-called Dynamic DNS (**DynDNS**). This permits the use of a PC with a changing 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 Router **WEP** encryption for secure data transmission over wireless networks.

### Ethernet

Ethernet is a network technology for local networks (**LAN**) defined by **IEEE** as Standard IEEE 802.3. Ethernet uses a base band cable with a transmission rate of 10 or 100 **Mbps**.

### Firewall

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

See also: **NAT, SPI**

### Flat rate

Flat rate is a particular billing system for **Internet** connections. The **Internet Service Provider** charges a monthly fee regardless of the duration and number of logins.

### Full duplex

Data transmission 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 transfer. Only one side can receive or send data at a time.

See also: **Full duplex**

**http proxy**

An HTTP proxy is a **Server** that network components use for their **Internet** connections. All requests are sent via the proxy.

**Hub**

A Hub connects several network components in a star-topology network by sending all the data it receives from one network component to all the other network components. See also **Switch, Bridge, Router, Gateway**

**IEEE**

Institute of Electrical and Electronics Engineers

IEEE is an international body for defining network standards, especially for standardizing **LAN** technologies, transmission protocols and speeds, and wiring.

**IEEE 802.11**

IEEE 802.11 is a standard for wireless 2.4-GHz band LANs. In so-called **Infrastructure mode** end devices can be connected to a base station (**Access point**) or connect with each other spontaneously (**Ad-hoc mode**).

**Infrastructure mode**

Infrastructure mode is a way of operating wireless local networks (**WEP**), in which an **Access point** handles the data traffic. Network components cannot establish a direct connection with each other as is the case in **Ad-hoc mode**.

**Internet**

The Internet is a wide-area network (**WAN**) linking several million users around the world. A number of **Protocols** have been defined for exchanging data known by the name **TCP/IP**. All participants in the Internet are identifiable by an **IP address**. Servers are addressed by a **Domain name** (e. g. siemens.com). Domain Name Service (**DNS**) is used to assign Domain names to IP addresses.

Among the most important Internet services are:

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

**Internet Service Provider**

An Internet Service Provider offers access to the **Internet** for a fee.

**IP**

Internet Protocol

The IP **Protocol** is one of the **TCP/IP** protocols. It is responsible for the addressing of participants in a network using **IP addresses** and routes data from the sender to the recipient. It decides the paths along which the data packets travel from the sender to the recipient in a complex network (routing).

**IP address**

An IP address is a network-wide unique address of a network component in a network based on the **TCP/IP** protocol (e. g. in a local network (**LAN**) or on the **Internet**). The IP address has four parts (decimal numbers) separated by periods (e. g. 192.168.2.1). The IP address comprises the network number and the computer number. Depending on the



## Glossary

**Subnet mask** one, two or three parts form the network number, the remainder the computer number. You can find out the IP address of your PC using the `ipconfig` command.

IP addresses can be assigned manually (see **Static IP address**) or automatically (see **Dynamic IP address**).

On the Internet **Domain names** are normally used instead of the IP addresses. **DNS** is used to assign Domain names to IP addresses.

The Gigaset Router has a **Private IP address** and a **Public IP address**.

### **IP address pool**

The Gigaset Router's IP address pool defines a range of **IP addresses** that the router's **DHCP Server** can use to assign **Dynamic IP addresses**.

### **IPSec**

Internet Protocol Security

The term IPSec covers a number of **Protocols** used for encrypted transmission of data packets over the **Internet**. IPSec uses digital certificates for device authentication. IPSec is offered by Internet Service Providers for implementing Virtual Private Networks (**VPN**).

See also: **PPTP**, **L2TP**

### **ISP**

Internet Service Provider see **Internet Service Provider**

### **L2TP**

Layer Two Tunneling Protocol

L2TP is an extension of **PPTP** and is offered by **Internet Service Providers** for implementing Virtual Private Networks (**VPN**). It covers most of the features of PPTP but with less overhead and is better for managed networks.

### **LAN**

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

With the Gigaset SE105 dsl/cable you can set up both a wired local **Ethernet** network and a wireless **IEEE 802.11b**-standard network.

### **Lease time**

Lease Time defines the period of time in which the PCs retain the **Dynamic IP address** assigned to them by the **DHCP** server without changing them.

### **Local IP address**

See **Private IP address**

### **MAC address**

Media Access Control

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

### **Mbps**

Million of bits per second

Specification of the transmission speed in a network.

**MTU**

Maximum Transmission Unit

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

**NAT**

Network Address Translation

NAT is a method for implementing IP addresses (mostly **Private IP addresses**) in a network on one or more **Public IP addresses** on the **Internet**. With NAT several network components in a **LAN** can share the router's public IP address to connect to the Internet. The network components of the local network are hidden behind the router's IP address registered on the Internet. As a result of this security function NAT is frequently used as part of the network **Firewall**. If you want to make services on a PC in the local network available on the Internet despite NAT, you can configure the Gigaset Router 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 files and peripherals. A general distinction is made between local networks (**LAN**) and wide-area networks (**WAN**).

**Network adapter**

The network adapter is the hardware device that realises the connection of a network component to a local network. The connection can be wired or wireless. A wired network adapter is for example an Ethernet network card. Wireless network adapters are for example the Gigaset USB Adapter 11 and the Gigaset PC Card 11.

A network adapter has a unique address, the **MAC address**.

**Port**

Data is exchanged between two applications in a network via a Port. The port number addresses an application within a network component. The combination **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 every time they need one.

**Port Forwarding**

In Port Forwarding the Gigaset Router 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 on the local network to offer services on the Internet without them needing a **Public IP address**.

See also: **Virtual server**

**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.

**PPTP**

Point-to-Point Tunneling Protocol = Punkt-zu-Punkt-**Tunneling**-Protokoll§

## Glossary

An **Internet** connection using PPTP **Protocol** that creates a "tunnel" within an Internet connection for secure private connection in which the data are sent in encrypted form. The PPTP protocol is used in a Virtual Private Network (**VPN**).

### Private IP address

The private **IP address** is a network component's address on 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 Router, have a private and a **Public IP address**.

### Protocol

A protocol describes the agreements for communicating on a network. A protocol contains rules for opening, administering and closing a connection, about data formats, time frames and error handling. Communications between two applications require different protocols at various levels, e. g the **TCP/IP** protocols for the **Internet**.

### Public IP address

The public **IP address** is a network component's address on the **Internet**. It is assigned by the **Internet Service Provider**. Devices that act as a link from a local network, such as the Gigaset Router have a public and a private **Private IP address**.

### Remote Management

Remote Management describes the possibility of administering a network from a network component that is not on the local network (**LAN**) itself.

### Router

A router directs data packets from one local network (**LAN**) to another via the fastest route. A router permits the connecting of network with different network technologies. For example, it can link a local network with **Ethernet** or **WEP** technology to the **Internet**. See also: **Bridge, Switch, Hub, Gateway**

### Server

A Server makes a service available to other network components (**Clients**). Frequently the term Server is used for a computer or PC. But it can also mean an application that provides a particular services such as **DNS** or Web service.

### SMTP

Simple Mail Transfer Protocol

The **SMTP Protocol** is part of the **TCP/IP** protocol family. It governs the exchange of electronic mail on the **Internet**. Your **Internet Service Provider** provides you with access to an SMTP server.

### SPI

Stateful Packet Inspection

SPI is a packet filter used in a **Firewall** as protection against hacker attacks. If SPI has been activated, the router applies particular security rules to inspect all data packets arriving from the **Internet**. This will identify **DoS attacks** (Denial of Service) for example.

### SSID

Service Set Identifier

The SSID is used to identify the stations of a wireless network (**WEP**). All wireless network component with the same SSID form a common network. The SSID can be assigned by the network operator.

**Static IP address**

A static **IP address** is assigned to a network component manually during network configuration. Unlike a **Dynamic IP address**, a static IP address never changes.

**Subnet mask**

The subnet mask determines how many parts of the **IP addresses** of a network represent the network number and how many the computer number.

The subnet mask administered by the Gigaset Router is always 255.255.255.0. That means the first three parts of the IP address form the network number and the final part is used for assigning computer numbers. The first three parts of the IP address of all network components are in this case always the same.

**Subnetwork**

A subnetwork divides a network into smaller units.

**Switch**

A Switch, like a **Hub**, is an element for linking different network segments or components. Unlike a hub, the switch has its own intelligence that enables it to further packets to only that subnetwork or network component they are meant for.

See also: **Bridge**, **Hub**, **Router**, **Gateway**

**TCP**

Transmission Control Protocol

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

See also: **UDP**

**TCP/IP**

**Protocol** family on which the **Internet** is based. **IP** forms the foundation for each 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.

**Tunneling**

Tunneling is a procedure in which the data traffic of the one **Protocol** is transmitted with the help of a different protocol. For example, data packets of a private network can be packed in **IP** packets and transported over the Internet as if in a tunnel. Tunneling procedures are used nowadays for the secure transmission of data in a Virtual Private Network (**VPN**). The IP packets from the local network are encrypted using a tunneling protocol (e. g. **PPTP**) before being sent over the Internet.

**UDP**

User Datagram Protocol

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

**UPnP**

Universal Plug and Play

## Glossary

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 on the network automatically.

### URL

Universal Resource Locator

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

### Virtual server

A virtual [Server](#) provides a service on the [Internet](#) that runs not on itself but another network component. The Gigaset Router can be configured as a virtual server. It then directs incoming calls for a service via [Port Forwarding](#) directly to the appropriate [Port](#) of the network component in question.

### VPN

Virtual Private Network = virtuelles privates Netzwerk§

A VPN is a network connection in which the data are transmitted over the [Internet](#) using special [Tunneling](#) protocols (e. g. [PPTP](#), [L2TP](#), [IPSec](#)) securely, i.e. encrypted. VPNs are used to connect private networks at different locations with each other without having to lease a transmission line. The Internet is used instead.

### WAN

Wide Area Network

A WAN is a network that is not restricted to one particular area, such as the [Internet](#). A WAN is run by one or more public providers to enable private access. You access the Internet via an [Internet Service Provider](#).

### WEP

Wired Equivalent Privacy

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

### Wireless network

See [WEP](#)

### WLAN

Wireless LAN

Wireless LANs enable network components to communicate with and access a network using radio waves and 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 so-called 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 SE105 dsl/cable complies with Standard 802.11b.

# Index

## Numerics

10 Mbps .....	15
display .....	10
10/100 Mbps Switch Port .....	11
100 Mbps .....	15
display .....	10
128-bit key .....	72
64-bit key .....	72

## A

Access point .....	50, 70, 100
Access to the Internet	
blocking .....	77
permitting .....	77
restricting .....	77
Access to the local network	
blocking .....	80
permitting .....	80
Address block for IP addresses .....	69
Address mapping .....	73
configuring .....	74
Ad-hoc mode .....	6, 100
Advanced Setup .....	44
Antenna .....	12, 14
Attempted access	
displaying an .....	91
Auto-reconnect .....	52
auto-reconnect .....	55, 57, 100

## B

Back panel .....	11
Backup .....	87
Basic Setup .....	44, 49
Block	
time limits .....	81
Bridge .....	64, 67, 100
Broadcast .....	70, 100
BSSID .....	100
Buttons	
Advanced Setup .....	48
Basic Setup .....	48

## C

Cable modem .....	56
connecting to the router .....	13

Channel	
for wireless connections .....	60
Checking network settings	
(Windows XP) .....	29
Client .....	100
for Microsoft Network .....	18
Command	
exit .....	42
ipconfig / release .....	42
ipconfig / renew .....	42
ping .....	43
Command prompt	
opening the .....	43
config.bin, configuration file .....	87
Configuration data	
restoring the .....	87
saving the .....	87
Configuration file, config.bin .....	87
Configuration session	
Time limit on inactivity .....	62
Connection	
checking to the router .....	43
statistics .....	43
Connection method .....	28
Connection type	
selecting the .....	53
ConnectionPoint .....	13, 14
Country selection .....	49, 60
Creating a network installation disk	
(Windows XP) .....	29

## D

Deactivating the http proxy	
Windows 2000 .....	41
Windows 98 .....	25
Windows XP .....	33
Define computer name	
Windows 2000 .....	36
Windows 98 .....	19
Windows XP .....	29
Define workgroup	
Windows 2000 .....	36
Windows 98 .....	19
Windows XP .....	29
Demilitarised zone see DMZ	
Denial-of-Service attack see DoS attack	

## Index

DHCP ..... 17, 100  
DHCP Server ..... 101  
DHCP Service see DHCP  
Digital Subscriber Line see DSL  
DMZ ..... 7, 82, 101  
DNS ..... 64, 101  
DNS configuration  
    Windows 2000 ..... 40  
    Windows 98 ..... 24  
    Windows XP ..... 32  
DNS Server ..... 64, 68, 101  
    defining for the router ..... 66  
DNS Service see DynDNS  
Domain blocking ..... 81  
Domain name ..... 83, 101  
Domain Name Service see DNS  
DoS attack ..... 78, 101  
DSL connection ..... 102  
    via PPPoE ..... 55  
    with fixed IP address ..... 55  
DSL modem  
    configuring the connection ..... 54  
    connecting to the router ..... 13  
Dynamic DNS see DynDNS  
Dynamic DNS Service see DynDNS  
Dynamic Host Configuration Protocol  
    see DHCP  
Dynamic IP address ..... 17, 64, 102  
DynDNS ..... 83, 102  
DynDNS Service see DynDNS  
DynDNS.org ..... 83

**E**

Encryption ..... 72, 102  
Ethernet ..... 6, 102  
    cable ..... 13, 15  
    Transmission speed ..... 6  
Ethernet cable ..... 15  
    Maximum length ..... 13  
exit command ..... 42

**F**

Factory settings ..... 87  
Fast Ethernet ..... 15  
Features ..... 6  
Firewall ..... 7, 77, 81, 102  
    activating the ..... 77  
Firmware  
    updating the ..... 88

    version ..... 91  
Flat rate ..... 52, 55, 57, 102  
Front panel ..... 10  
full duplex ..... 102

## G

Games on the Internet ..... 76  
Gateway ..... 23, 102  
Gigaset Router see Router  
Gigaset SE105 dsl/cable ..... 5  
Global IP address see Public IP address

## H

Hacker attack ..... 7, 78, 101  
    notification of ..... 79  
half duplex ..... 102  
Host name ..... 56  
http proxy ..... 103  
Hub ..... 103

## I

IEEE ..... 103  
Infrastructure mode ..... 6, 103  
Installation ..... 8  
Installing network services  
    (Windows 2000) ..... 35  
Installing the TCP/IP protocol  
    Windows 2000 ..... 37  
    Windows 98 ..... 20  
Institute of Electrical and Electronics  
    Engineers see IEEE  
Internet ..... 103  
Internet access ..... 5  
    restricting ..... 77  
Internet connection ..... 49  
    auto-reconnect ..... 52, 55, 57  
    connecting manually ..... 86  
    disconnect automatically ..... 52, 57  
    disconnecting automatically ..... 55  
    disconnecting manually ..... 86  
Internet Protocol see IP address  
Internet Service Provider ..... 103  
    select ..... 51  
IP address ..... 103  
    Address block ..... 69  
    assigning automatically ..... 68  
    assigning automatically an ..... 17  
    assigning static addresses ..... 68  
    dynamic ..... 17, 64, 83, 102

- forcing an assignment . . . . . 86
- local . . . . . 73
- private . . . . . 106
- public . . . . . 73, 75, 106
- releasing an . . . . . 86
- router . . . . . 44
- static . . . . . 55, 107
- IP address pool . . . . . 69, 104
- IP Protocol . . . . . 103
- ipconfig / release . . . . . 42
- ipconfig / renew . . . . . 42
- IPSec . . . . . 6, 104
- ISP see Internet Service Provider
  
- K**
- Keyword filtering . . . . . 81
  
- L**
- L2TP . . . . . 6, 104
- LAN . . . . . 5, 104
- LAN socket . . . . . 11
  - transmission speed . . . . . 15
- Language file . . . . . 46
- Language selection . . . . . 46
- Layer Two Tunneling Protocol see L2TP
- Lease time . . . . . 69, 104
- LED displays . . . . . 10
- Local Area Connection
  - creating a wired . . . . . 15
  - setting up a wireless . . . . . 14
- local IP address see private IP address
- Local network . . . . . 6, 104
  - configuring a . . . . . 17
- Login screen . . . . . 44
  
- M**
- MAC address . . . . . 56, 104
  - cloning the . . . . . 56
  - LAN connection . . . . . 91
  - WAN connection . . . . . 91
- MAC filtering table . . . . . 80
- Maximum Transmission Unit see MTU
- Mbps . . . . . 104
- Menu bar . . . . . 47
- MTU . . . . . 105
  
- N**
- NAT . . . . . 73, 105
  - configuration . . . . . 73
  - Firewall function . . . . . 7
- Navigation bar . . . . . 47
- Network . . . . . 105
- Network adapter . . . . . 105
- Network Address Translation
  - see NAT
- Network configuration . . . . . 17
  - Windows 2000 . . . . . 35
  - Windows 98 . . . . . 18
  - Windows XP . . . . . 27
  
- O**
- Obtain an IP address automatically
  - Windows 2000 . . . . . 40
  - Windows 98 . . . . . 22
  - Windows XP . . . . . 32
- Opening screen . . . . . 45
- Operating state . . . . . 10
  
- P**
- Parental control . . . . . 7
- Password . . . . . 45
  - assigning a . . . . . 62
  - changing a . . . . . 62
- PC
  - defining a name (Windows 2000) . . 36
  - defining a name (Windows 98) . . . 19
  - defining a name (Windows XP) . . . 29
  - IP address . . . . . 17
  - isolating a . . . . . 81
  - network settings . . . . . 17
  - Setting up as Client for Microsoft
    - Networks . . . . . 18
  - ping command . . . . . 43
  - rejecting from WAN side . . . . . 79
- Point-to-Point Protocol over Ethernet
  - see PPPoE
- Point-to-Point Tunneling Protocol
  - see PPTP
- Port . . . . . 105
  - opening for an application . . . . . 76
  - Public Port . . . . . 76
  - Trigger Port . . . . . 76
- Port Forwarding . . . . . 105
- Port number . . . . . 105
  - mapping . . . . . 75
- Power supply unit
  - socket . . . . . 11



## Index

PPPoE . . . . . 6, 64, 105  
PPPoE DSL . . . . . 55  
PPTP . . . . . 6, 57, 64, 106  
Private IP address . . . . . 106  
Problem solving . . . . . 92  
Protection functions . . . . . 81  
Protocol . . . . . 106  
Public IP address . . . . . 106

## R

Releasing TCP/IP settings  
    Windows 2000 . . . . . 34, 42  
    Windows 98 . . . . . 26  
Remote Management . . . . . 63, 106  
Reset button . . . . . 11  
Reset function . . . . . 11  
RIP error . . . . . 79  
Router . . . . . 106  
    activating the . . . . . 16  
    Back panel . . . . . 11  
    backing up the configuration . . . . . 87  
    booting the . . . . . 89  
    configuration file . . . . . 87  
    configuring as a bridge . . . . . 64  
    configuring the . . . . . 44  
    connecting . . . . . 13  
    displaying information . . . . . 90  
    dynamic IP address . . . . . 83  
    front panel . . . . . 10  
    host name . . . . . 56  
    installation . . . . . 8  
    IP address . . . . . 44, 68  
    launching the user interface . . . . . 44  
    protecting against hacker attacks . . . . . 78  
    protecting with a password . . . . . 62  
    public IP address . . . . . 73  
    resetting the . . . . . 89  
    restoring the configuration . . . . . 87  
    setting up a . . . . . 12  
    setting up as a virtual server . . . . . 75  
    status information . . . . . 47, 90  
    temperature range for  
        operation . . . . . 12

## S

Safety precautions . . . . . 4  
Security log  
    clearing the . . . . . 91  
    saving the . . . . . 91

    updating the . . . . . 91  
Security measures . . . . . 7  
Serial number . . . . . 91  
Server . . . . . 106  
    virtual . . . . . 108  
Service Set Identifier see SSID  
Setting up a Network Client  
    (Windows 98) . . . . . 18  
Simple Mail Transfer Protocol see SMTP  
SMTP . . . . . 106  
Socket  
    for cable modem . . . . . 11  
    for DSL modem . . . . . 11  
    for power supply unit . . . . . 11  
    LAN . . . . . 11  
    WAN . . . . . 11  
Special Applications . . . . . 73  
Special applications  
    configuring . . . . . 76  
    games . . . . . 76  
SPI . . . . . 106  
SSID . . . . . 8, 70, 106  
    Factory setting on the router . . . . . 8  
    not visible . . . . . 71  
    preconfigured . . . . . 70  
    visible . . . . . 71  
Stateful Packet Inspection see SPI  
Static IP address . . . . . 64, 107  
Status of the router . . . . . 47, 90  
Subnet mask . . . . . 69, 107  
Subnetwork . . . . . 107  
Summer time selection . . . . . 61  
Supplied items . . . . . 9  
Switch . . . . . 107  
Synchronising the TCP/IP settings  
    with the router  
        Windows 2000 . . . . . 42  
        Windows 98 . . . . . 26  
        Windows XP . . . . . 34  
System configuration . . . . . 60  
System Requirements . . . . . 9

## T

TCP . . . . . 107  
TCP/IP . . . . . 107  
TCP/IP protocol . . . . . 17  
TCP/IP settings  
    Windows 2000 . . . . . 39  
    Windows 98 . . . . . 21

## Index

Windows XP . . . . . 30  
Temperature range for operation . . . . . 12  
Time . . . . . 90  
Time zone selection . . . . . 60  
Tools . . . . . 59, 87  
Trademarks . . . . . 4  
Transmission Control Protocol see TCP  
Transmission mode  
    full duplex . . . . . 15  
    half duplex . . . . . 15  
Transmission speed . . . . . 105  
    LAN socket . . . . . 15  
    on Ethernet LAN . . . . . 6  
    on wireless LAN . . . . . 6  
Trigger Port . . . . . 76  
Tunnel . . . . . 106  
Tunneling . . . . . 107

## U

UDP . . . . . 107  
UI elements . . . . . 47  
Universal Plug and Play see UPnP  
Universal Resource Locator see URL  
UPnP . . . . . 108  
    activating . . . . . 85  
URL . . . . . 108  
    filtering . . . . . 81  
User Datagram Protocol see UDP  
User interface  
    buttons . . . . . 48  
    dialog box . . . . . 48  
    launching the . . . . . 44  
    menu bar . . . . . 47  
    navigation bar . . . . . 47  
    selecting the language . . . . . 46  
    selection list . . . . . 48  
    working area . . . . . 48

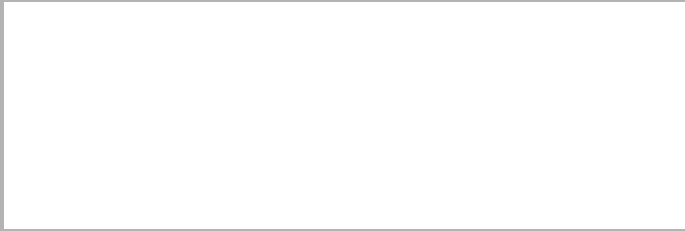
## V

Virtual Private Network see VPN  
Virtual server . . . . . 7, 73, 75, 108  
    setting up a . . . . . 75  
VPN . . . . . 6, 108

## W

WAN . . . . . 5, 108  
WAN connection  
    via cable modem . . . . . 56  
    via DSL modem . . . . . 54

    via PPPoE . . . . . 55  
    via PPTP . . . . . 57  
    with dynamic IP address . . . . . 56  
    with fixed IP address . . . . . 55  
WAN interface  
    configuring the . . . . . 49  
WAN socket . . . . . 11  
    Transmission speed . . . . . 6  
Web browser . . . . . 44  
WEP . . . . . 108  
WEP encryption . . . . . 72  
Wide Area Network see WAN  
Wired Equivalent Privacy see WEP  
Wireless cell . . . . . 108  
Wireless channel . . . . . 70  
    settings . . . . . 71  
Wireless LAN see WLAN  
Wireless network . . . . . 108  
Wireless settings . . . . . 50, 70  
WLAN . . . . . 108  
    Transmission speed . . . . . 6  
Working area . . . . . 48



Issued by  
Information and Communication mobile  
Haidenauplatz 1  
D-81667 Munich

© Siemens AG 2003  
All rights reserved.  
Subject to availability.  
Subject to change.  
06/2003

Siemens AG  
<http://www.my-siemens.com>

Order No.: A31008-E105-B100-2-7619