

SIEMENS

Gigaset WLAN Practical tips



CORDLESS HOME COMMUNICATION **Gigaset**

Contents

Introduction 3

Local networks with Gigaset products	4
Wired local network (Ethernet)	5
Wireless local network (WLAN)	6
Ad-hoc network	6
Infrastructure Network	7
Extending a wireless network using a repeater	9
Roaming	10
Possible uses	11

Releasing files and printers for shared use 13

Making your own files and printers available (Windows XP)	15
Configuring the network	15
Selecting computer names and workgroup	18
Checking the network settings	19
Completing the installation procedure	20
Releasing files and printers	21
Making your own files and printers available (Windows 2000)	24
Installing network services	24
Selecting computer names and workgroup	26
Setting the TCP/IP protocol	27
Setting up user names	29
Releasing files and printers	32
Making your own files and printers available (WIN 98 / 98 SE / ME)	37
Setting up a PC as Client for Microsoft Networks	37
Selecting computer names and workgroup	40
Selecting the access control	40
Setting the TCP/IP protocol	41
Installing utilities for file and printer release	44
Releasing files and printers	46

Using released files and printers 49

Using files and printers on the network (Windows XP)	50
Setting up a user account	50
Accessing released drives or folders from your PC	53
Accessing released printers from your PC	55
Using files and printers on the network (Windows 2000)	58
Setting up user names	58
Accessing released drives or folders from your PC	58
Accessing released printers from your PC	61
Using files and printers on the network (Win 98 / 98 SE / ME)	63
Setting up user names	63

Contents

- Accessing released drives or folders from your PC 66
- Accessing released printers from your PC 69
- Defining IP addresses 72**
 - Private IP addresses 72
 - Windows 98 73
 - Windows XP 77
 - Windows 2000 80
- Glossary 84**
- Index 95**

Introduction

This document provides a number of example applications for the use of Siemens Gigaset devices for local networks. It describes the most frequently used of the variety of options that these Siemens products offer you.

This chapter provides an overview of the various network configurations and possible applications. The following chapters provide more detailed descriptions of how to use these options.

Please note:

- ◆ The user interfaces depicted in this guide may differ from those on your screen because of the settings you have made. For Windows screens, the default state has been presented. There may also be minor differences due to different update cycles of user interface and this manual.
- ◆ In the examples we assume that the Gigaset network components have been installed and configured as per the corresponding operating instructions.
- ◆ This document is not part of the official package. It does not give rise to any legal rights.

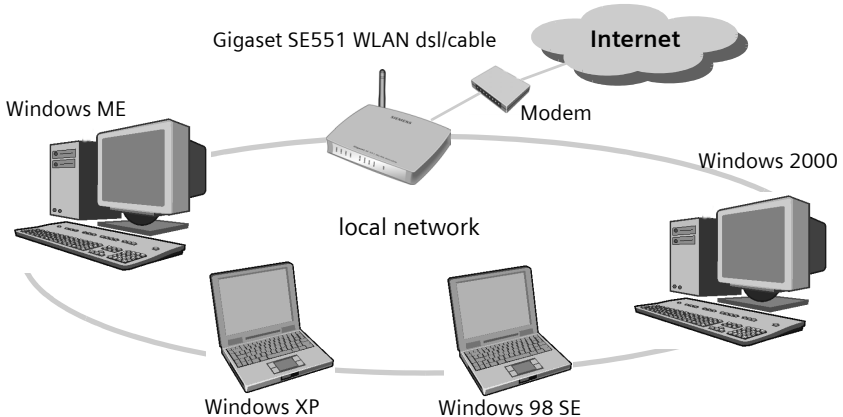
Trademarks

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

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

Local networks with Gigaset products

You can use Siemens Gigaset WLAN devices to set up a local network, e.g. a home network. All the PCs in this network can communicate with each other and have access to the Internet. The PCs can run on Windows 98, Windows ME, Windows 2000 or Windows XP. Gigaset Routers e.g. the Gigaset SE551/WLAN dsl/cable have an interface to enable Internet access, so that you can connect a DSL or cable modem for Internet access (WAN interface).

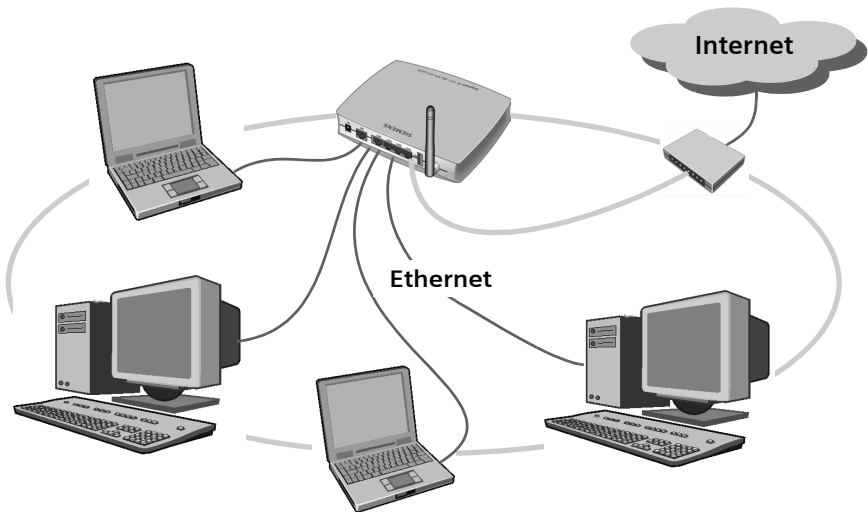


You can set up the network in a number of ways. You can

- ◆ Use a Gigaset SE551 WLAN dsl/cable to set up a wired local network (see page 5).
- ◆ Use the Gigaset SE551 WLAN dsl/cable to set up a local network comprising wireless and wired network components (see page 8).
- ◆ Use the wireless network adapters Gigaset PC Card 108, a Gigaset USB Adapter 108 or a Gigaset USB Stick 108 to set up a wireless network without routers, i.e. connect PCs directly with each other (see page 6), or connect PCs to a Gigaset SE551 WLAN dsl/cable (see page 7).
- ◆ Use one or more Gigaset WLAN Repeaters to extend the range of your wireless local network (see page 10).

Wired local network (Ethernet)

In a wired local network the PCs are linked via an Ethernet cable. The Siemens Gigaset SE551 WLAN dsl/cable has four Ethernet LAN ports for connecting four PCs. The PCs must have an Ethernet network adapter that is connected via an Ethernet cable to a LAN port on the router. New PCs frequently come supplied with such a socket. You can buy Ethernet cables (CAT-5) from specialist retailers.



The WAN interface on the Gigaset SE551 WLAN dsl/cable allows all PCs in the network to access the Internet simultaneously. To use this feature you will need the access data from an Internet Service Provider, e. g. T-Online.

Introduction

Wireless local network (WLAN)

In a wireless local network (WLAN), the PCs are linked to each other via a wireless connection. The PCs must be equipped with a wireless network adapter (e.g. the Gigaset PC Card 108 or Gigaset USB Adapter).

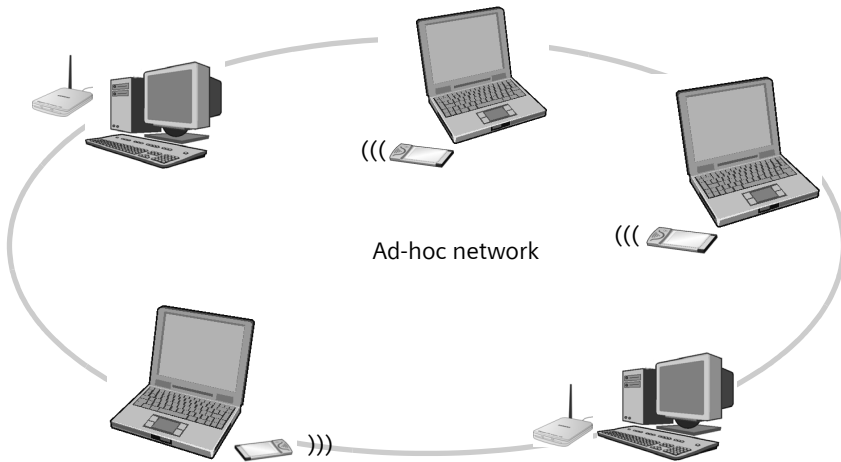
We generally differentiate between two types of wireless networks:

- ◆ ad-hoc mode
- ◆ infrastructure mode

Ad-hoc network

Ad-hoc networking is a new concept in network communications that is rapidly gaining in popularity. Ad-hoc networks do not have any fixed network infrastructure. The mobile network components that communicate with each other directly and without wire connections form the network "ad-hoc", i.e. as and when required. All the stations on the network have the same rights. Ad-hoc networks are used wherever communications networks have to be set up quickly and without any existing network infrastructure and where the participants are on the move.

An ad-hoc network is a wireless network set up without using a router.



Infrastructure Network

The infrastructure mode is used to connect wireless and wired networks with each other. In addition to the mobile stations, the infrastructure mode needs an access point, also known as a base station. In infrastructure mode, the stations on the network always communicate with each other via an access point. Unlike the ad-hoc mode, the access point sets up the wireless network on a permanent basis, and every station that wants to be part of the wireless network has to register with the access point before it is allowed to exchange data. Using an access point also extends the range of the wireless network.

The access point establishes the connection from the mobile stations of a wireless network to a wired LAN (Ethernet) or to the Internet. In this case, this is referred to the router functionality of the device. The access point sends data packets that are not addressed to stations in its network "outside" and passes data packets coming from "outside" to the appropriate station in its network.

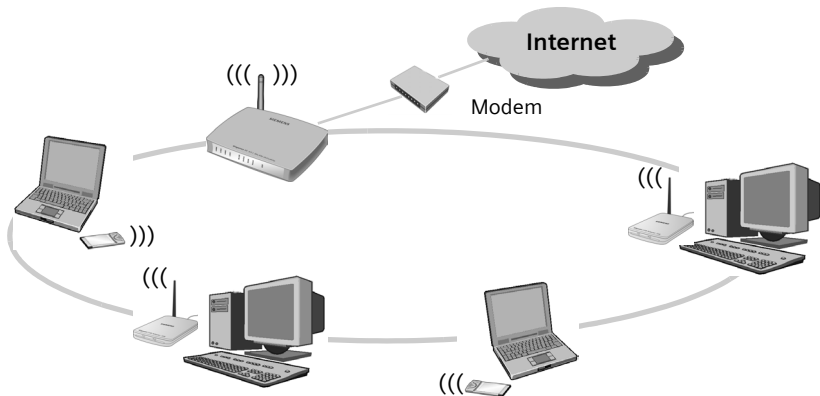
The Gigaset SE551 WLAN dsl/cable is such an access point. You can use it for connecting

- ◆ wireless linked PCs to the Internet and
- ◆ connect PCs with a wireless connection to a wired network.

Infrastructure mode is the standard configuration for the Gigaset SE551 WLAN dsl/cable. This configuration is described in the quick guide enclosed with the router.

Connecting wireless networks to the Internet

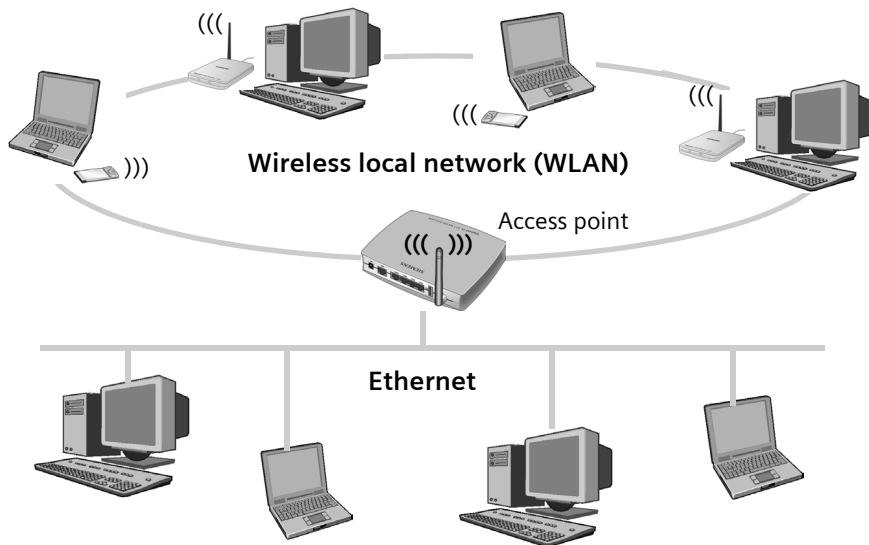
The Gigaset SE551 WLAN dsl/cable has a WAN interface that permits simultaneous access of all the stations to the Internet. To use this feature, you will need a DSL or cable connection from an Internet Service Provider. Please check whether your Internet Service Provider supports parallel access by several PCs.



Introduction

Linking a wireless network (WLAN) to a wired network (LAN)

A major advantage of wireless networks is their ability to work easily with existing wired networks. You can set up a wireless network to link mobile stations with an existing wired network. This requires all the stations in the wireless network to work in infrastructure mode.



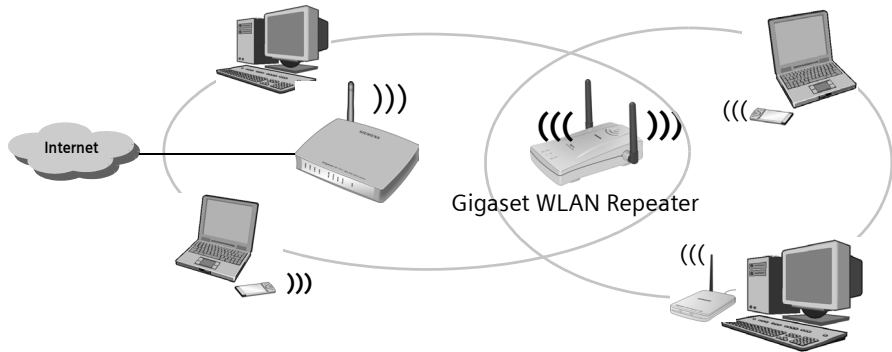
The Gigaset SE551 WLAN dsl/cable has four Ethernet interfaces (LAN ports). Up to four PCs can be connected directly to these LAN ports. These PCs also access the Internet via the Gigaset SE551 WLAN dsl/cable.

Please note:

You can also connect an Ethernet router to a LAN port, providing access to a larger wired network. If you want to connect the Gigaset network to an existing network, a variety of settings need to be taken into account. Therefore we cannot provide a general example for this use; the configuration depends greatly on the networks in question. We advise having configuration of such a network carried out by an expert.

Extending a wireless network using a repeater

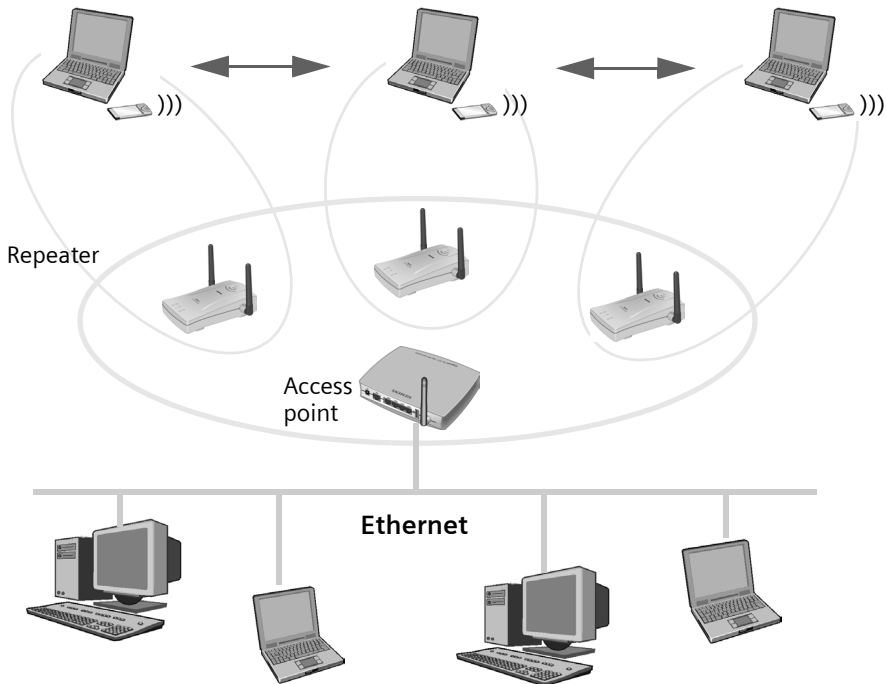
You can use a repeater, e.g. the Gigaset WLAN Repeater 108 to extend the coverage of your wireless network. To do this, set it up at the limit of the range of your wireless network. The Gigaset WLAN Repeater will now transmit data traffic into its own wireless area. This technology allows you to set up wireless networks that cover a much larger area than would be possible with the Gigaset SE551 WLAN dsl/cable alone.



PCs to be connected in a wireless local network via a Gigaset WLAN Repeater must be equipped with a wireless network adapter.

Roaming

In a wireless network with several repeaters, roaming allows the connected subscribers (PCs) to move freely between the different repeaters without breaking their contact with the access point. As soon as there is a risk of losing contact, the PC automatically searches for another repeater with a stronger signal. This allows you to set up wireless networks that cover a much larger area than would be possible with just a single access point (and a single additional repeater). Multiple repeaters also allow more subscribers to be served simultaneously. The main area of application for WLANs with roaming is on large company sites and in universities.



In a roaming network, all the users must use the same SSID and encryption. The access point must be connected to a wired network (Ethernet). For details, refer to the operating instructions on the CD supplied.

Possible uses

No matter which type of network you have opted for, Gigaset products for local networks offer a wealth of uses.

◆ Shared use of files

You can use your Gigaset SE551 WLAN dsl/cable or a PC in the network as a file server.

All central data are then

- stored in a bulk memory connected directly to the USB interface on your Gigaset SE551 WLAN dsl/cable
- or in the data system of a PC in the network.

Users on other PCs can hook up folders or entire drives on this file server to their own PCs and work with them as if they were actually on their local PC. Various access rights can be assigned.

How to connect a bulk memory to the Gigaset SE551 WLAN dsl/cable and use it in the network is described in the device's user guide.

How to release files on one PC for access to users on other PCs is described in Chapter "Releasing files and printers for shared use":

- for Windows XP from page 21
- for Windows 2000 from page 32
- for Windows 98, 98 SE, ME from page 46

How to make released files on other PCs available on your PC is described in Chapter "Using released files and printers":

- for Windows XP from page 53
- for Windows 2000 from page 58
- for Windows 98, 98 SE, ME from page 66

◆ Shared use of printers

Printers can be made available to PCs in the network in two ways:

- directly via the USB interface on your Gigaset SE551 WLAN dsl/cable
- via the PC on the network to which the printer is connected

All users can print their files at these printers.

Being directly connected to the Gigaset SE551 WLAN dsl/cable offers the advantage that the printer is always available without having to ensure that a specific PC is switched on. How to connect a printer to the Gigaset SE551 WLAN dsl/cable and use it in the network is described in the device's user guide.

How to release a printer on one PC is described in Chapter "Releasing files and printers for shared use":

- for Windows XP from page 23
- for Windows 2000 from page 36
- for Windows 98, 98 SE, ME from page 47

Introduction

How to make the printer connected to another PC available on your PC is described in Chapter ""Using released files and printers" on page 49":

- for Windows XP from page 55
- for Windows 2000 from page 61
- for Windows 98, 98 SE, ME from page 69

◆ **Controlled access to the Internet**

You want to prevent users accessing particular Internet services or children having access to any Internet pages at all. With the Gigaset Routers you can

- completely isolate PCs from the Internet.
- restrict access to Internet services,
- prevent access to particular web domains or Internet sites.

◆ **Protecting local networks from unauthorised access**

To protect your network from unauthorised access, you can for example

- set up access control for wireless users,
- set data encryption (only on wireless networks).

◆ **Running games, conferences and telephony via the Internet**

The Gigaset SE551 WLAN dsl/cable comes programmed with a comprehensive fire-wall functionality that protects your local network against unauthorized access from the Internet. Some applications however, such as games, video conferences, Internet telephony etc., require the possibility of external access from the Internet to local applications. The normal configuration of the router does not permit "external" access and supports only those Internet applications that do not need more than one connection (e.g. file transfer, email ...).

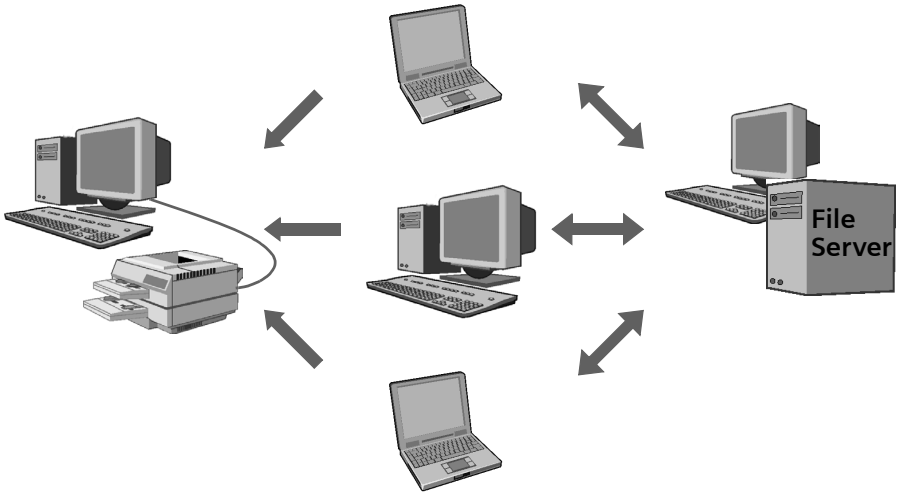
◆ **Making your own server available on the Internet**

Advanced Internet users might like to set up a Web server of their own so that they can have their own home page or other offerings on the Internet. This requires a particular configuration for the Gigaset SE551 WLAN dsl/cable.

You will find information regarding the configuration of the four above-named functions of your Gigaset SE551 WLAN dsl/cable in the device's user guide.

Releasing files and printers for shared use

A very common function of local networks is to allow the shared use of files and printers. Users can access from any PC on the network those files made available by another PC on that network, or they can print their files via a printer administered on another PC.



This chapter describes what steps you must carry out to release files and printers for network usage. It assumes that the network cards or wireless network adapters have already been installed in the PCs and that the PCs are either connected via a router or directly via an ad-hoc network.

The following steps are necessary before files and printers can be shared on the network:

- ◆ The network has to be set up on all the computers. The Internet protocol (TCP/IP) has to have been set as the connection method.
- ◆ All PCs have to have been assigned to the same network (workgroup).
- ◆ Users who want to make their files or printer available have to release them on their PC.
- ◆ After that, users who want to use other users' files or printers can make them available on their PC. This is described in Chapter "Using released files and printers" from page 49.

Releasing files and printers for shared use

Network configuration, release and use differ depending on the Windows operating system used.

Please note:

If you are using Windows 2000 on your network, you have to set up for all users who are to have access to resources on a Windows 2000 PC the appropriate user IDs on the Windows 2000 PC and their own PCs.

The following table provides an overview as to where you can find the relevant information.

	Windows XP	Windows 2000	Windows 98
Setting up the network	page 15	page 24	page 37
Releasing your files	page 21	page 32	page 46
Releasing your printers	page 23	page 36	page 47
Setting up user names	page 50	page 29	page 63
Using files on other PCs	page 53	page 58	page 66
Using printers on other PCs	page 55	page 61	page 69

Making your own files and printers available (Windows XP)

To release files or printers on a PC with Windows XP for other users on the network:

1. Configure the network (see below).
2. Select computer names and workgroup (see page 18).
3. Accept network settings (see page 19).
4. Close installation procedures (see page 20).
5. Release files and printer (see page 21).

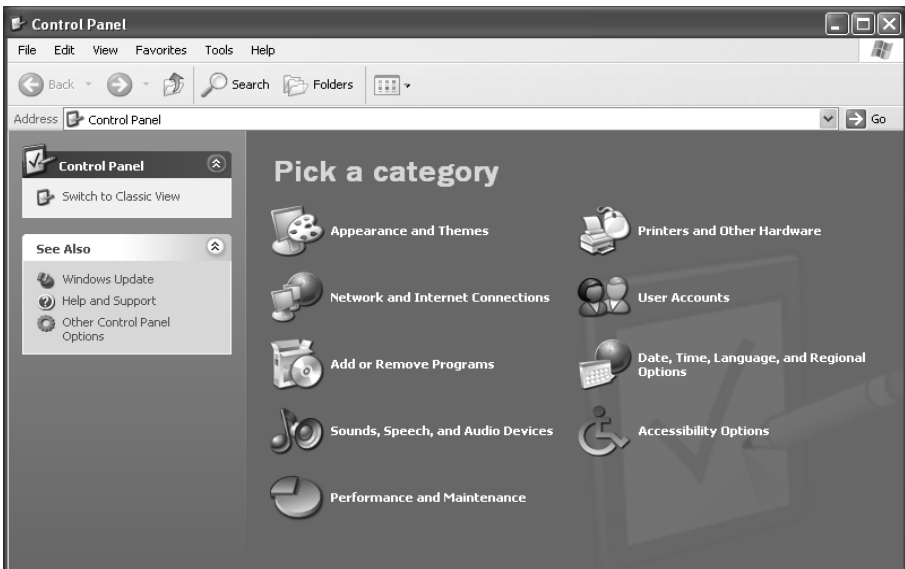
Configuring the network

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

Launching the network wizard

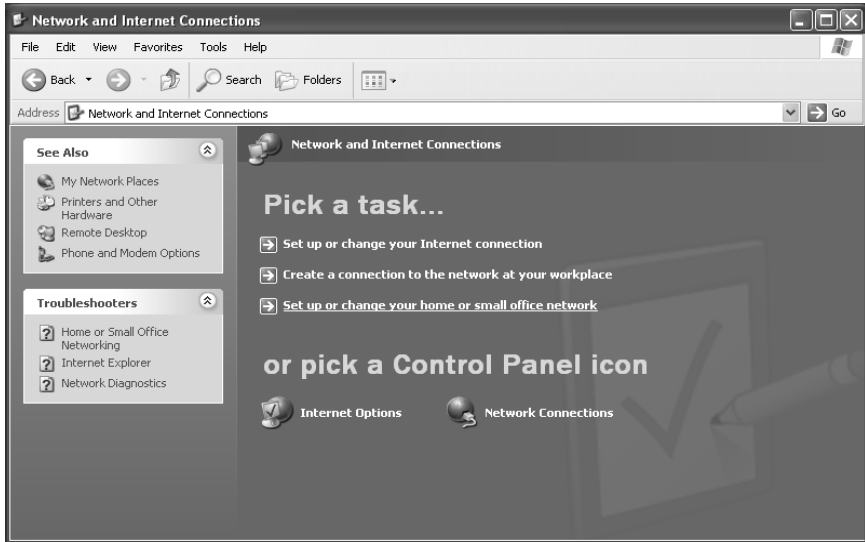
Launch the network wizard as follows:

➔ Open the **Control Panel** and then **Network and Internet Connections**.



Releasing files and printers for shared use

➔ Now select **Set up or change your home or small office network**.



This launches the network wizard.

➔ Skip the welcome screen and the checklist by clicking **Next** each time.

Selecting Internet connection as connection method

You will be prompted to select a connection method.

- ➔ Select **Other** 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 **Next**.
- ➔ In the next window select your network adapter and click **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 on the network. This name must be unique within the network. You can complete the **Computer description** box or leave it empty. Then click **Next**.
- ➔ Enter a name for the workgroup the PC is to belong to. This name must be identical for all the PC's in the network. Confirm this with **Next**.

Network Setup Wizard

Give this computer a description and name.

Computer description:
Examples: Family Room Computer or Monica's Computer

Computer name:
Examples: FAMILY or MONICA

The current computer name is HAMBURG.

Some Internet connections often true for...
If this is the case, click Next to skip this step.

Learn more...

Network Setup Wizard

Name your network.

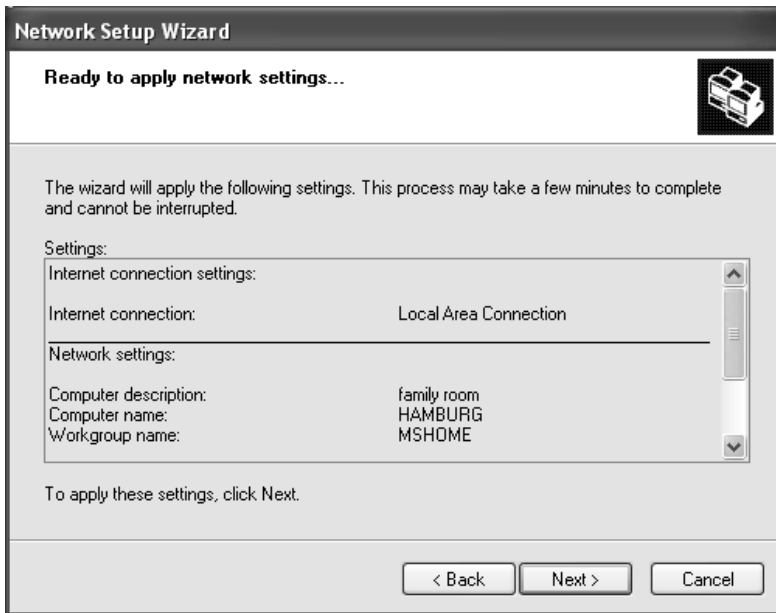
Name your network by specifying a workgroup name below. All computers on your network should have the same workgroup name.

Workgroup name:
Examples: HOME or OFFICE

< Back Next > Cancel

Checking the network settings

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



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

Completing the installation procedure

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 **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 restarting the PC, your local network is installed.

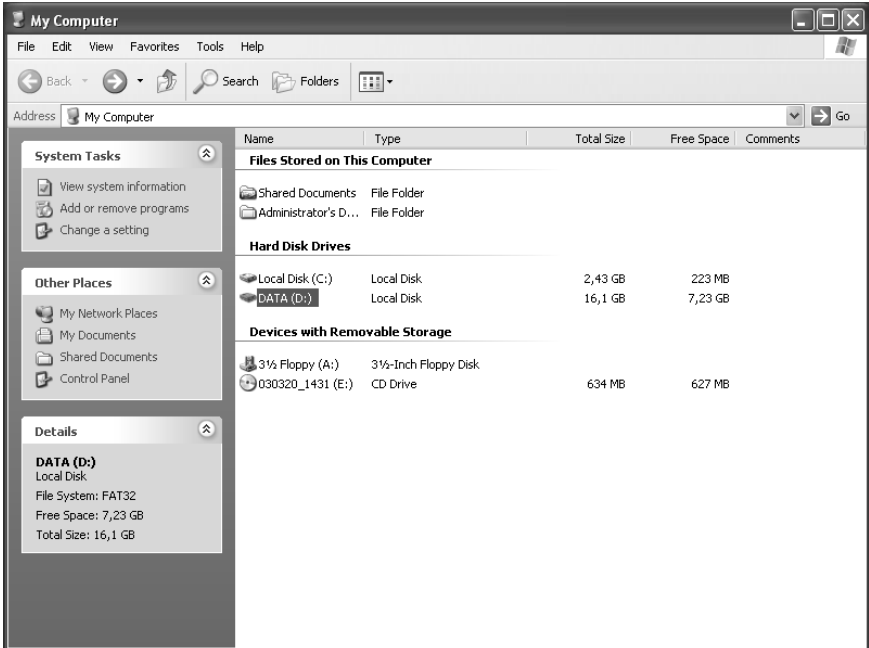
To set up the network on the other PCs with the same settings, insert the disk in the drive and run **Netsetup** with a double click.

Releasing files and printers

You can now release files and printers on your PC for other users on the network.

Releasing files

- ➔ Open the **Desktop** and left-click the folder or drive you want to release.
- ➔ Now select the entry **Release and security** with the right-hand mouse button from the pop-up menu.



- ➔ In the window that now opens, select in **Network release and security** the options:
 - **Release this folder on the network** and
 - **Network users can edit files.**



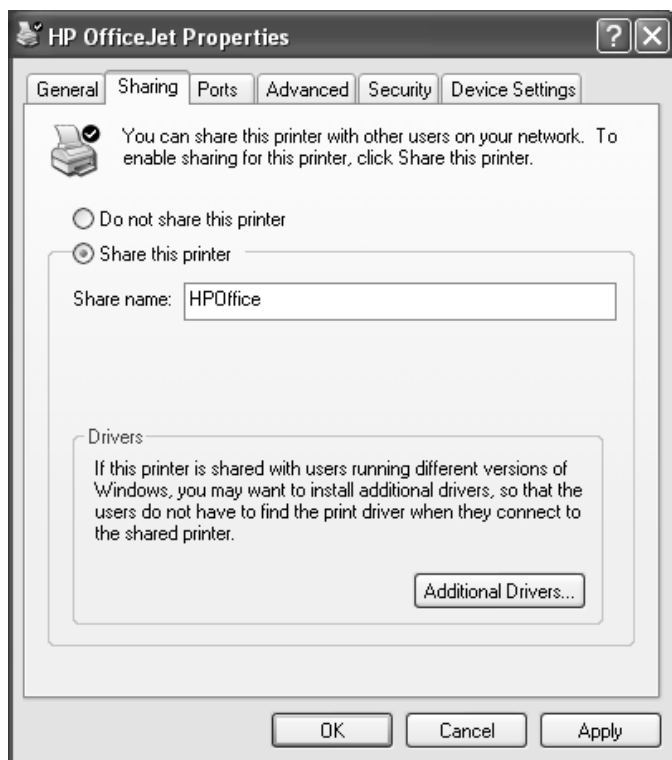
➔ Finally assign a **Share name**. From now on, your drive or folder will appear on the network under this name.

➔ Use **Apply** to save the current settings. Click **OK** to close release configuration.

If a hand now appears below your folder or drive on the Desktop then you have configured everything correctly.

Releasing printers

- ➔ To release printers select **Printers and Faxes** in the start menu.
- ➔ Left-click the printer you want to release.
- ➔ Now select the entry **Sharing** with the right-hand mouse button.
- ➔ The window for defining the printer properties will appear, and the **Sharing** tab is open.



- ➔ Select **Share this printer** and assign a **Share name**. From now on, your printer will be available to all the other users on the network under this name.
- ➔ Use **Apply** to save the current settings. Click **OK** to close release configuration.

Making your own files and printers available (Windows 2000)

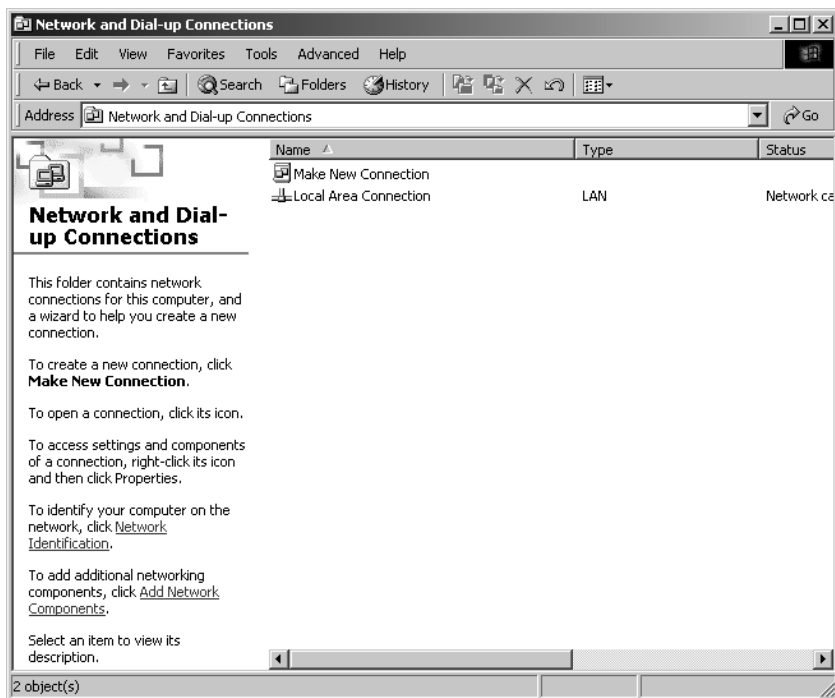
To release files or printers on a PC with Windows 2000 for other users on the network:

1. Install the network services (see below).
2. Select computer names and workgroup (see page 26).
3. Set TCP/IP protocol (see page 27).
4. Set up users (see page 29).
5. Release files and printer (see page 32).

Installing network services

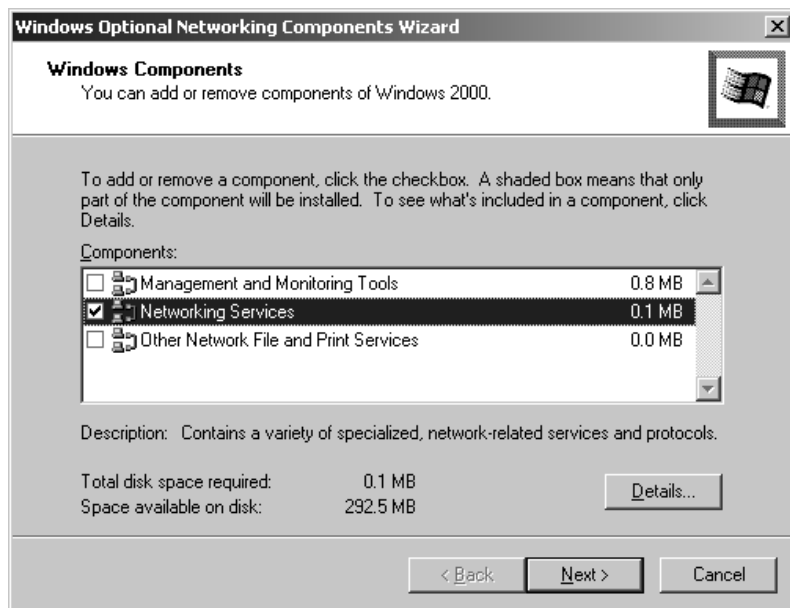
You have to install the network services before the PCs in your network can access shared resources. Have your Installation CD to hand. Then:

➔ Open the **Control Panel** and then open **Network and Dial-up Connections**.

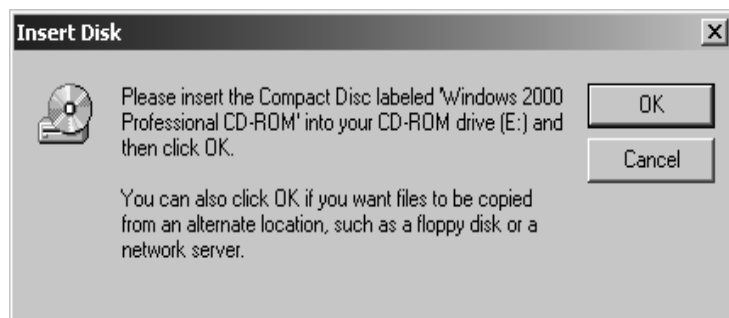


➔ Select in the left-hand pane the entry **Add network components**.

- ➔ Select **Networking services** and click **Next**



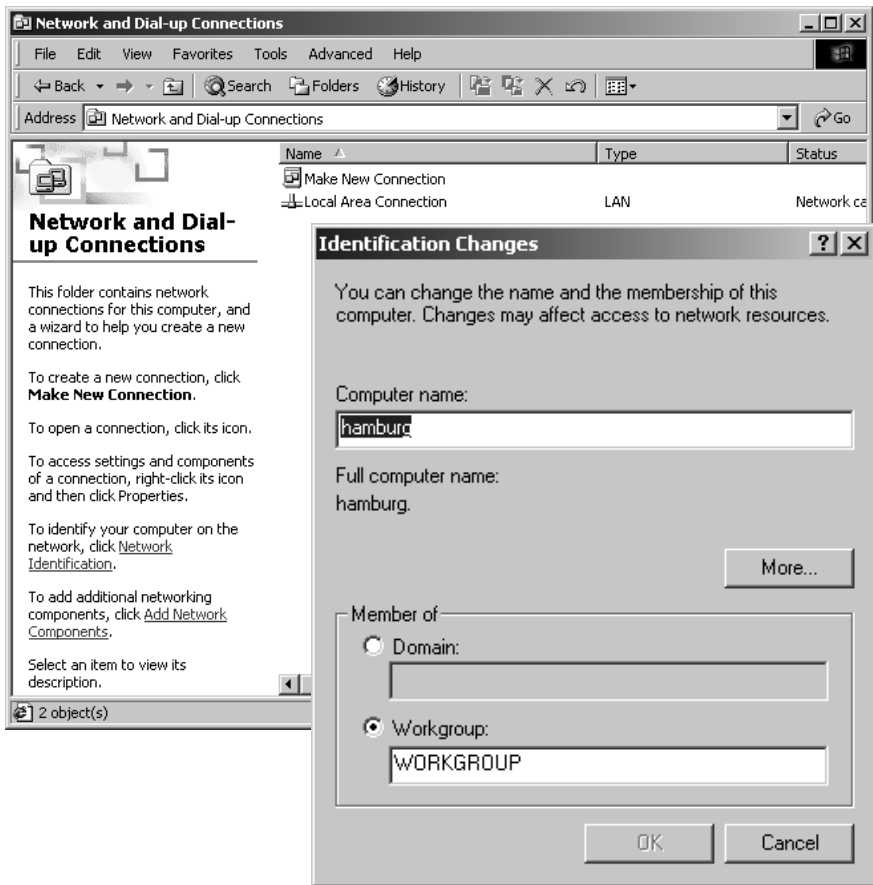
- ➔ Insert the WIN2000 CD and click the **OK** button to install all the required components.



Selecting computer names and workgroup

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

➔ Click **Network identification** and then **Properties**

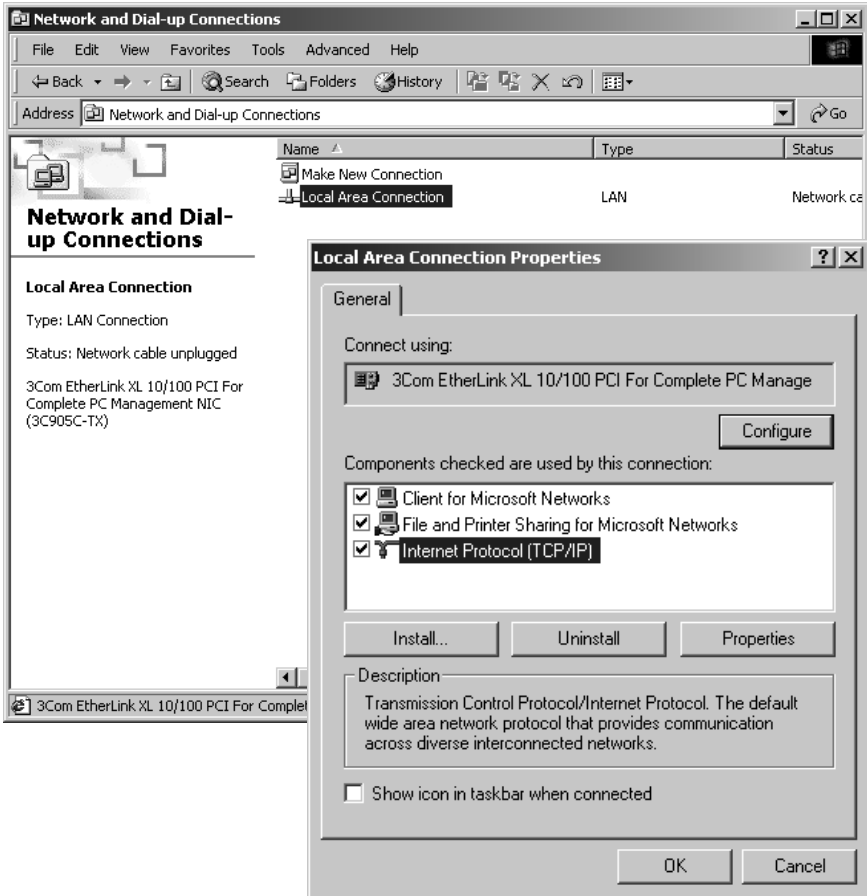


- ➔ In the **Computer name** box, enter the name the PC is to appear under on the network. This name must be unique within the network.
- ➔ In the **Workgroup** box, enter a name for the workgroup. This name must be the same for all the PCs on the network.
- ➔ Confirm this with **OK**.

Setting the TCP/IP protocol

The TCP/IP protocol ensures that the PCs on the network can communicate with each other. This protocol requires certain settings which you will now make so that it can function smoothly.

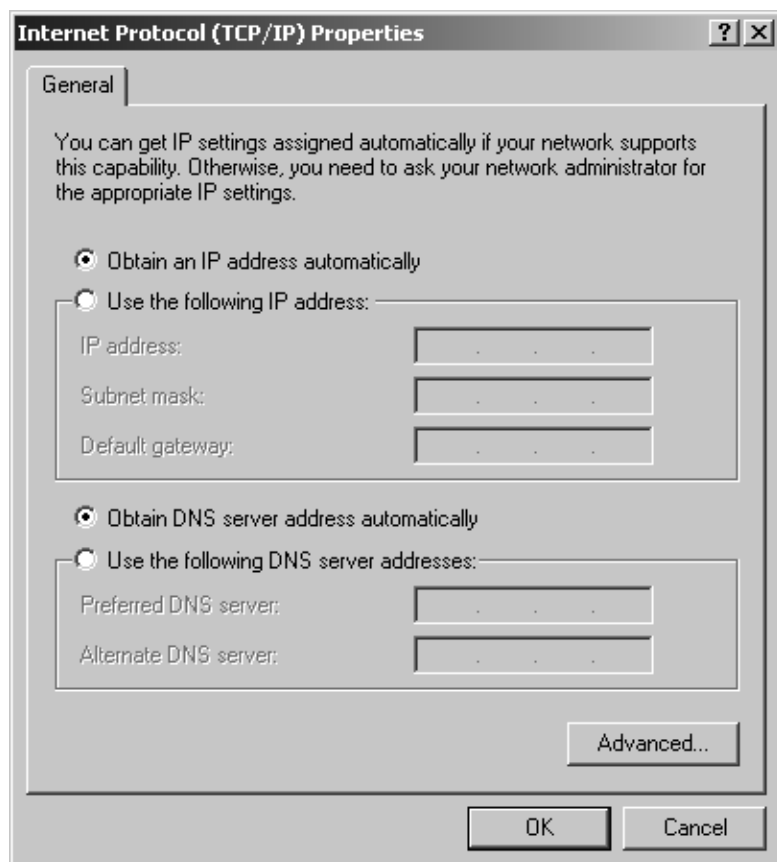
➔ Right click to open **Local Area Connection**. In the next window click **Properties**.



➔ In the lower section of the window, select the option **Display icon in taskbar when connected**.

➔ Left-click to select **Internet Protocol (TCP/IP)** and click **Properties**.

- ➔ Select the entries *Obtain an IP address automatically* and *Obtain DNS server address automatically*.



- ➔ Close this and the next window with **OK**.

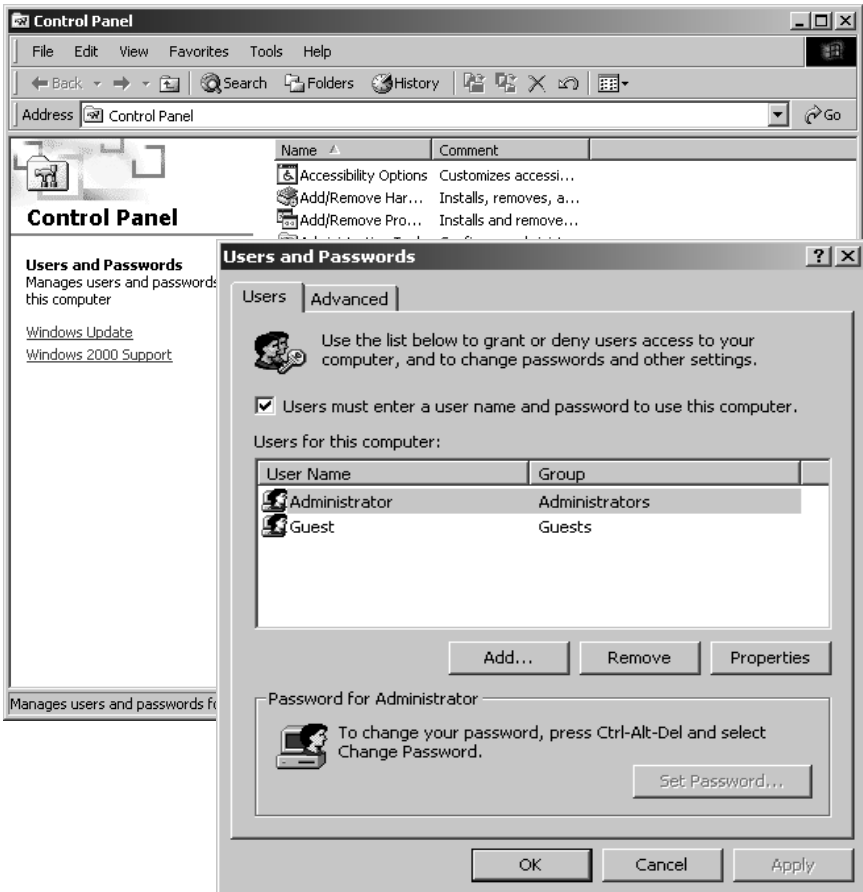
Note:

You can of course define IP addresses manually. This is necessary for example in ad-hoc networks. How to assign static IP addresses is described on page 72 onwards.

Setting up user names

All the users who want to access resources released on your PC have to be given a user entry. You should set up these users now so that you can assign access rights for them.

➔ Open the **Control Panel** and then open **Users and passwords**.



➔ Select **Users must enter a user name and password for this computer**.

➔ Click **Add**.

Releasing files and printers for shared use

- ➔ Enter a user name of your choice. This must be unique on the network. The boxes **Full name** and **Description** can be left blank.
- ➔ Confirm this with **Next**.



The screenshot shows the 'Add New User' dialog box with the title bar 'Add New User' and a close button. On the left is a dark area with a white icon of a computer monitor. The main area contains the text 'Enter the basic information for the new user.' followed by three input fields: 'User name:' with 'Anny', 'Full name:' with 'Anny Gray', and 'Description:' which is empty. Below these fields is the text 'To continue, click Next.' At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

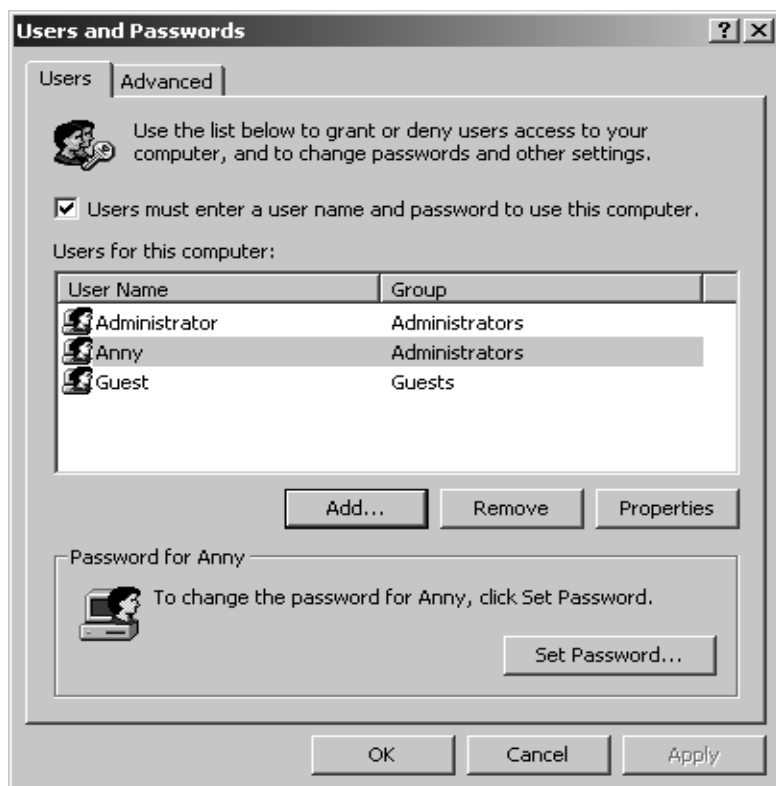
- ➔ Now assign a password and confirm it by entering it again. Confirm this with **Next**.
- ➔ In the next window you can define the type of access. Select **Other**, choose **Administrators** from the selection list and click **Finish**.



The screenshot shows the 'Add New User' dialog box with the title bar 'Add New User' and a close button. On the left is a dark area with a white icon of a computer monitor. The main area contains the text 'What level of access do you want to grant this user?' followed by three radio button options: 'Standard user (Power Users Group)' with a description, 'Restricted user (Users Group)' with a description, and 'Other: Administrators' with a dropdown menu showing 'Administrators' and a description. At the bottom are three buttons: '< Back', 'Finish', and 'Cancel'.

- ➔ Save the settings with **Apply** and close user administration with **OK**.

- ➔ If you ever want to change your password, open this window again, select the user name in question and click **Set Password**.

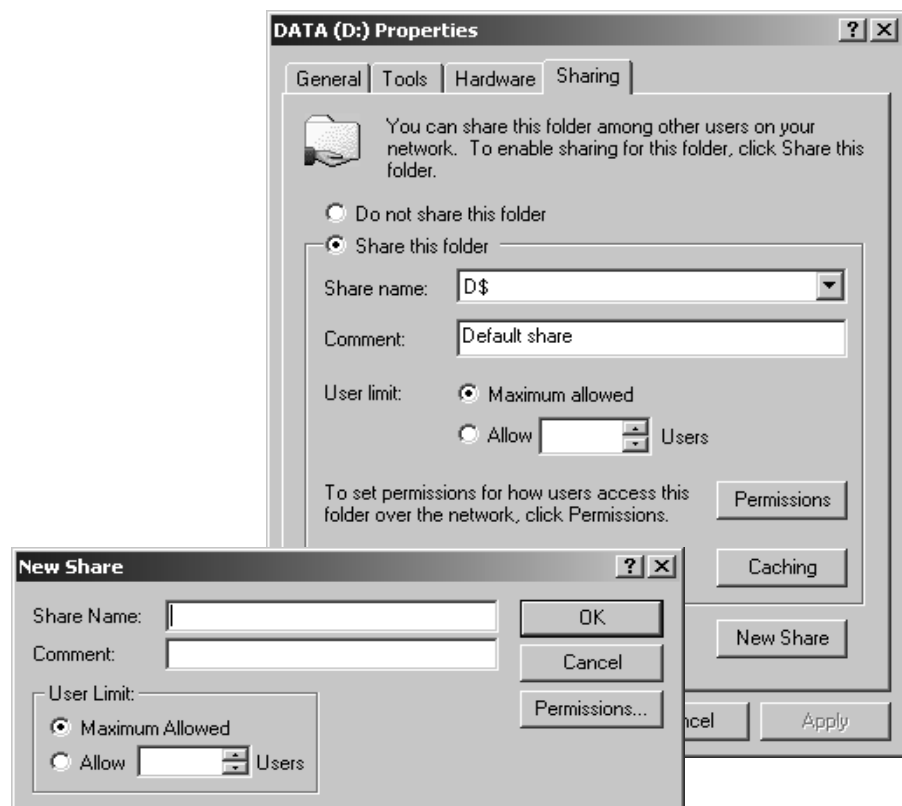


Releasing files and printers

You can now release files and printers on your PC for other users on the network.

Releasing files

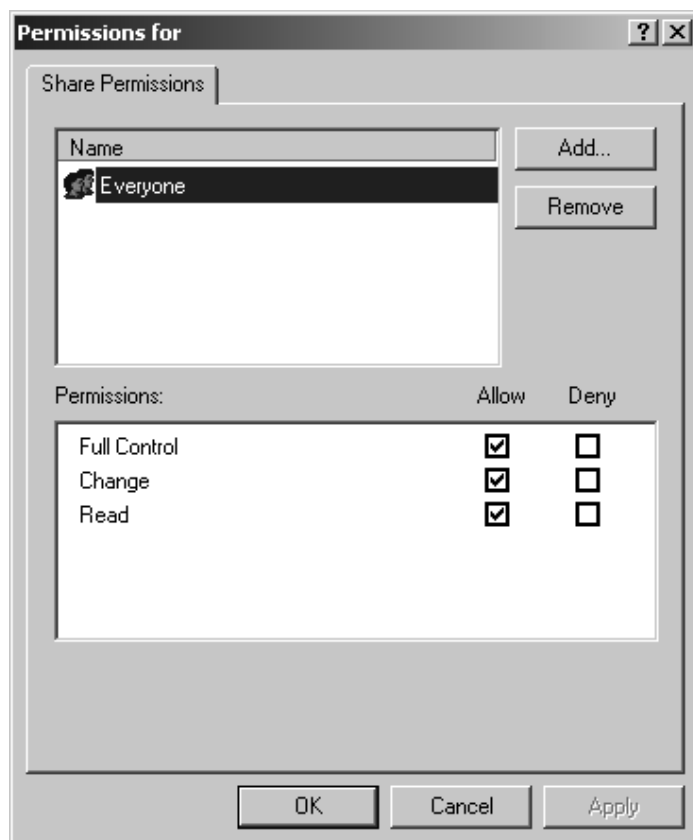
- ➔ Open the **Desktop** and right click the folder or drive you want to release.
- ➔ Now select the entry **Share** with the left-hand mouse button from the pop-up menu.



- ➔ Select **Share this folder** and click **New share**.
- ➔ Assign a share name and, if you want, a comment of your choice. From now on, your drive or folder will appear on the network under this name.
- ➔ Now click **Permissions**.

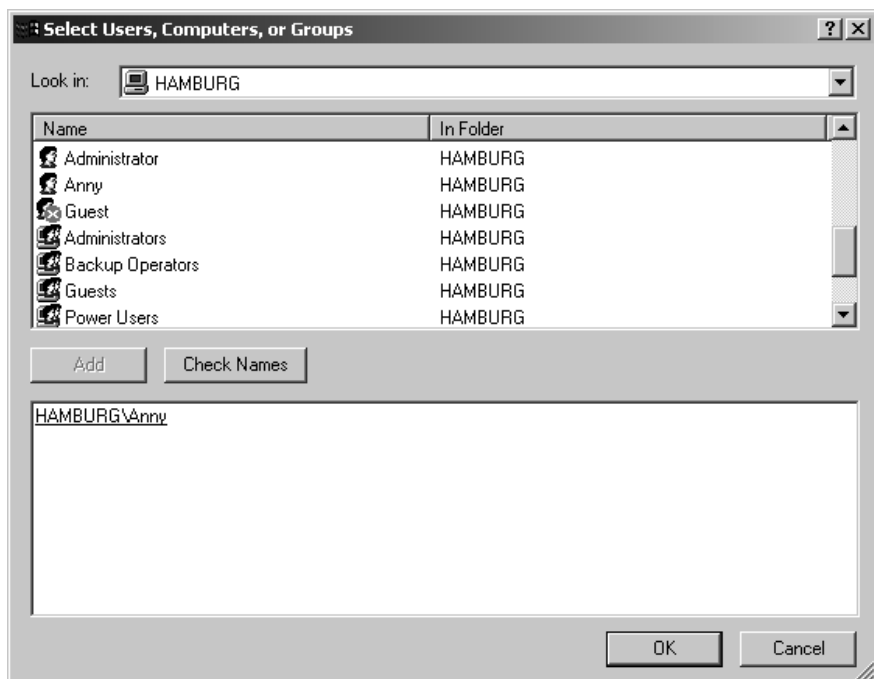
Now you can assign user rights to the registered users.

➔ Click **Add**.



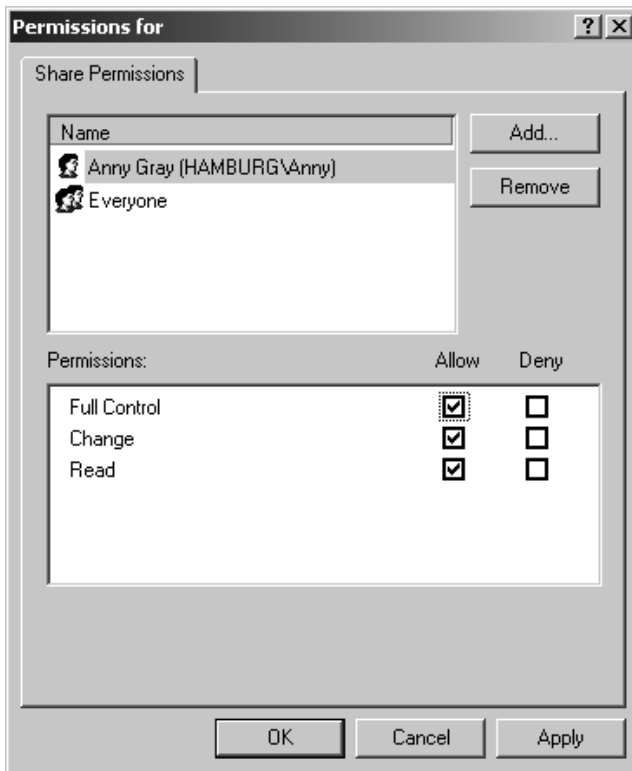
Releasing files and printers for shared use

➔ Select the users you created earlier and click **Add**.



In the next window you can define who should have which access rights to your PC. Normally the read only right is chosen.

- ➔ Select a user in the upper pane, and then in the lower pane the rights you want to assign.



- ➔ To save the settings you have made, click **Apply** and **OK**. Close the next window as well with **OK**. Close the properties window with **OK**.

Releasing files and printers for shared use

Releasing printers

- ➔ To release printers select **Printers and Faxes** in the start menu.
- ➔ Right-click the printer you want to release.
- ➔ Now select the entry **Sharing with the left-hand mouse button**.



- ➔ Select **Shared as** and assign a share name. From now on, your printer will be available to all the other users on the network under this name.
- ➔ If this printer is to be accessed by users with PCs that have a different operating system, you will have to install additional drivers. To do this click **Additional drivers...** and follow the instructions.
- ➔ Use **Apply** to save the current settings. Click **OK** to close share configuration.

Making your own files and printers available (WIN 98 / 98 SE / ME)

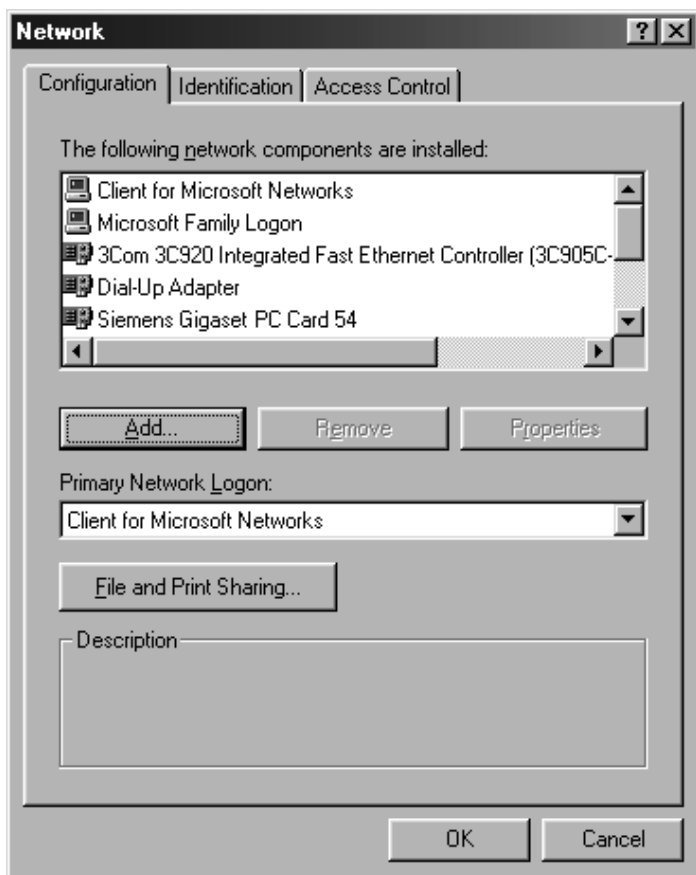
To release files or printers on a PC with Windows 98 for other users on the network:

1. Set up PC as Client for Microsoft Networks (see page 37).
2. Select computer names and workgroup (see page 40).
3. Select type of access control (see page 40).
4. Set TCP/IP protocol (see page 41).
5. Install utilities for file and printer release (see page 44).
6. Release files and printer (see page 46).

Setting up a PC as Client for Microsoft Networks

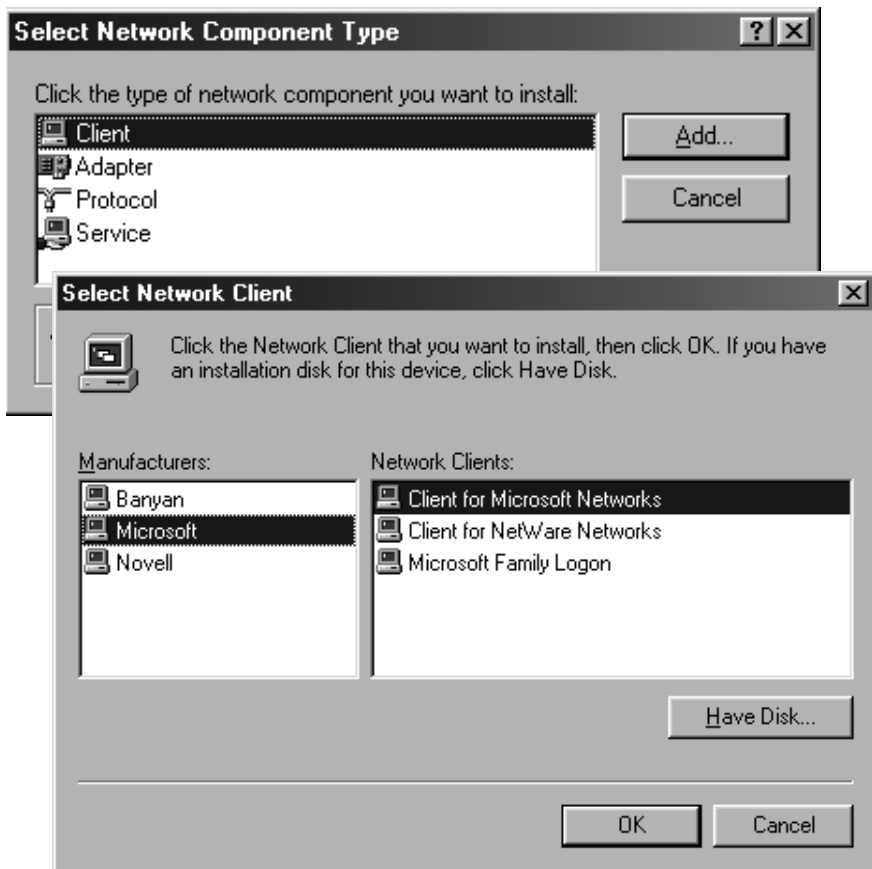
Before the PCs in your network can access shared resources, you have to define a Microsoft Network, i.e. all the PCs have to be configured as Clients of a Microsoft Network. This can be done as follows:

- ➔ Open the **Control Panel** and then open **Network**.
- ➔ Check whether the list of components contains the entry **Client for Microsoft Networks**.



If the entry exists, please continue from page 40.

- ➔ If the entry does not exist, click **Add**.



- ➔ Select as network component type **Client** and click **Add**.
- ➔ Select in **Manufacturers** the entry **Microsoft** and in **Network clients** the entry **Client for Microsoft Networks** before confirming 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 **Configuration** to the **Identification** tab.
- ➔ In the **Computer name** box, enter the name the PC is to appear under on 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 on the network.
- ➔ The **Description** box can be left empty.

Selecting the access control

Now you can define which access rights are to be assigned to resources you want to release.

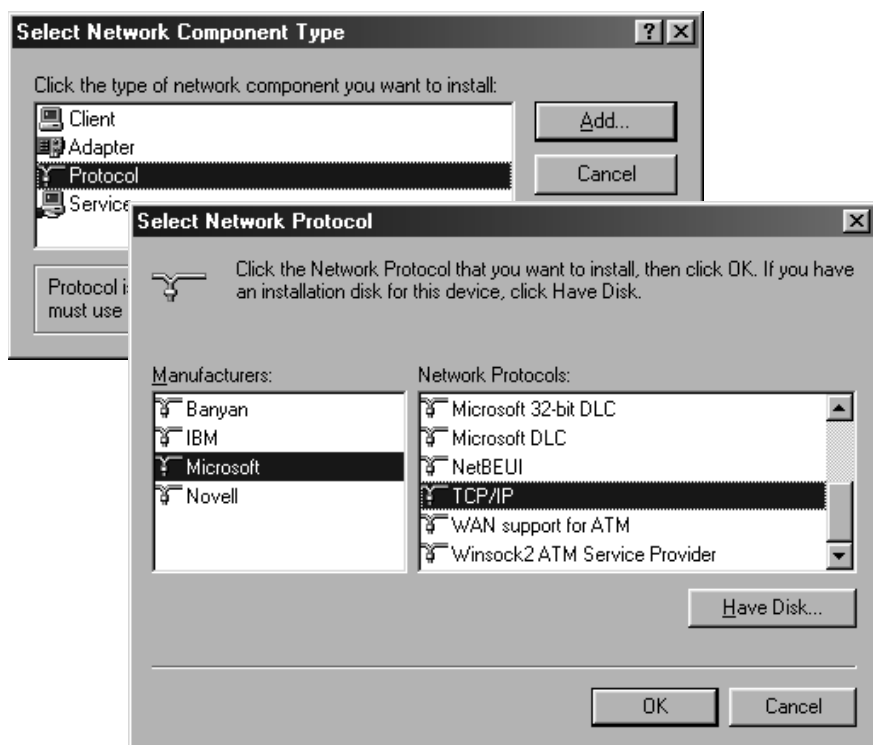
- ➔ In the **Network** window move from **Identification** to the **Access control** tab.
 - Use the option **Access control at release level** to define that access to released files or printer is to be password protected.
 - The option **Access control at user level** defines that access is permitted only for certain users or groups.

Setting the TCP/IP protocol

The TCP/IP protocol ensures that the PCs on the network can communicate with each other. This protocol requires certain settings which you will now make so that it can function smoothly.

Checking the TCP/IP entry

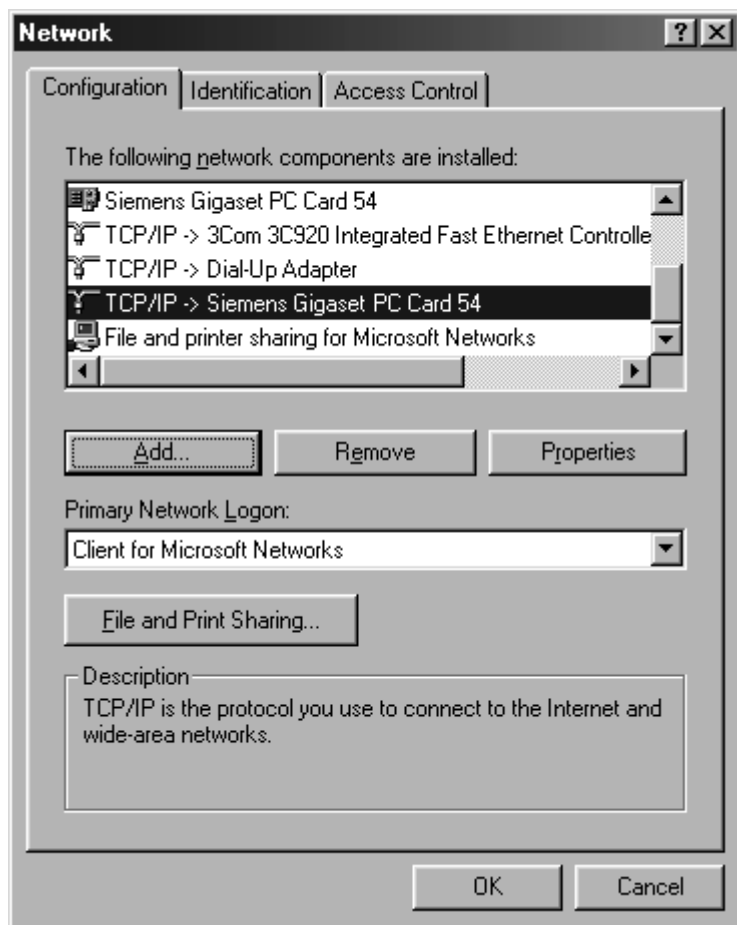
- ➔ In the **Network** window, check that there is a **TCP/IP >** entry for your network card or network adapter in the list of components. To do this, in the **Network** window, switch to the **Configuration** tab. If for example you are using a Gigaset PC Card 108 as the wireless network adapter, the list must contain the entry **TCP/IP > Siemens Gigaset PC Card 108**.
- ➔ If the entry for your network card or network adapter is there, please turn to page 41.
- ➔ If the entry does not exist, click **Add**.



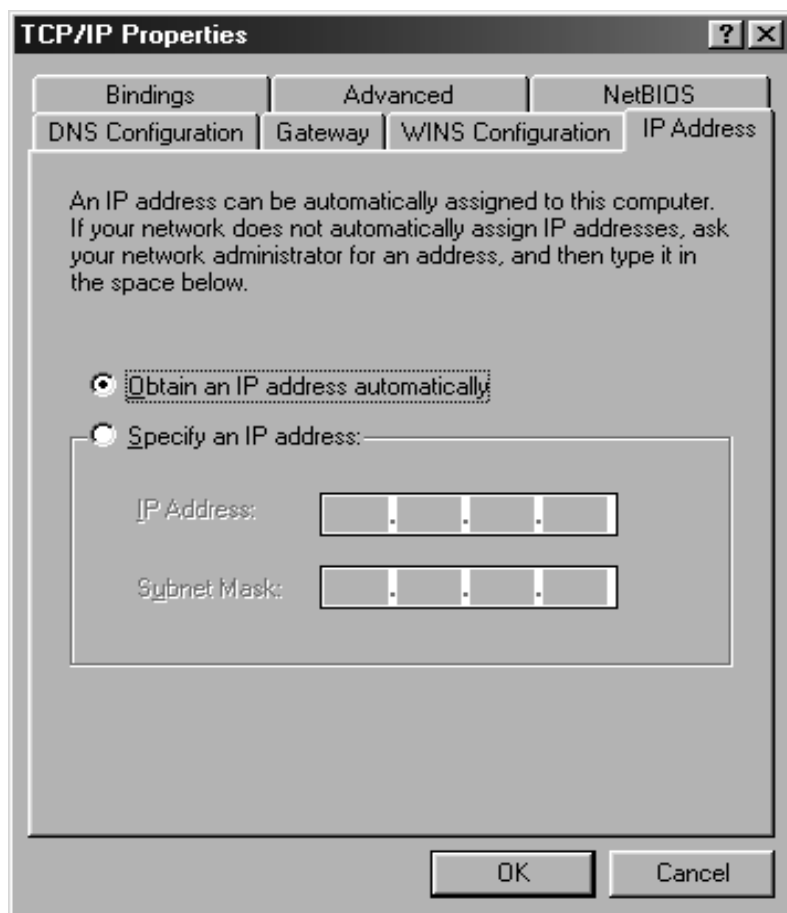
- ➔ Select as network component type **Protocol** and click **Add**.
- ➔ Select in **Manufacturers** the entry **Microsoft** and in **Network protocol** the entry **TCP/IP** before confirming with **OK**.
- ➔ Set TCP/IP protocol.

Releasing files and printers for shared use

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



- ➔ Open the *IP address* tab, select the entry *Obtain an IP address automatically* and finish with *OK*.

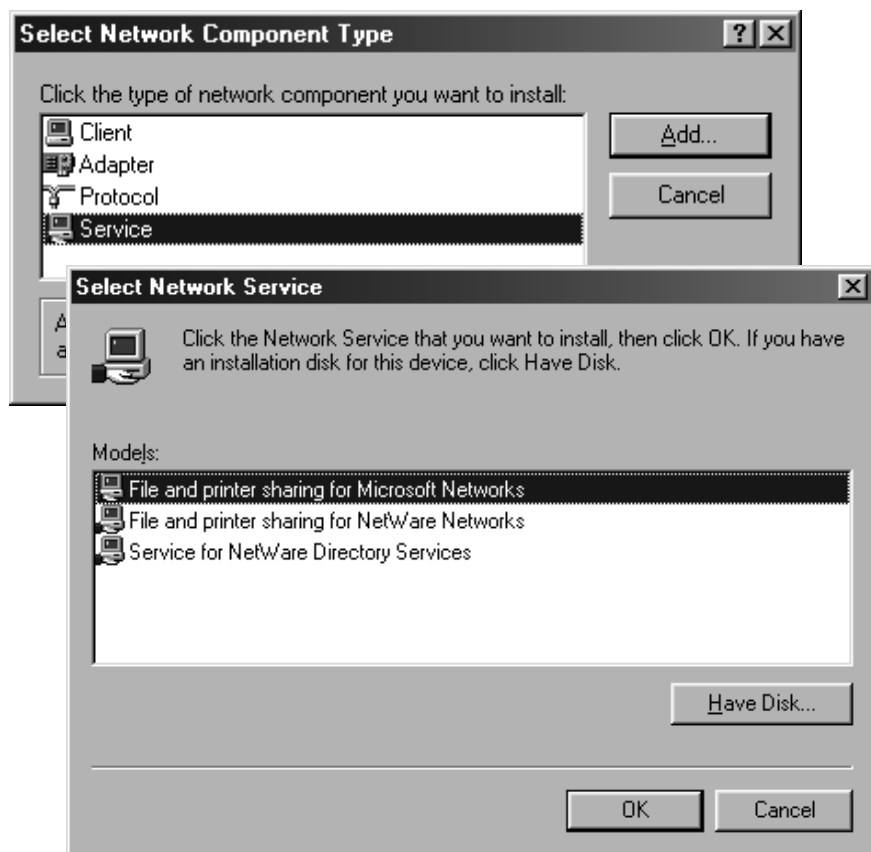
**Note:**

You can of course define IP addresses manually. This is necessary for example in ad-hoc networks. How to assign static IP addresses is described on page 72 onwards.

Installing utilities for file and printer release

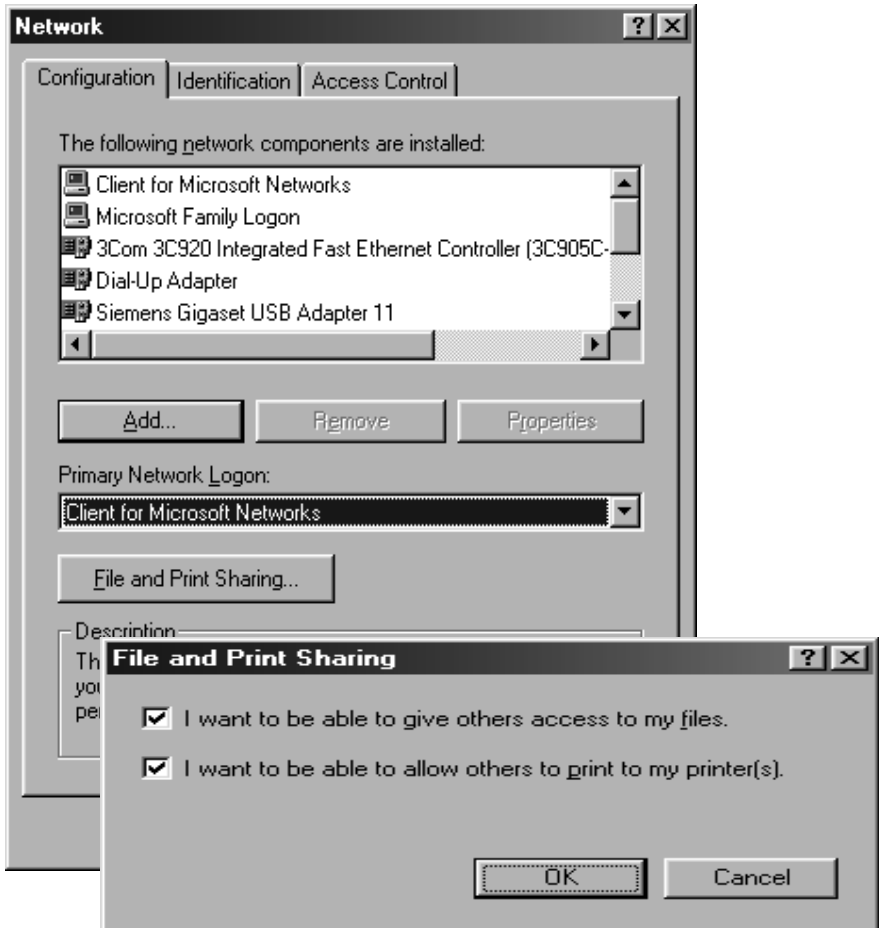
You cannot release files and printers on your PC for other users on the network if the utility for file and printer release has not been installed.

- ➔ First of all you have to check in the **Network** window whether the list of components has the entry **File and printer sharing for Microsoft Networks**.
- ➔ If the entry exists, please continue from page 45.
- ➔ If the entry does not exist, click **Add**.



- ➔ From the list select the entry **Service** and click **Add**.
- ➔ Select **File and printer sharing for Microsoft Networks** and click **OK**.

- ➔ Now select in the **Primary network logon** box the entry **Client for Microsoft Networks** and then click **File and print sharing**.



- ➔ In the **File and print sharing** window you can choose whether to release files or printers or both for other users.
- ➔ Close all the windows with **OK**.

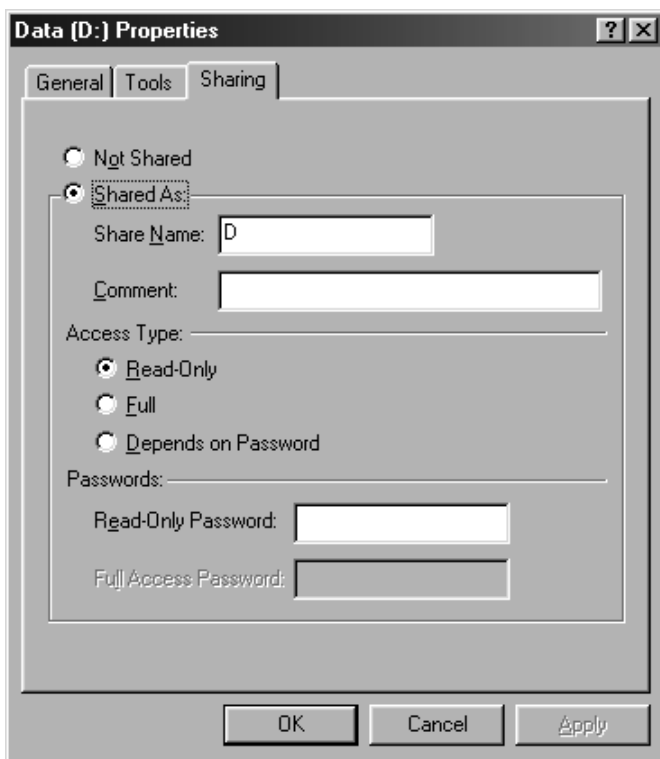
You will now need the Windows installation CD. Windows will copy some files from the installation CD before prompting you to reboot your computer. Then the network is ready for use.

Releasing files and printers

You can now release drives, folders or printers on your PC for other users on the network.

Releasing files

- ➔ Open the **Desktop** and select with the left mouse button what you want to release.
 - Select a drive or
 - Open a drive and select a folder.
- ➔ Now select **Share** with the right-hand mouse button from the pop-up menu. The following window will appear.



- ➔ Now select the **Shared as** box and enter a share name and, if you want, a comment of your choice. From now on, your drive or folder will appear on the network under this name.

- ➔ Select one of the following access types:

Read only: If you want to allow other users to open and read documents but not edit or delete them.

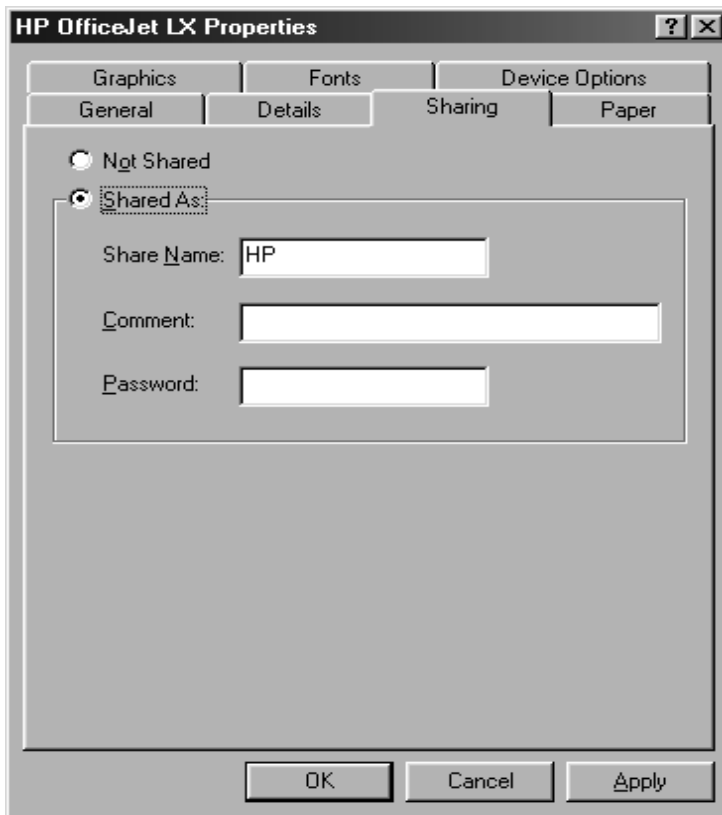
Full: If you want to allow other users to edit, add or delete files.

Depends on password: If you want to grant various users different access rights.

- ➔ Click **Apply** to save your settings and finish with **OK**.

Releasing printers

- ➔ Open the printer manager with **Start – Settings – Printers**.
- ➔ Left-click the printer you want to release.
- ➔ Now select **Share** with the right-hand mouse button from the pop-up menu. The following window will appear.



Releasing files and printers for shared use

- ➔ Now select the ***Shared as*** box and enter a share name and, if you want, a comment of your choice. From now on, your printer will be available to all the other users on the network under this name.
- ➔ Click ***Apply*** to save your settings and finish with ***OK***.

Using released files and printers

This chapter describes the steps for using files or printers that are shared on the network on your system. It assumes that the network cards or wireless network adapters are installed in your PC and that the PCs are either connected via a router or directly via an ad-hoc network.

Network configuration, release and use differ depending on the Windows operating system used.

The following table provides an overview of where you can find the relevant information in this chapter.

	Windows XP	Windows 2000	Windows 98
Setting up user names	page 50	page 58	page 63
Using files on other PCs	page 53	page 58	page 66
Using printers on other PCs	page 55	page 61	page 69

Using files and printers on the network (Windows XP)

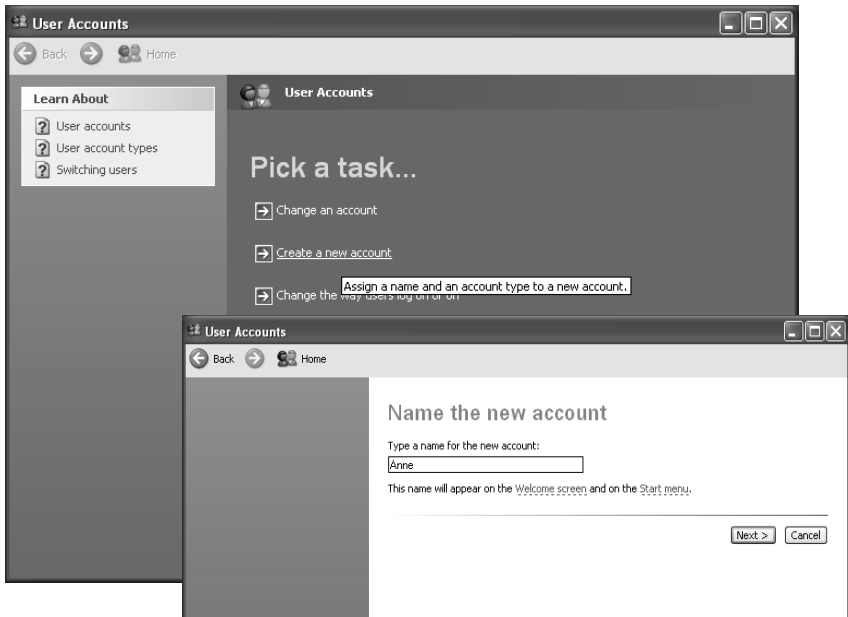
You can use resources on your PC such as files and printers that have been made available by other PCs.

If the resource you want to use on your PC is on a Windows 2000 system then you have to set up user accounts for all the users who are to have access. The same user IDs have to be entered as on the releasing system.

Setting up a user account

To set up a user account:

➔ Open the **Control Panel** and then **User accounts**.

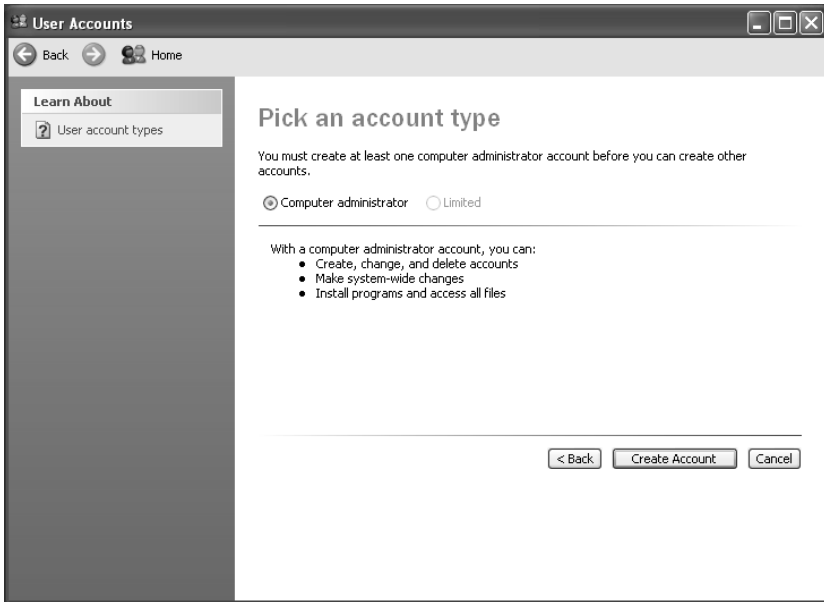


➔ Select **Create new account**.

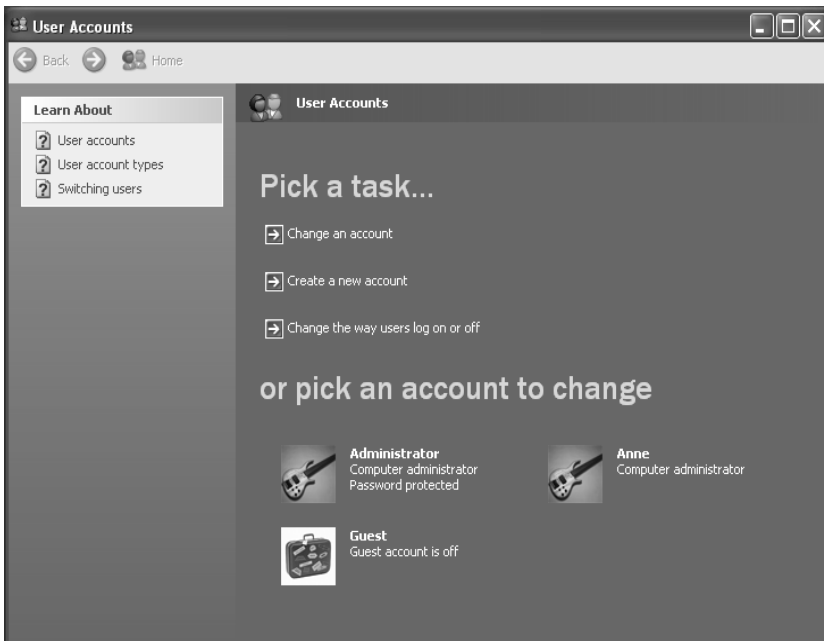
➔ Enter a name for the user.

➔ Click **Next**.

- ➔ Select **Limited** as account type. Then the newly created user will not have any administrator rights on your PC.

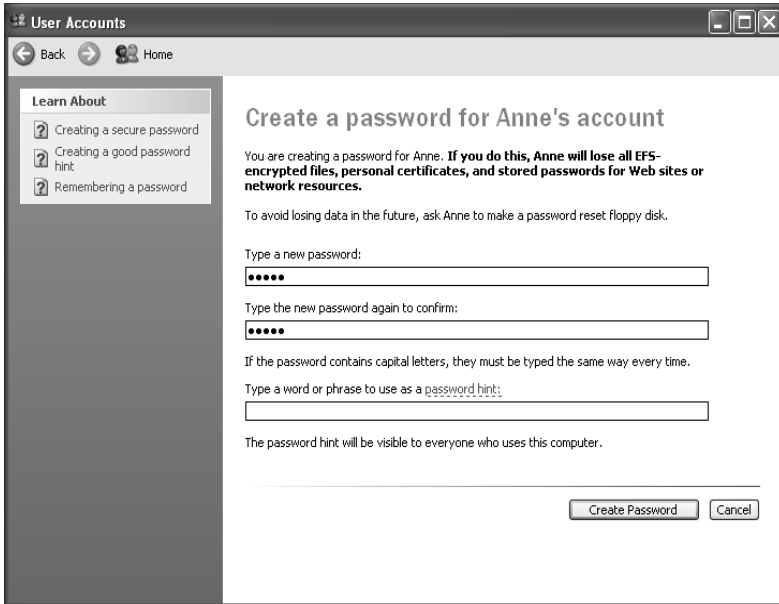


- ➔ Click **Create account**. You will now see the new user account.



Using released files and printers

- ➔ You should now assign a password. To do this click the new user account.
- ➔ Select **Create Password**.



The screenshot shows the 'User Accounts' window in Windows XP. The title bar reads 'User Accounts'. Below the title bar are navigation buttons: 'Back', 'Home', and a user icon. On the left is a 'Learn About' sidebar with three links: 'Creating a secure password', 'Creating a good password hint', and 'Remembering a password'. The main content area is titled 'Create a password for Anne's account'. It contains the following text: 'You are creating a password for Anne. If you do this, Anne will lose all EF5-encrypted files, personal certificates, and stored passwords for Web sites or network resources.' Below this is a warning: 'To avoid losing data in the future, ask Anne to make a password reset floppy disk.' There are three input fields: 'Type a new password:' (with a masked password '*****'), 'Type the new password again to confirm:' (with a masked password '*****'), and 'Type a word or phrase to use as a password hint:' (with an empty field). A note states: 'If the password contains capital letters, they must be typed the same way every time.' At the bottom right are two buttons: 'Create Password' and 'Cancel'.

- ➔ Enter a password and then enter it again as confirmation.
- ➔ Click **Create Password**.

Accessing released drives or folders from your PC

You can access drives and folders released on other PCs in two different ways:

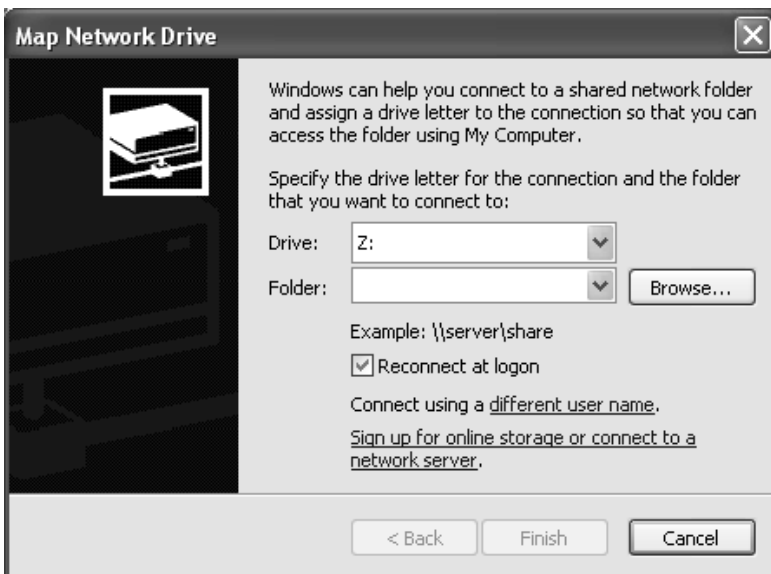
- ◆ via the My NetworkPlaces of your PC (see page 66).
You should choose this alternative if for example you want to copy files or folders from another PC to your own or vice versa.
- ◆ by hooking on to your PC's file system (see page 53).
You should choose this alternative if you want to work directly with the files or folders of the other PC. In this case, hook on an entire released drive or folder in your PC's file system and work with the files as if they were files on your PC.

Please note:

Drives or folders can be simultaneously hooked onto several PCs. It is therefore possible for other users to access the data. Most applications (e. g. word processing software) lock files once they have been opened. This prevents inconsistent data pools. If you cannot open a file because it is locked, you will normally see a message to that effect.

To hook up network drives:

- ➔ Open the **Desktop**.
- ➔ In the **Extras** menu, select **Map network drive**.



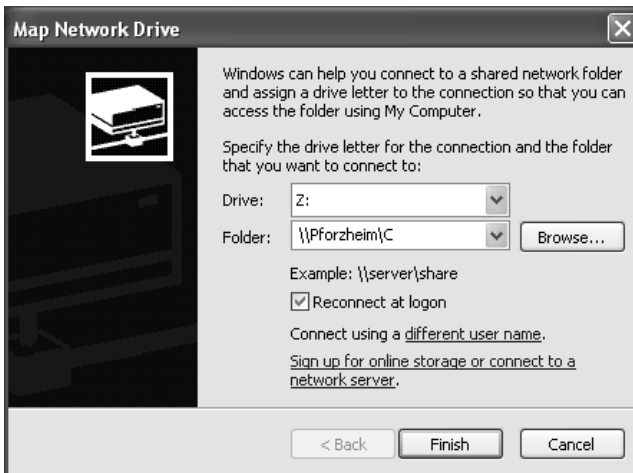
- ➔ Select the drive name under which the remote drive is to be hooked on to your PC.

Using released files and printers

- ➔ Enter a name under which the drive or folder is to be released for the network. To do this click **Browse**. This will open a screen in which you can search the network environment.



- ➔ Select the resource you want and click **OK**.



- ➔ If you select the option **Reconnect at logon**, Windows will hook the drive on every time you start your PC, provided the remote PC is running.
- ➔ Click **Finish**.
- ➔ Now open the desktop. The remote drive is now available as the network drive. You can access the files as if they were on your own PC.

Accessing released printers from your PC

If there is a printer on your local network and it has been released, you can use it to print out your data. To do this you have to set it up on your PC as the network printer. This can be done as follows:

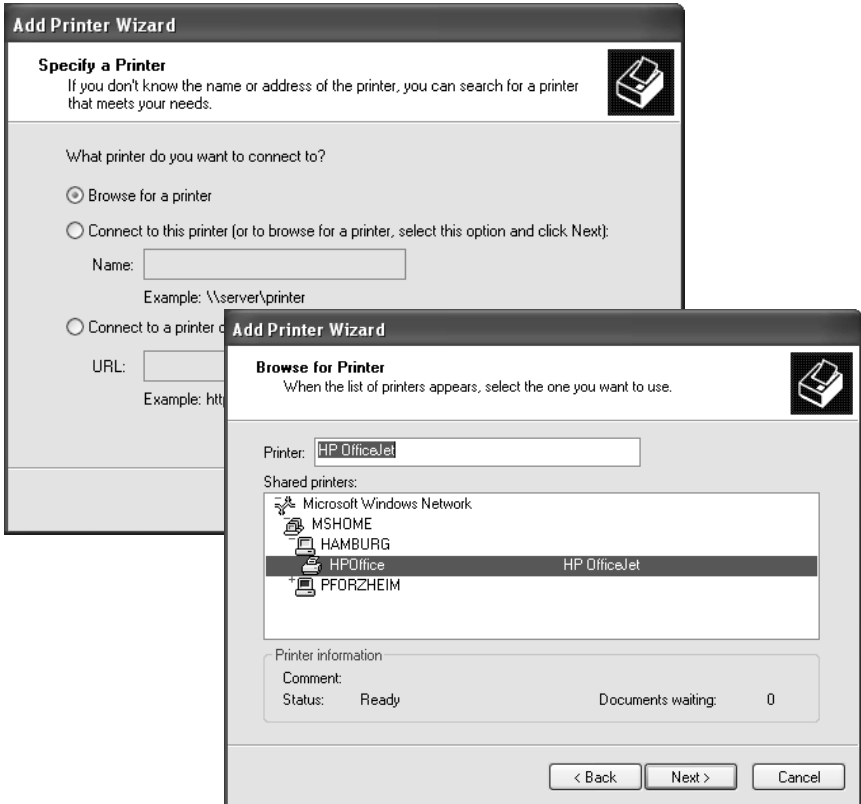
- ➔ Open the printer manager with **Printers and Faxes** in the Start menu.



- ➔ Select **Add printer**. This opens the printer installation wizard.
- ➔ Click **Next**.
- ➔ In the next window select **Network printer or printer connected to another computer**.
- ➔ Click **Next** again.
- ➔ Select **Browse for a printer** to look for the printer on the network.

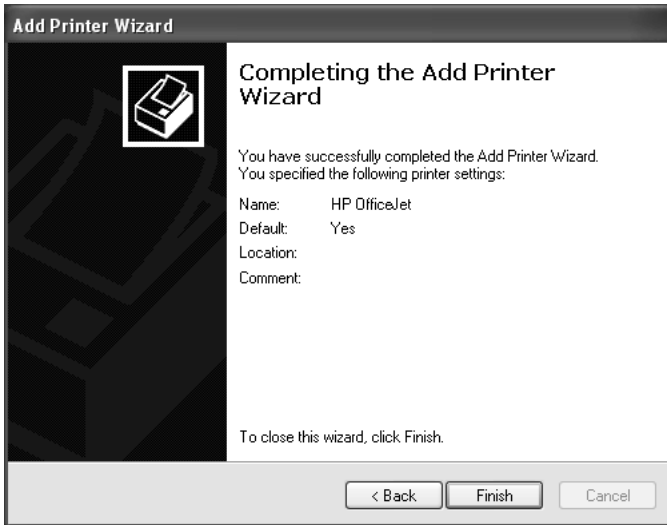
Using released files and printers

- ➔ Click **Next**. This will open a screen in which you can search the network environment for the printer.



- ➔ Select the printer you want and click **Next**.

➔ Complete printer installation with **Finish**.



The newly installed printer will now appear in the printer list and can be used just like a local printer.

Using files and printers on the network (Windows 2000)

You can use resources on your PC such as files and printers that have been made available by other PCs. To do this you have to make these resources available on your PC.

Setting up user names

To access files or printers on a Windows 2000 computer, you must set up a user name that corresponds to the release. This user name must also have been set up on the system which is releasing the files or printers. That is why setting up a user name has already been described in Chapter "Releasing files and printers for shared use" in the section "Setting up user names" on page 29.

Accessing released drives or folders from your PC

You can access drives and folders released on other PCs in two different ways:

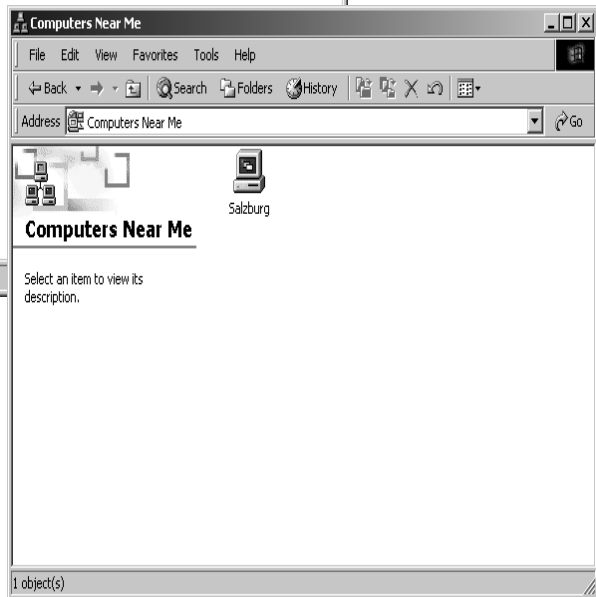
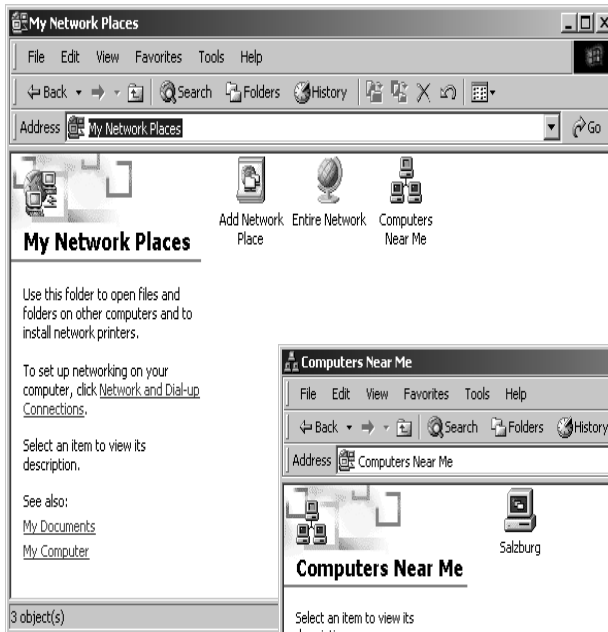
- ◆ via the My NetworkPlaces of your PC (see page 66).
You should choose this alternative if for example you want to copy files or folders from another PC to your own or vice versa.
- ◆ by hooking on to your PC's file system (see page 59).
You should choose this alternative if you want to work directly with the files or folders of the other PC. In this case, hook on an entire released drive or folder in your PC's file system and work with the files as if they were files on your PC.

Please note:

Drives or folders can be simultaneously hooked onto several PCs. It is therefore possible for other users to access the data. Most applications (e. g. word processing software) lock files once they have been opened. This prevents inconsistent data pools. If you cannot open a file because it is locked, you will normally see a message to that effect.

To hook up network drives:

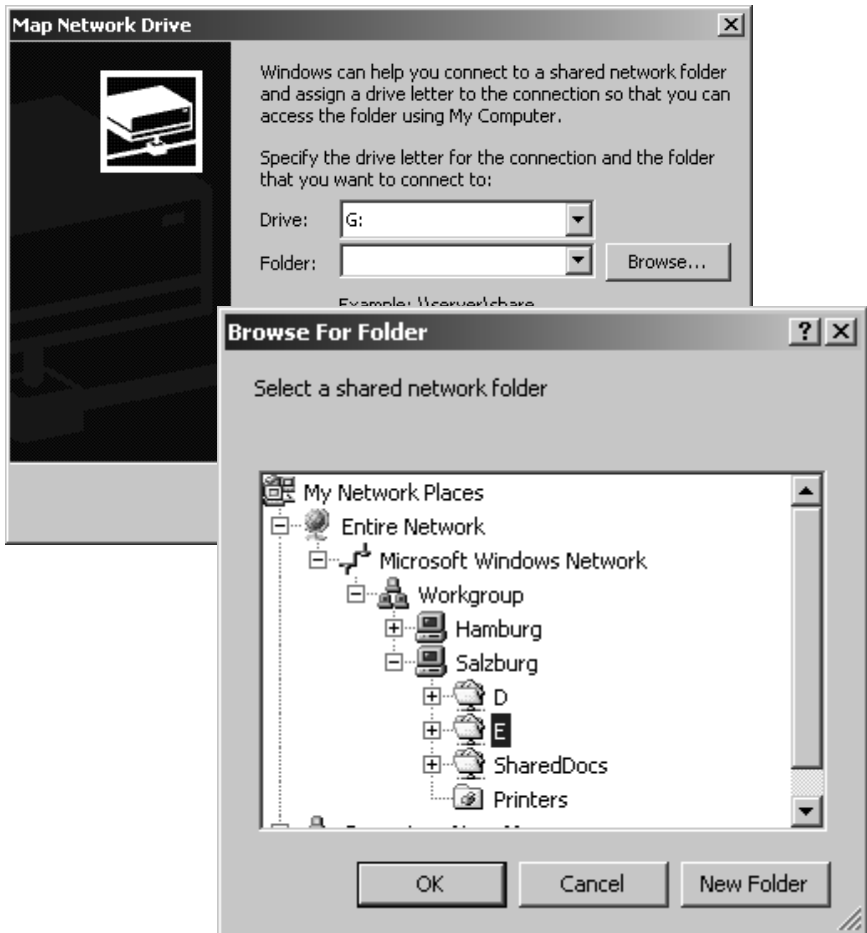
➔ Open the **My Network Places** and then **Computers near me**.



➔ Open the PC containing the resources you want to access with a double click. You will now see the shared resources on that PC.

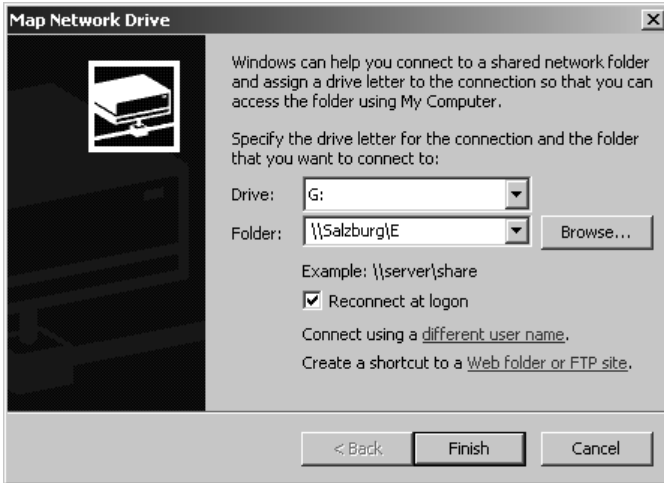
Using released files and printers

- ➔ Left-click the resource you want to attach to your PC and open the pop-up menu with the right-hand mouse button **Map network drive**.



- ➔ Select the drive name under which the remote drive is to be hooked on to your PC.
- ➔ Enter a name under which the drive or folder was released or click **Browse**. This will open a screen in which you can search the network environment.

- ➔ Select the resource you want and click **OK**.



- ➔ If you select the option **Reconnect at logon**, Windows will hook the drive on every time you start your PC, provided the remote PC is running.
- ➔ Click **Finish**.
- ➔ Now open the **Desktop**. The remote drive is now available as the network drive. You can access the files as if they were on your own PC.

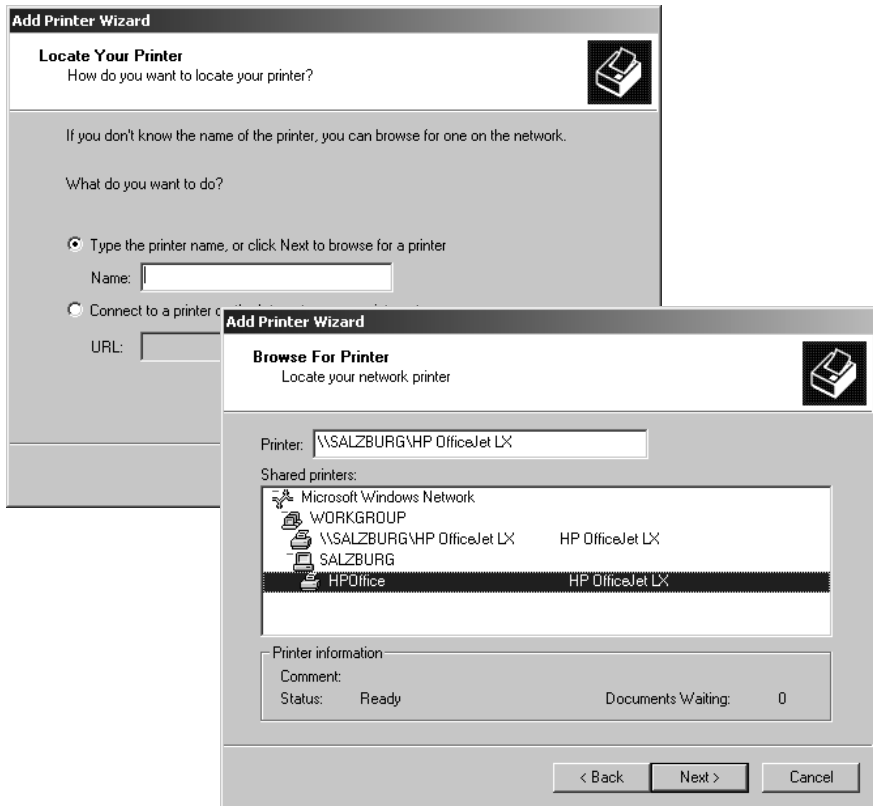
Accessing released printers from your PC

If there is a printer on your local network and it has been released, you can use it to print out your data. To do this you have to set it up on your PC as the network printer. This can be done as follows:

- ➔ Open the printer manager with **Start – Settings – Printers**.
- ➔ Click the **Add printer** icon. This opens the printer installation wizard.
- ➔ Click **Next**.
- ➔ In the next window select **Network printer**.
- ➔ Click **Next** again.
- ➔ Select **Enter printer name or click "next" to look for a printer** and click **Next**. This will open a screen in which you can search the network environment for the printer.

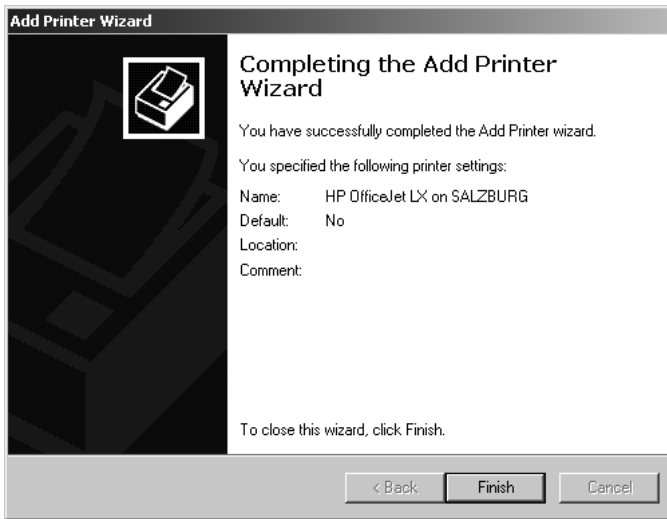
Using released files and printers

➔ Select the printer you want and click **Next**.



➔ Answer the prompt whether the printer is to be used as the standard printer with **Yes** or **No** and click **Next**.

➔ Complete printer installation with **Finish**.



The newly installed printer will now appear in the printer list and can be used just like a local printer.

Using files and printers on the network (Win 98 / 98 SE / ME)

You can use resources on your PC such as files and printers that have been released by other PCs.

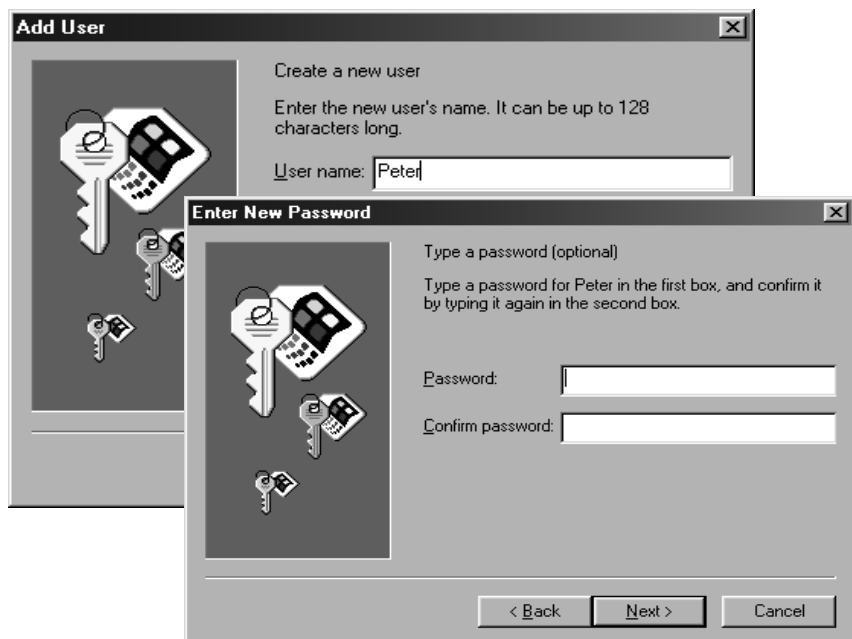
Please note:

If the resource you want to use on your PC is on a Windows 2000 system then you have to set up user IDs for all the users who are to have access. The same user IDs have to be entered as on the releasing system.

Setting up user names

To set up a user ID:

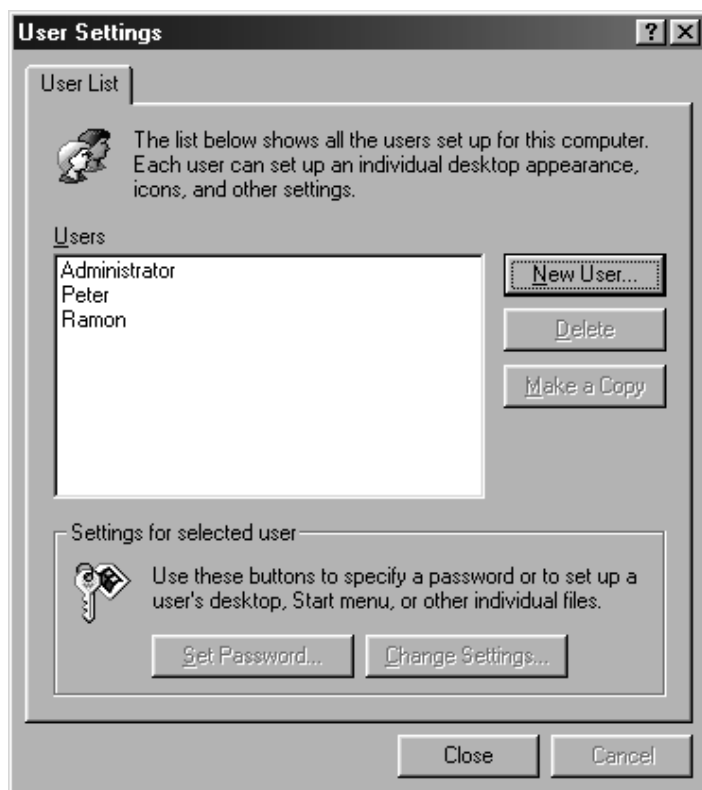
- ➔ Open the **Control Panel** and then open **User**.
- ➔ If there are no user entries yet, you will see a welcome screen. Confirm this with **Next**.
- ➔ If there are user names already, you will see the user list. Click **New user** and then **Next**.



- ➔ Enter a user name and click **Next**.
- ➔ Enter a password, repeat it and click **Next**.
- ➔ Define the settings for the user's interface. If you want to apply the current settings for the user, click **Next**.



The user has now been registered.



➔ Either enter further users or close user administration with **Close**.

Accessing released drives or folders from your PC

You can access drives and folders released on other PCs in two different ways:

- ◆ via the My NetworkPlaces of your PC (see page 66).
You should choose this alternative if for example you want to copy files or folders from another PC to your own or vice versa.
- ◆ by hooking on to your PC's file system (see page 67).
You should choose this alternative if you want to work directly with the files or folders of the other PC. In this case, hook on an entire released drive or folder in your PC's file system and work with the files as if they were files on your PC.

Please note:

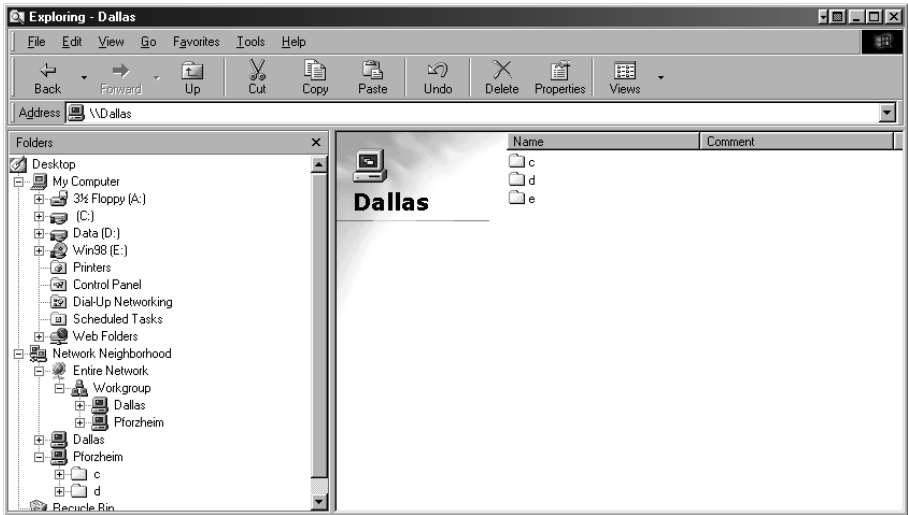
Drives or folders can be simultaneously hooked onto several PCs. It is therefore possible for other users to access the data. Most applications (e. g. word processing software) lock files once they have been opened. This prevents inconsistent data pools. If you cannot open a file because it is locked, you will normally see a message to that effect.

Accessing external files via the My NetworkPlaces

If the network has been set up on all the PCs with the same workgroup, then you can access released drives and folders via your PC's network environment.

You will find the **My NetworkPlaces** both as an icon on your PC desktop and also in the file tree in the left-hand pane of Windows Explorer. The illustration depicts as an example the **My NetworkPlaces** in Windows Explorer. In the **My NetworkPlaces** you will find the entry **Entire network**, under this the workgroup to which the PCs have been assigned and then the names of all the PCs comprising this workgroup.

Workgroups are marked with the  symbol:



Clicking a PC name shows the released drives and folders on this PC under the name assigned when they were released. You can navigate through the file system in the usual Windows Explorer way by clicking a drive or folder and then opening other branches of the file tree.

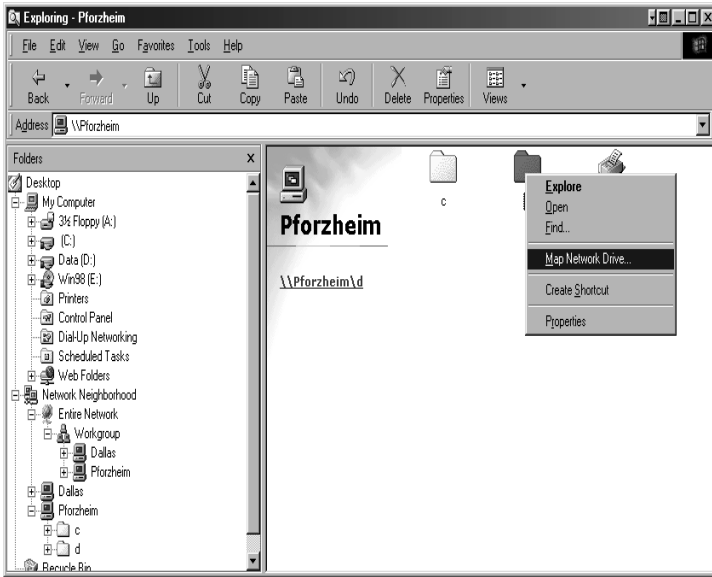
Hooking external files on to your own file system

You can hook released drives or folders on to your PC and use them as if they were actually on your own computer.

➔ Open the **My NetworkPlaces**.

Using released files and printers

- ➔ Open the PC containing the resources you want to access with a double click. You will now see the released resources on that PC.



- ➔ Left click the resource you want to hook on.
- ➔ Open the pop-up menu with the right-hand mouse button and select **Map network drive**.

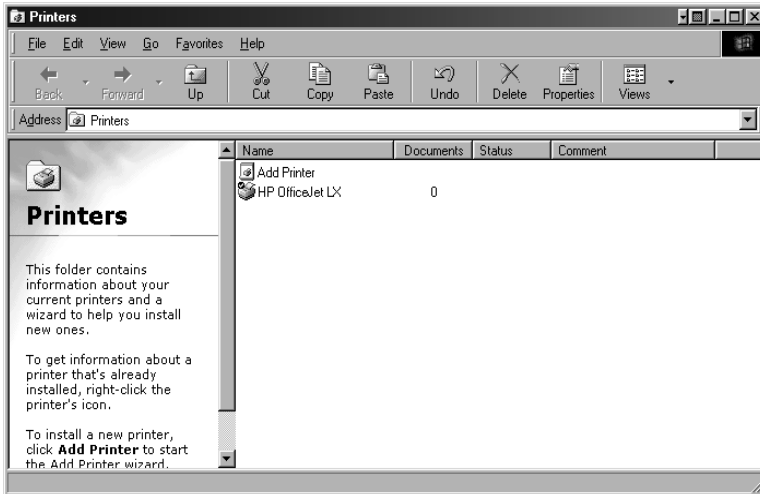


- ➔ Select the drive name under which the remote drive is to be hooked on to your PC. The next free drive will be prompted. If you select the option **Reconnect at logon**, Windows will hook the drive on every time you start your PC, provided the remote PC is running.
- ➔ Now open the desktop. The remote drive is now available as the network drive. You can access the files as if they were on your own PC.

Accessing released printers from your PC

If there is a printer on your local network and it has been released, you can use it to print out your data. To do this you have to set it up on your PC as the network printer. This can be done as follows:

➔ Open the printer manager with **Start – Settings – Printers**.



➔ Double-click the **Add printer** icon. This opens the printer installation wizard.

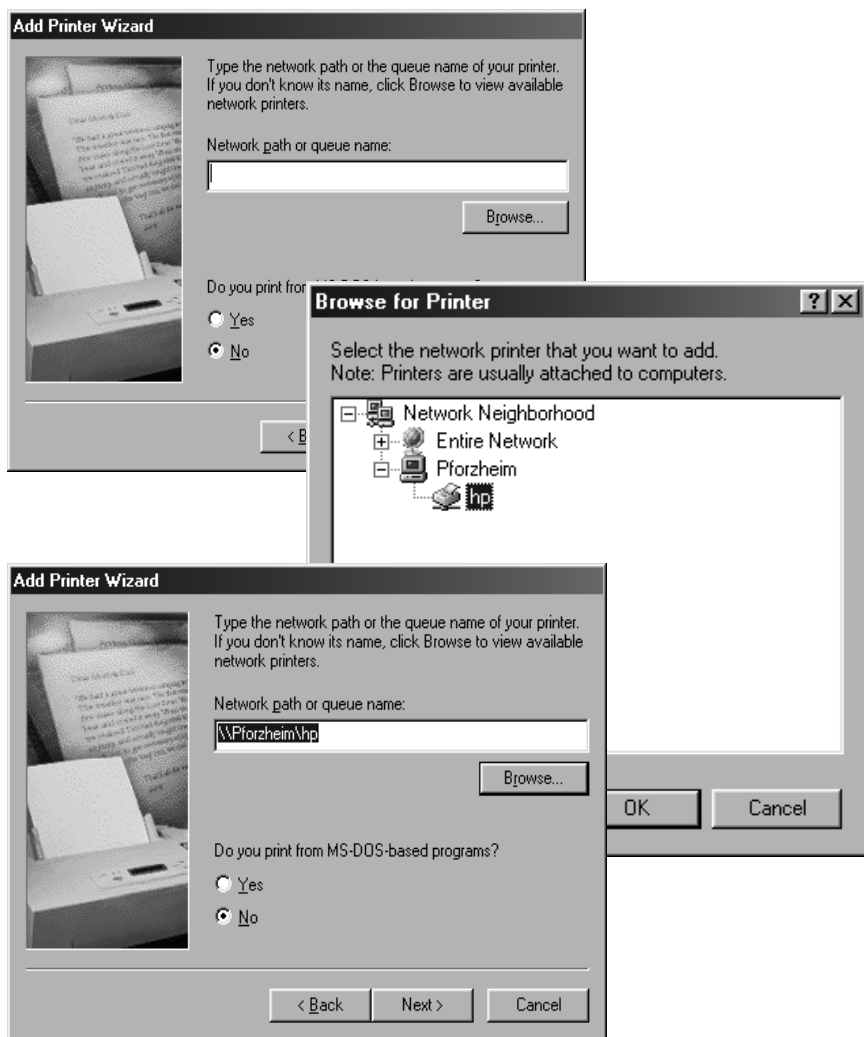
➔ Click **Next**.

➔ In the next window select **Network printer**.

➔ Click **Next** again.

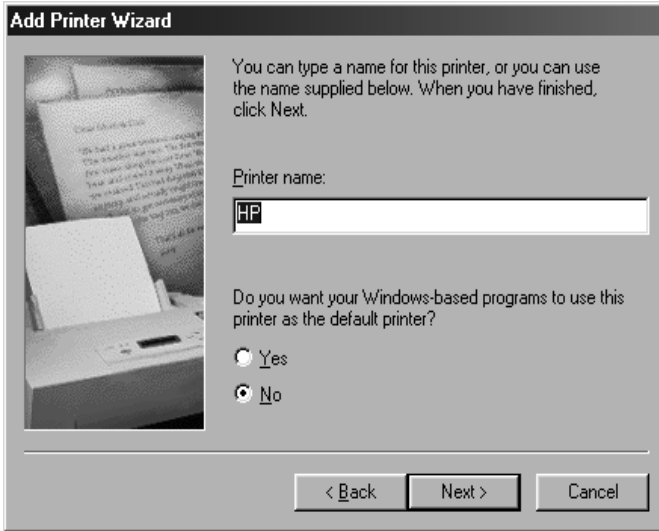
Using released files and printers

- ➔ Enter the name under which the printer was released for the network. To do this click **Browse**. This will open a screen in which you can search the network environment for the printer.
- ➔ Select the printer you want and click **OK**.

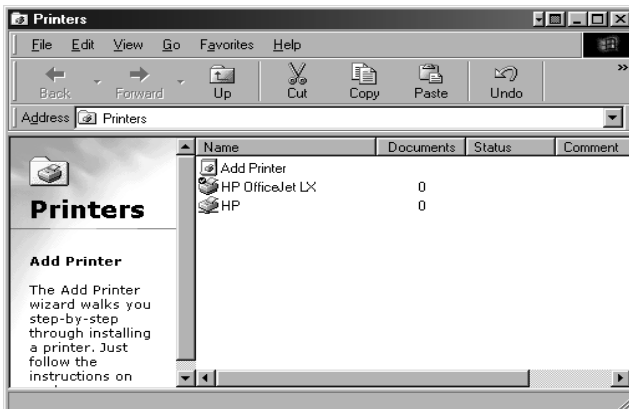


- ➔ The printer will now be displayed. Click **Next**.

- ➔ Now enter a name for the printer on your PC.



- ➔ Click **Next**.
- ➔ You can now print a test page if you want. This will show you whether the printer is functioning properly on the network.
- ➔ Click **Finish**.
- ➔ Windows will now need some driver files. You will be prompted to insert your Windows CD in the CD drive. Insert the CD and click **OK**.
- ➔ Once the driver files have been successfully installed, a test page will be printed.
- ➔ The newly installed printer will now appear in the printer list and can be used just like a local printer.



Defining IP addresses

The IP address is used for the unique identification of a network component. You can define IP addresses as static or dynamic. This is done while defining the PC network configuration. In many cases the IP addresses are defined as dynamic and so can change every time you log in to the network.

For some applications however you have to make sure that the PCs always have the same IP address.

If you opted for automatic assignment of IP addresses during installation, you can change this via the PC network configuration.

Network configuration differs depending on the Windows operating system you are using. Below you will find the procedure for Windows 98 from page 73, for Windows XP from page 77 and for Windows 2000 from page 80.

Private IP addresses

You can determine your own private IP addresses for the PCs in your local network. To do this use addresses from an address block reserved for private use. This is the address block

192.168.0.0 – 192.168.255.254

Example:

PC 1: 192.168.15.1

PC 2: 192.168.15.2 etc.

Please note:

The subnet mask used must be 255.255.255.0. This means that the first three address segments for all network components (including the router) must be identical.

◆ Correct is e. g.:

Router address: 192.168.2.1

PC 1: 192.168.2.12

PC 2: 192.168.2.60 ...

◆ Incorrect would be e. g.:

Router address: 192.168.2.1

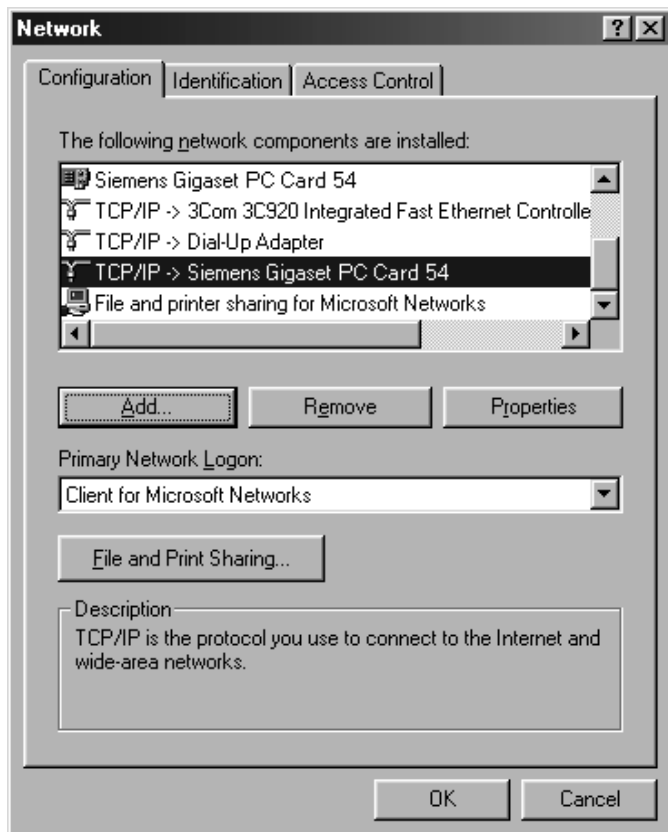
PC 1: 192.168.3.2

PC 2: 192.168.4.3

Windows 98

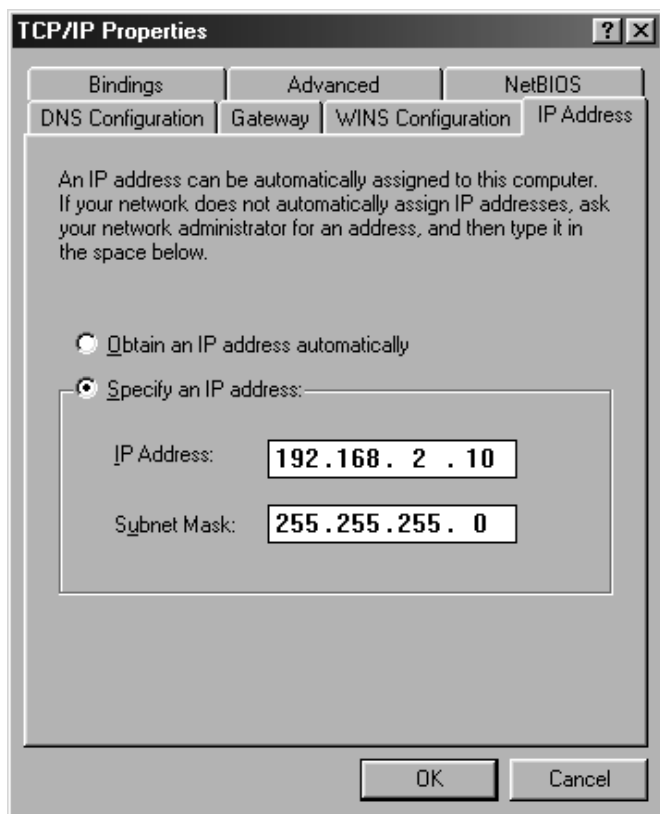
To set an IP address for your PC:

- ➔ Select **Start – Settings – Control Panel**.
- ➔ Double-click the **Network** icon.
- ➔ In the **Network** window, select the **TCP/IP** entry for your network card or network adapter in the **Configuration** tab. Make sure you select the right TCP/IP entry if there are several in the selection list.



Defining IP addresses

➔ Click **Properties**.



➔ Click the **IP address** tab and check the **Specify an IP address** option.

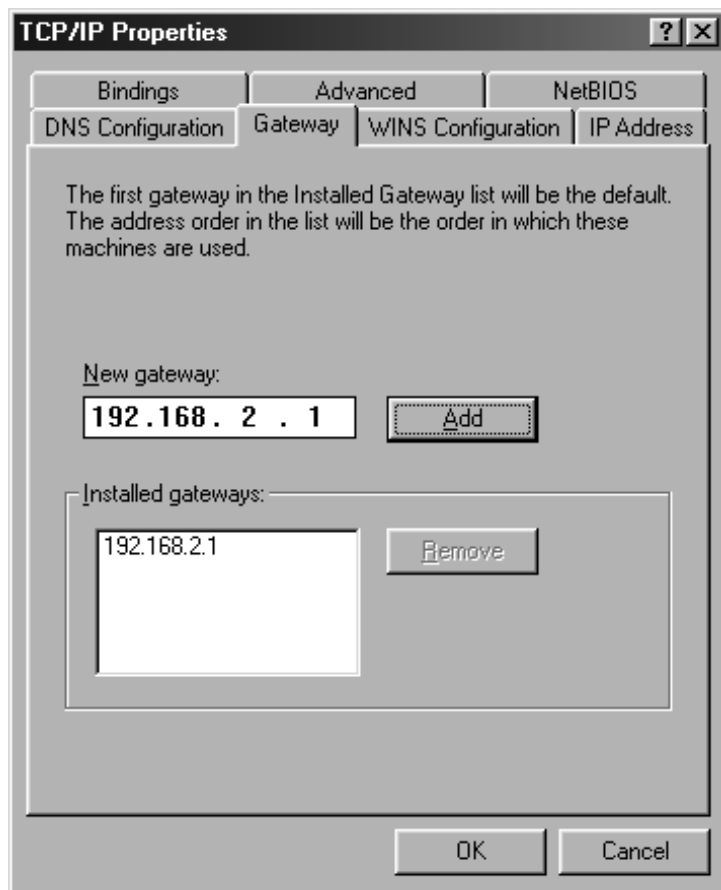
➔ Enter the IP address for the PC in the **IP address** box. Please bear in mind the information on page 72.

➔ Enter the subnet mask 255.255.255.0 in the box **Subnet Mask**.

Note:

If your PC has already been configured with a static IP address and you now need a dynamic one, select **Obtain an IP address automatically**. Then no further information will be required.

➔ Open the **Gateway** tab.



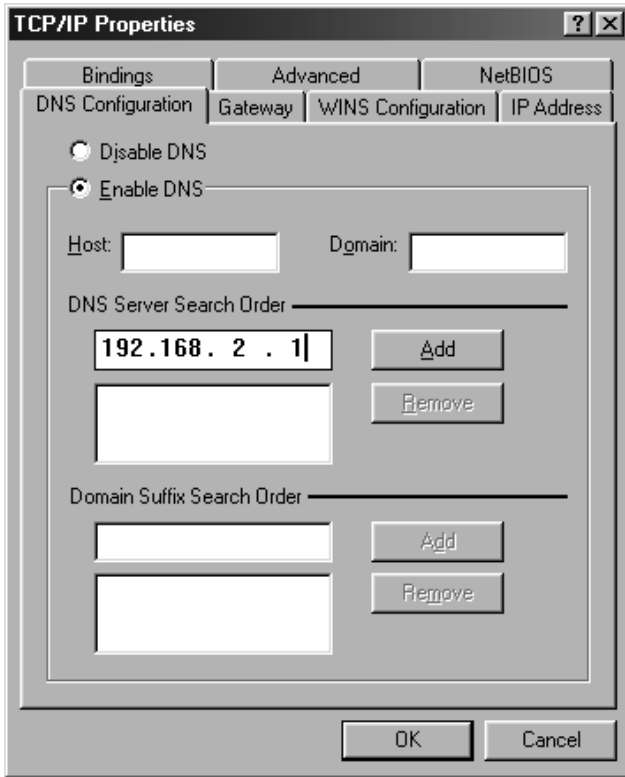
Note:

A gateway acts as a bridge between two networks with a different architecture. In our case this is the Gigaset Router between the local TCP/IP network and the WAN

➔ Enter the IP address of the router in the **New Gateway** box and then click **Add**.

Defining IP addresses

➔ Open the **DNS configuration** tab.



➔ Select **Enable DNS**.

Note:

DNS (Domain Name System) allows IP addresses to be assigned to a PC or domain names.

➔ Enter the IP address of the router in **DNS Server Search Order**.

➔ Click **Add**.

➔ Click **OK** twice to close the **Network** window.

➔ Restart your network.

Windows XP

Please note:

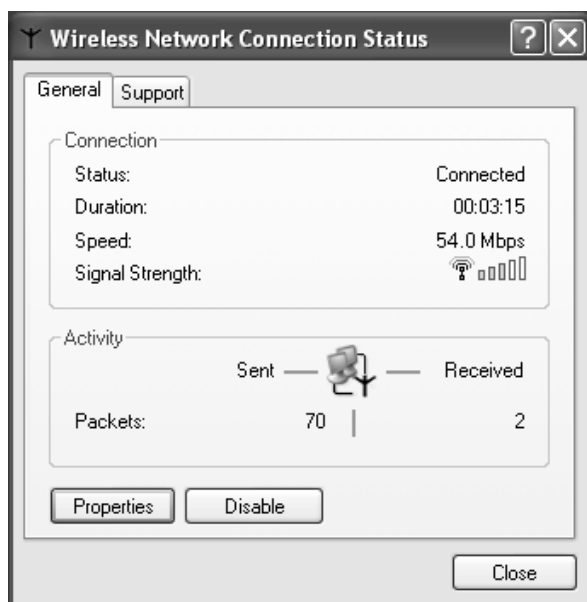
If you have a wireless connection between the router and PC: Make sure that the **Use Windows to configure the settings** function has been disabled.

This can be done as follows:

1. Click **Start – Settings – Control Panel – Network Connections – LAN or High-Speed Internet – Wireless Network Connection – Properties**.
2. In **Wireless Network Connection Properties** click **Wireless Networks**.
3. Deactivate **Use Windows to configure my wireless network settings**.

To set a static IP address for your PC:

- ➔ Click **Start – Control Panel**.
- ➔ Select **Network and Internet Connections** and then click the **Network Connections** icon.
- ➔ Double-click the LAN connection with which you are connected to the router.



Defining IP addresses

➔ In the **General** tab click **Properties**.



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

Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 2 . 61

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 2 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 2 . 1

Alternate DNS server: . . .

Advanced...

OK Cancel

- ➔ Select **Use the following IP address**.
- ➔ Enter the IP address for the PC in the **IP address** box. Please bear in mind the information on page 72.

Note:

If your PC has already been configured with a static IP address and you now need a dynamic one, select **Obtain an IP address automatically**. Then no further information will be required.

- ➔ Enter the subnet mask 255.255.255.0 in the **Subnet mask** box.
- ➔ Enter the IP address for the router in the **Standard-Gateway** box.

Note:

A gateway acts as a bridge between two networks with a different architecture. In our case this is the Gigaset Router between the local TCP/IP network and the WAN

Defining IP addresses

- ➔ Select *Use the following DNS server addresses*.

Note:

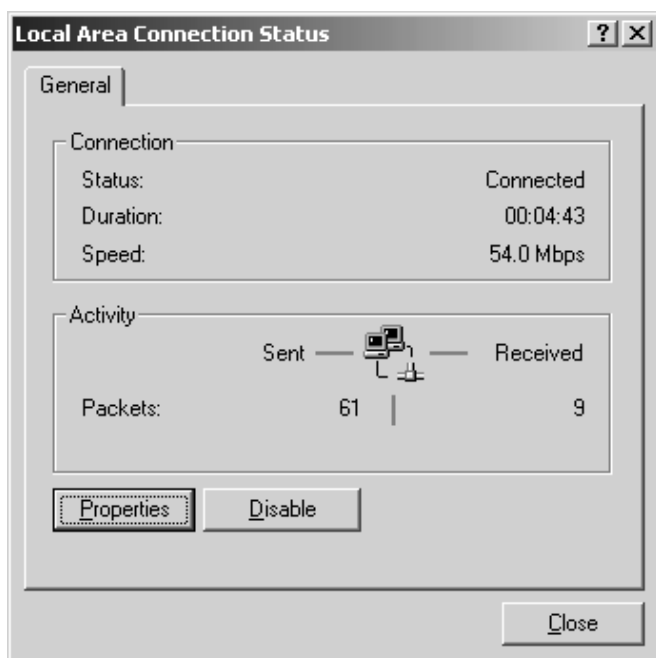
DNS (Domain Name System) allows IP addresses to be assigned to a PC or domain names.

- ➔ Enter the IP address for the router in the **Preferred DNS server** box.
- ➔ Click **OK** or **Cancel** to close each window.
- ➔ Restart your network.

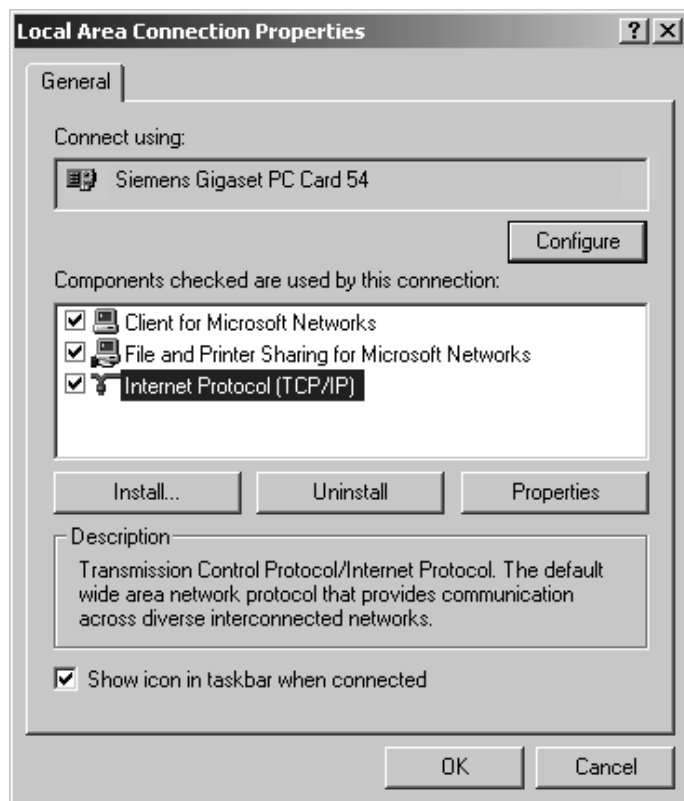
Windows 2000

To set a static IP address for your PC:

- ➔ Click **Start – Settings – Control Panel**.
- ➔ Double click the **Network and Dial-up Connections** icon and then **Local Area Connection**.



➔ In the **General** tab click **Properties**.



Defining IP addresses

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

The screenshot shows the 'Internet Protocol (TCP/IP) Properties' dialog box with the 'General' tab selected. The dialog has a title bar with a question mark and a close button. Inside, there is a text box explaining that IP settings can be assigned automatically or manually. Two radio buttons are present: 'Obtain an IP address automatically' (unselected) and 'Use the following IP address:' (selected). Below the selected radio button are three text boxes: 'IP address:' with the value '192 . 168 . 2 . 61', 'Subnet mask:' with '255 . 255 . 255 . 0', and 'Default gateway:' with '192 . 168 . 2 . 1'. Below these, there are two more radio buttons: 'Obtain DNS server address automatically' (unselected) and 'Use the following DNS server addresses:' (selected). Below the selected radio button are two text boxes: 'Preferred DNS server:' with '192 . 168 . 2 . 1' and 'Alternate DNS server:' with empty fields. At the bottom right of the dialog is an 'Advanced...' button. At the very bottom are 'OK' and 'Cancel' buttons.

- ➔ Select **Use the following IP address**.
- ➔ Enter the IP address for the PC in the **IP address** box. Please bear in mind the information on page 72.

Note:

If your PC has already been configured with a static IP address and you now need a dynamic one, select **Obtain an IP address automatically**. Then no further information will be required.

- ➔ Enter the subnet mask 255.255.255.0 in the **Subnet mask** box.
- ➔ Enter the IP address for the router in the **Standard-Gateway** box.

Note:

A gateway acts as a bridge between two networks with a different architecture. In our case this is the Gigaset Router between the local TCP/IP network and the WAN.

- ➔ Select ***Use the following DNS server addresses.***

Note:

DNS (Domain Name System) allows IP addresses to be assigned to a PC or domain names.

- ➔ Enter the IP address for the router in the ***Preferred DNS server*** box.
- ➔ Close this and the next window with ***OK***.
- ➔ Restart your network.

Glossary

Access point

An Access Point, such as the Gigaset SE551 WLAN dsl/cable, is the heart of a wireless local network ([WLAN](#)). It ensures the connecting of network components linked by wire and handles the data traffic in the wireless network. The Access Point is also the interface to other networks, e. g. an existing [Ethernet](#) LAN or via a modem to the [Internet](#). The operating mode of wireless networks with an Access Point is called [Infrastructure mode](#).

Ad-hoc mode

The Ad-hoc mode is a way operating wireless local networks ([WLAN](#)) in which the network components set up a spontaneous network without an [Access point](#), e. g. several Notebooks used in a conference. All the network components have equal rights. They must be fitted with a wireless [Network adapter](#).

Auto-Reconnect

Auto-Reconnect means that applications such as Web Browser, Messenger and E-Mail automatically open a connection to the [Internet](#) when they are launched. This can lead to high charges if you are not using [Flat rate](#). This function can be deactivated at the Gigaset SE551 WLAN dsl/cable to reduce costs.

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 SE551 WLAN dsl/cable 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 ([WLAN](#)) from another. In [Infrastructure mode](#) the BSSID is the [MAC address](#) of the [Access point](#). In wireless networks in [Ad-hoc mode](#) the BSSID is the MAC address of any one of the participants.

Client

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

DHCP

Dynamic Host Configuration Protocol

DHCP handles the automatic assignment of [IP addresses](#) to network components. It was developed because 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 SE551 WLAN dsl/cable includes a DHCP Server and so it can automatically assign IP addresses for the PCs on its local network. You can define for a particular PC that its IP address 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

DNS permits the assignment of IP addresses to computers 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 on the local network and the next higher Name Server, which again knows addresses on 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](#).

Glossary

DSL

Digital Subscriber Line

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](#). This means that the IP address of a network component [can](#) change with every login or at certain intervals.

See also: [Static IP address](#)

DynDNS

Dynamic DNS

Domain Name Service ([DNS](#)) is used to assign [Domain names](#) and [IP addresss](#). For [Dyna-mic IP addresss](#) this service is now enhanced with the 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 on the [Internet](#) can always be addressed 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 SE551 WLAN dsl/cable uses [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 control the data flow between the private network to be protected and an unprotected network such as the [Internet](#).

See also: [NAT](#)

Flat rate

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

Full duplex

Data 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 Electronic 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 ([WLAN](#)), 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)
- ◆ World-Wide Web (WWW)
- ◆ file transfer (FTP)
- ◆ discussion forums (Usenet / Newsgroups)

Glossary

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 [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 SE551 WLAN dsl/cable has a [Private IP address](#) and a [Public IP address](#).

IP address pool

The Gigaset SE551 WLAN dsl/cable 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](#).

You can use the Gigaset SE105 dsl/cable to set up both a wired local [Ethernet](#) network and also as wireless network as per the [IEEE 802.11g](#) standard.

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 bits per second

Specification of the transmission speed in a network.

MRU

Maximum Receive Unit

The MRU defines the maximum payload data within a data packet.

MTU

Maximum Transmission Unit

The MTU defines the maximum length of a data packet that can 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 on the local network available on the Internet despite NAT, you can configure the Gigaset SE551 WLAN dsl/cable 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 PC Card 108 and Gigaset USB Adapter 108.

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 of [IP address](#)/port number uniquely identifies the recipient or sender of a data packet within a network. Some applications (e. g. Internet services such as HTTP or FTP) work with fixed port numbers, others are allocated a free port number every time they need one.

Port Forwarding

In Port Forwarding the Gigaset SE551 WLAN dsl/cable 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 wired network to the [Internet](#) via a modem.

PPTP

An [Internet](#) connection using PPTP [Protocol](#) that creates a "tunnel" within an Internet connection for secure private connection in which the data is 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 SE551 WLAN dsl/cable, 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 SE551 WLAN dsl/cable, have a public and a [Private IP address](#).

Re-key Interval

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

Remote Management

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

Roaming

Roaming involves the use of several routers to extend the range of a network. The PCs on the network can switch dynamically between several Access Points.

Router

A router directs data packages 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 [WLAN](#) 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. But it can also mean an application that provides a particular service 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.

SSID

Service Set Identifier

The SSID identifies the stations of a wireless network ([WLAN](#)). All the wireless network components with the same SSID form a shared network. The SSID can be freely assigned.

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 SE551 WLAN dsl/cable 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.

Glossary

Super G

Super G technology can increase the transmission rate in the network to up to 108 Mbps by using channel bundling.

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](#) form the basis for every PC-to-PC 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 packages from a local network are encrypted and transmitted over the Internet using a tunnelling protocol (e. g. [PPTP](#)).

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

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 SE551 WLAN dsl/cable 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

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 [WLAN](#) against unauthorised access through [Encryption](#) of the data transmitted.

Wireless network

See [WLAN](#)

WLAN

Wireless LAN

Wireless LANs enable network components to communicate with and access a network using radio waves as the transport medium. A wireless LAN can be connected as an extension to a wired LAN or it can form the basis for a new network. The basic element of a wireless network is the so-called wireless 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 SE551 WLAN dsl/cable complies with Standard 802.11g.

WPA

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

Glossary

WPA-PSK

WPA Preshared Key: Variant of [WPA](#) data encryption, in which new keys are automatically generated at regular intervals by means of a keyword (Pre-shared key). The key is updated after defined periods ([Re-key Interval](#)).

XR

eXtended Range

The Access Point's XR function (Extended Range) is activated if the range is too large to establish a connection. It increases the range and, at the same time, decreases the transmission rate.

Index

- A**
- Access control
 - at release level 40
 - at user level 40
 - defining (Windows 98) 40
 - Access point 7, 84
 - Address block for IP addresses 72
 - Ad-hoc mode. 6, 84
 - Ad-hoc network. 6
 - Assigning static IP addresses
 - Windows 2000 80
 - Windows 98 73
 - Windows XP 77
 - Auto-Reconnect. 84
- B**
- Base station. 7
 - Bridge 84
 - Broadcast 84
 - BSSID. 84
- C**
- Change user passwords
 - Windows 2000 31
 - Checking network settings
 - (Windows XP) 19
 - Client 84
 - Connecting network drives
 - Windows 2000 60
 - Windows 98 68
 - Windows XP 53
 - Connection method. 17
- D**
- Define computer name
 - Windows 2000 26
 - Windows 98 40
 - Windows XP 18
 - Define workgroup
 - Windows 2000 26
 - Windows 98 40
 - DHCP. 85
 - Digital Subscriber Line see DSL
 - DMZ. 85
 - DNS 85
 - DNS Server. 76, 85
 - Domain name 85
 - Domain Name Service see DNS
 - DSL 86
 - Dynamic DNS Service see DynDNS
 - Dynamic Host Configuration Protocol
 - see DHCP
 - Dynamic IP address 86
 - DynDNS 86
- E**
- Encryption 86
 - Entering a gateway
 - Windows 2000 82
 - Windows 98 75
 - Windows XP 79
 - Ethernet. 5, 7, 86
 - Ethernet network
 - linking with wireless network 8
 - Extending coverage 9
 - Extending range. 4
- F**
- Files
 - shared use in a network 13
 - Firewall 86
 - Flat rate 86
 - Full duplex 86
- G**
- Gateway. 75, 79, 82, 87
 - Gigaset PC Card 108. 4, 6
 - Gigaset Router see Router
 - Gigaset SE551 WLAN dsl/cable 4, 5
 - Gigaset USB Adapter 108 4
 - Global IP address see public IP address
- H**
- Half duplex 87
 - Home network. 4

Index

- HTTP proxy 87
- Hub 87
- I
- IEEE 87
- Infrastructure mode 7, 87
- Infrastructure network 7
- Institute of Electrical and Electronic Engineers see IEEE
- Internet 7, 87
- Internet access 4
- Internet Protocol see IP Protocol
- Internet provider see Internet Service Provider
- Internet Service Provider 5, 88
- IP address 72, 88
 - address block 72
 - dynamic 86
 - pool 88
 - private 72, 90
 - public 90
 - static 91
- IP protocol 88
- IPSec 88
- ISP see Internet Service Provider
- L
- L2TP 88
- LAN 8, 89
- Launch
 - network wizard 15
- Launch network wizard (Windows XP) 15
- Layer Two Tunneling Protocol see L2TP
- Local IP address see private IP address
- Local network 89
- M
- MAC address 89
- Making drives available
 - Windows 2000 58
 - Windows 98 66
 - Windows XP 53
- Making files available
 - Windows 2000 58
 - Windows 98 66
- Windows XP 53
- Making folders available
 - Windows 2000 58
 - Windows 98 66
 - Windows XP 53
- Making printers available
 - Windows 2000 61
 - Windows 98 69
 - Windows XP 55
- Maximum Receive Unit see MRU
- Maximum Transmission Unit see MTU
- Mbps 89
- Microsoft Network 37
- Mobile network 6
- MRU 89
- MTU 89
- N
- NAT 89
- Network 89
 - ad-hoc 6
 - infrastructure 7
 - wired 5
 - wireless 6
- Network adapter 90
 - Ethernet 5
 - wireless 6
- Network Address Translation see NAT
- Network Client
 - setting up a (Windows 98) 39
- Network components
 - mobile 6
- Network configuration
 - Windows 2000 24
 - Windows 98 37
 - Windows XP 15
- Network environment
 - Windows 98 66
- Network service
 - installing a (Windows 2000) 24
- P
- Password for users
 - Windows 2000 30
 - Windows 98 64

- PC
 - configuring as Microsoft Network
 - Client 37
 - defining a name (Windows 2000) . . . 26
 - defining a name (Windows 98) . . . 40
 - defining a name (Windows XP) . . . 18
- Point-to-Point Protocol over Ethernet
 - see PPPoE
- Point-to-Point Tunneling Protocol
 - see PPTP
- Port 90
- Port Forwarding 90
- Port number 90
- Possible uses 11
- PPPoE 90
- PPTP 90
- Printer
 - shared use in a network 13
- Private IP address 90
- Protocol 90
- Public IP address 90
- R
- Releasing files
 - Windows 2000 32
 - Windows 98 46
 - Windows XP 21
- Releasing printers
 - Windows 2000 36
 - Windows 98 47
 - Windows XP 23
- Remote Management 91
- Repeater 9
- Rights for user access
 - (Windows 2000) 35
- Roaming 10, 91
- Router 4, 91
 - for wired networks 5
- S
- Server 91
 - virtual 93
- Service Set Identifier see SSID
- Setting the TCP/IP protocol
 - Windows 2000 27
 - Windows 98 41
- Setting up network printers
 - Windows 2000 61
 - Windows 98 69
 - Windows XP 55
- Setting up user IDs
 - Windows 2000 29
 - Windows 98 63
- Simple Mail Transfer Protocol see SMTP
- SMTP 91
- Specify workgroup
 - Windows XP 18
- SSID 91
- Static IP address 91
- Subnet mask 74, 79, 82, 91
- Subnetwork 92
- Switch 92
- T
- TCP 92
- TCP/IP 92
- TKIP (Temporal Key Integrity Protocol) 93
- Transmission Control Protocol see TCP
- Transmission speed 89
- Tunnel 90
- Tunneling 92
- U
- UDP 92
- Universal Plug and Play see UPnP
- Universal Resource Locator see URL
- UPnP 92
- URL 93
- User
 - settings for user interface
 - (Windows 98) 64
- User account
 - setting up a (Windows XP) 50
- User Datagram Protocol see UDP
- User list (Windows 98) 65
- User name
 - Windows 2000 30
 - Windows 98 64
 - Windows XP 50
- User password
 - Windows 2000 30
 - Windows 98 64
 - Windows XP 52

Index

Utility		Wide Area Network see WAN
for file and printer release		Wired Equivalent Privacy see WEP
(Windows 98)	44	and WEP encryption 5
V		Wired network 5
Virtual Private Network see VPN		Wireless cell 93
Virtual server.	93	Wireless LAN see WLAN
VPN.	93	Wireless network 93
W		ad-hoc mode 6
WAN	93	infrastructure mode 7
WAN interface	4, 7	Wireless network adapter 6
WEP.	93	WLAN. 6, 8, 93
		operating types. 6

Issued by
Siemens Communications
Haidenauplatz 1
D-81667 Munich

© Siemens AG 2005
All rights reserved. Subject to availability.
Rights of modification reserved.

Siemens Aktiengesellschaft
www.siemens.com/gigaset

No.: A31008-M1029-B101-1-7643