

SIEMENS

Be inspired

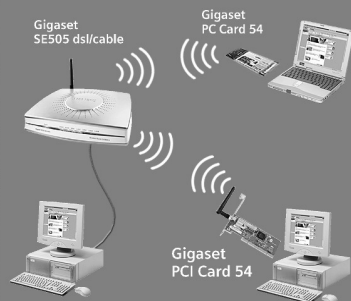
Practical Tips and Configuration Examples

Gigaset

SE 505

PC Card 54

PCI Card 54



Contents

Introduction 4

Local networks with Gigaset products	5
Wired local network (Ethernet)	6
Wireless local network (WLAN)	7
Ad-hoc network	7
Infrastructure Network	8
Roaming	10
Possible uses	11

Connecting PCs simply and quickly 13

Using ad-hoc networks	13
Requirements	15
Setting network adapters for ad-hoc mode	15
Checking the connection	17

Restricting access to the Internet 19

Requirements	20
Configuring the filter	21
Starting filter configuration	21
Providing and restricting access to Internet services	22
Permitting all services for a PC	23
Permitting non pre-defined services for a PC	24
Permitting pre-defined services for a PC	25
Activating the filter	26
Blocking access to certain Internet pages	27

Configuring security features 28

Launching Security Setup	29
Protecting your configuration with a password	30
Changing the SSID and disabling Broadcast	31
Sending encrypted data	33
64- and 128-bit key	33
Setting WEP encryption on the router	34
Setting up access control	36
Backing up the configuration	39
Security configuration on the network adapters	40
Changing the SSID on network adapters	40
Setting WEP encryption on the network adapters	41

Internet games 44

Starting configuration	44
Setting up Port Forwarding for games	45

Network conferences with MS Netmeeting 48

Starting configuration 48

Setting up Port Forwarding for MS Netmeeting 49

Offering your own server on the Internet 51

Starting configuration 51

Setting up Port Forwarding for Internet servers 52

Setting up demilitarised zones for servers 56

Sharing files and printers 58

Making your own files and printers available (WIN 98 / 98 SE / ME) 59

 Setting up a PC as Client for Microsoft Networks 59

 Selecting computer names and workgroup 62

 Selecting the access control 62

 Setting the TCP/IP protocol 63

 Installing utilities for file and printer release 66

 Releasing files and printers 68

Using files and printers on the network (Win 98 / 98 SE / ME) 71

 Setting up user names 71

 Accessing released drives or folders from your PC 74

 Accessing released printers from your PC 77

Making your own files and printers available (Windows XP) 80

 Configuring the network 80

 Selecting computer names and workgroup 83

 Checking the network settings 84

 Completing the installation procedure 85

 Releasing files and printers 86

Using files and printers on the network (Windows XP) 89

 Setting up a user account 89

 Accessing released drives or folders from your PC 92

 Accessing released printers from your PC 95

Making your own files and printers available (Windows 2000) 98

 Installing network services 98

 Selecting computer names and workgroup 100

 Setting the TCP/IP protocol 101

 Setting up user names 103

 Releasing files and printers 106

Using files and printers on the network (Windows 2000) 111

 Accessing released drives or folders from your PC 111

 Accessing released printers from your PC 115

Appendix: Defining IP addresses 117

Private IP addresses 117

Windows 98 118

Windows XP 122

Windows 2000 126

Glossary 130

Index 140

Introduction

This manual contains some examples of the many ways to use Siemens Gigaset products for local networks.

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.

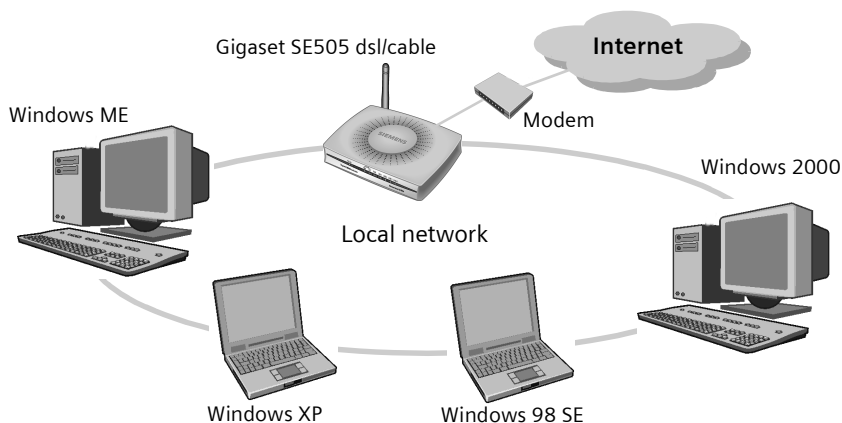
<i>i</i>	◆ The user interfaces depicted in this guide may differ from those on your screen because of the settings you have made. For Windows screens, the default state has been presented. There may also be minor differences due to different update cycles of user interface and this manual. ◆ In the examples we assume that the Gigaset network components have been installed and configured as per the corresponding operating instructions. ◆ This document is supplied with Siemens Gigaset SE505 dsl/cable, Gigaset PC Card 54 and Gigaset PCI Card 54 but is not part of the official packet. It does not give rise to any legal rights.
----------	---

Trademarks

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

Local networks with Gigaset products

You can use the Siemens Gigaset SE505 dsl/cable Router 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. The Gigaset SE505 dsl/cable has an interface so that you can connect a DSL or cable modem for Internet access (WAN interface).

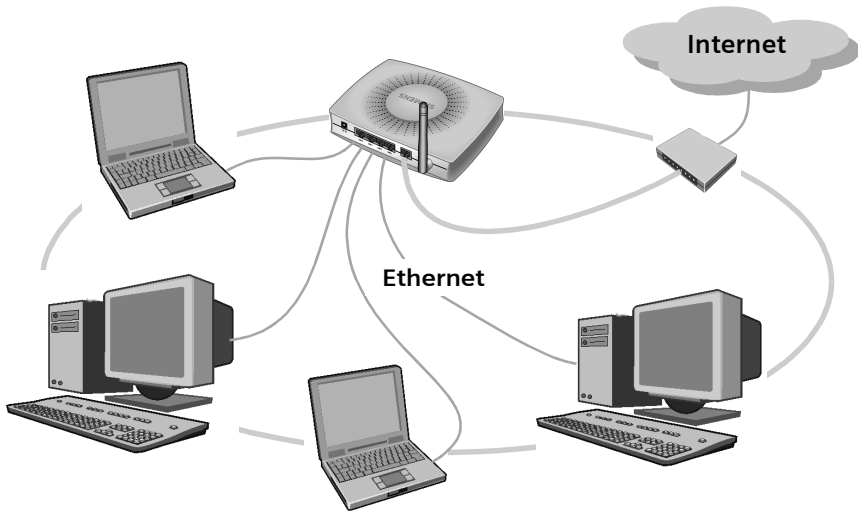


You can set up the network in a number of ways. You can

- ◆ use a Gigaset SE505 dsl/cable to set up a wired local network (see page 6).
- ◆ use the Gigaset SE505 dsl/cable to set up a local network comprising wireless and wired network components (see page 9).
- ◆ use the wireless network adapters Gigaset PC Card 54 or Gigaset PCI Card 54 to set up a wireless network without routers, i.e. connect PCs directly with each other (see page 7) or PCs to a Gigaset SE505 dsl/cable (see page 8).
- ◆ use several Gigaset SE505 dsl/cable units 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 SE505 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 Gigaset SE505 dsl/cable has a WAN interface that permits simultaneous access of all the PCs to the Internet. To use this feature you will need the access data from an Internet Service Provider, e. g. T-Online.

Wireless local network (WLAN)

In a wireless local network (WLAN) the PCs are linked to each other via a wireless connection. The PCs must have a wireless network adapter (WLAN adapter such as the Gigaset PC Card 54 or Gigaset PCI Card 54).

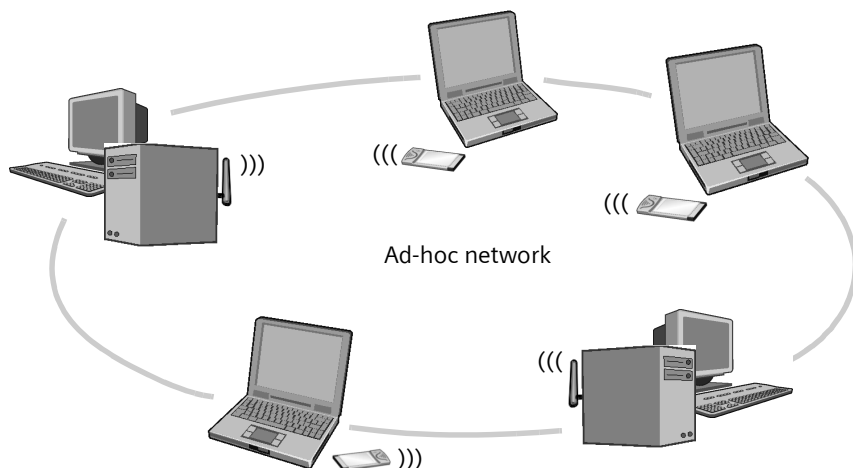
We generally differentiate between two types of wireless networks:

- ◆ 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.



How to set up an ad-hoc network is described in Chapter "Connecting PCs simply and quickly" from page 13.

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 as 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.

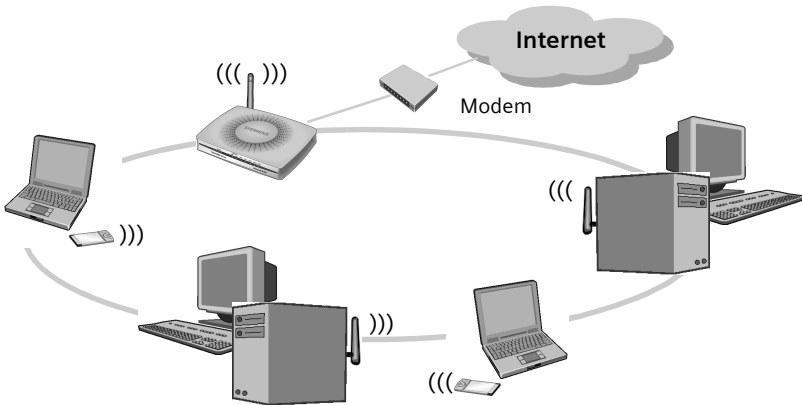
The Gigaset SE505 dsl/cable is such an access point. You can use it for connecting

- ◆ wireless linked PCs to the Internet and
- ◆ wireless linked PCs to an Ethernet network.

Infrastructure mode is the standard configuration for the Gigaset SE505 dsl/cable. This configuration is described in the quick guide enclosed with the router.

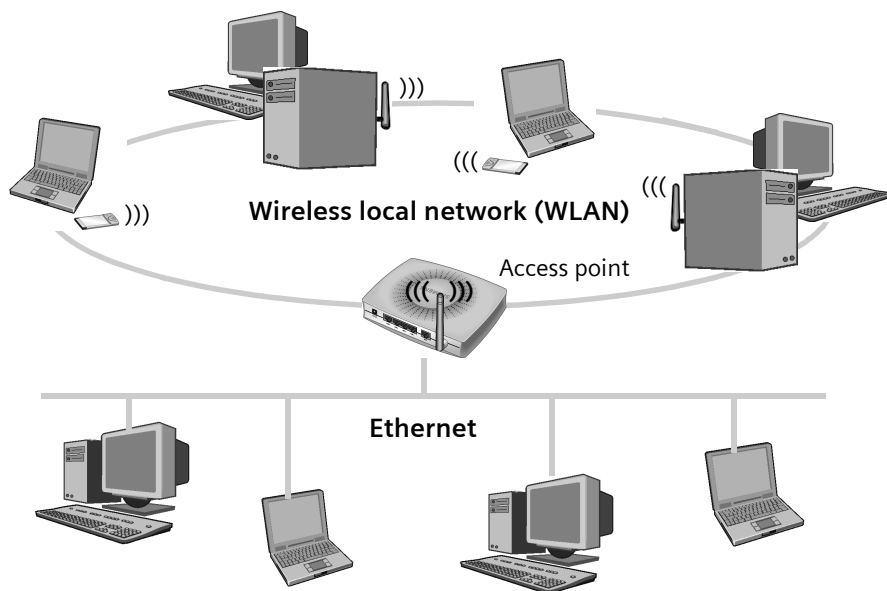
Connecting wireless networks to the Internet

The Gigaset SE505 dsl/cable has a WAN interface that permits simultaneous access of all the stations to the Internet. To use this functionality you will require a DSL connection that is provided by an Internet Service Provider. Please check whether your Internet Service Provider supports parallel access by several PCs.



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

A major advantage of wireless networks is their ability to work with existing Ethernet 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.



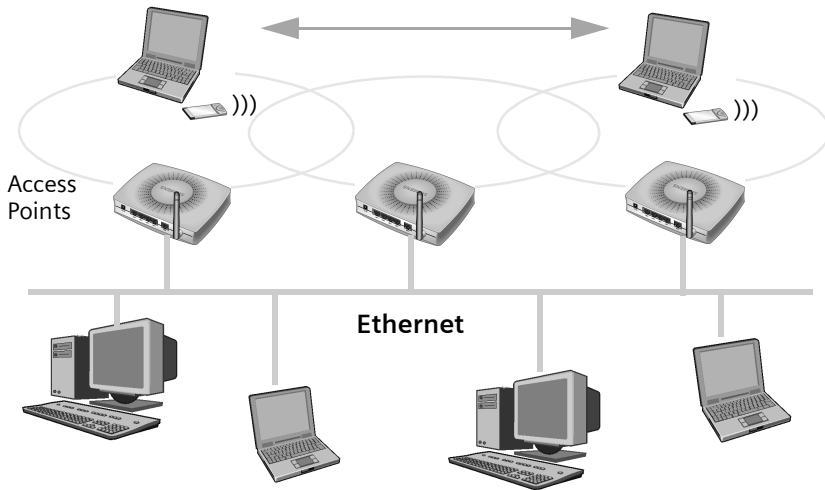
The Gigaset SE505 dsl/cable has four Ethernet LAN ports. Up to four PCs can be connected directly to these LAN ports. These PCs also access the Internet via the Gigaset SE505 dsl/cable.

i

You can also connect an Ethernet router to a LAN port for access to a larger Ethernet. If you want to link the Gigaset WLAN network to an existing network, a large number of settings have to be applied. Therefore we cannot provide a general example for this use; the configuration depends greatly on the networks in question. We advise having configuration of such a network carried out by an expert.

Roaming

Roaming allows connected users (PCs) to move freely between the various access points in a wireless local network without breaking the contact to the network. As soon as the wireless contact might be lost, the PC automatically looks for a different access point with a stronger signal. This technology permits the setting up of wireless networks that cover a much larger area than one access point alone could do. In addition, more users can be accommodated with the many access points. The main areas of use for WLANs with roaming are company sites and universities.



In a roaming network, all the users must use the same SSID (see page 31) and encryption (see page 33). The access points have to be connected via a shared wired network (Ethernet). This means you have to operate the Gigaset SE505 dsl/cable in bridge mode. Please consult the operating instructions supplied on the CD.

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 turn a PC on the network into a file server. All the central data is then stored on this PC. 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 release files for access to users on other PCs is described in Chapter "Sharing files and printers",

- for Windows 98, 98 SE, ME from page 68
- for Windows XP from page 86
- for Windows 2000 from page 106

How to make released files on other PCs available on your PC is described:

- for Windows 98, 98 SE, ME from page 74
- for Windows XP from page 92
- for Windows 2000 from page 111

◆ Shared use of printers

A printer is connected to a PC. In a network all the users can print their files using this one printer.

How to release printers for users on other PCs is described in Chapter "Sharing files and printers":

- for Windows 98, 98 SE, ME from page 70
- for Windows XP from page 88
- for Windows 2000 from page 110

How to make the printer connected to another PC available on your PC is described:

- for Windows 98, 98 SE, ME from page 77
- for Windows XP from page 95
- for Windows 2000 from page 115

◆ **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,
- block access to certain Web domains or pages.

How to set up these control functions is described in Chapter "Restricting access to the Internet" from page 19.

◆ **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).

How to activate the security functions for your network is described in Chapter "Configuring security features" from page 28.

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

The Gigaset SE505 dsl/cable comes programmed with a comprehensive firewall 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 ...).

How to run such applications is described in Chapters "Internet games" from page 44 and "Network conferences with MS Netmeeting" from page 48.

◆ **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 of the Gigaset router. This is described in Chapter "Offering your own server on the Internet" from page 51.

Connecting PCs simply and quickly

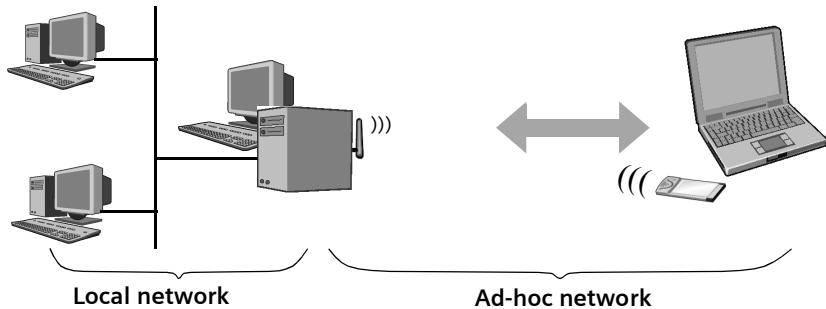
The easiest and fastest way of connecting two or more PCs is using an ad-hoc network (see also page 7). In an ad-hoc network all the computers have the same rights. Each computer can make resources available to users on the other PCs. This permits fast data exchange or shared use of files and printers (see also Chapter "Sharing files and printers" on page 58).

The most simple ad-hoc network comprises two PCs that communicate with each other without the need for an access point such as the Gigaset SE505 dsl/cable. The only requirement for each PC forming the ad-hoc network is a WLAN adapter such as the Gigaset PC Card 54 or Gigaset PCI Card 54.

Using ad-hoc networks

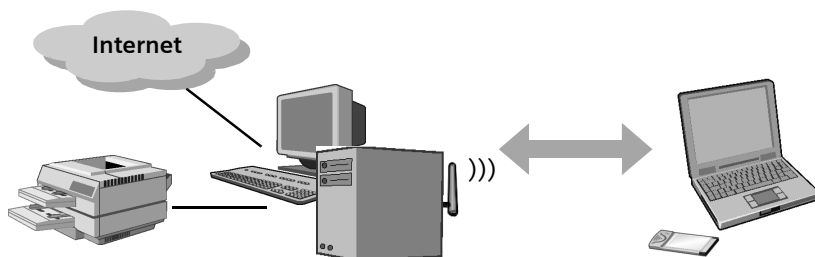
Setting up an ad-hoc network could be useful in the following situations.

1. You want to integrate your notebook into an existing local network temporarily to exchange files or programs for example.

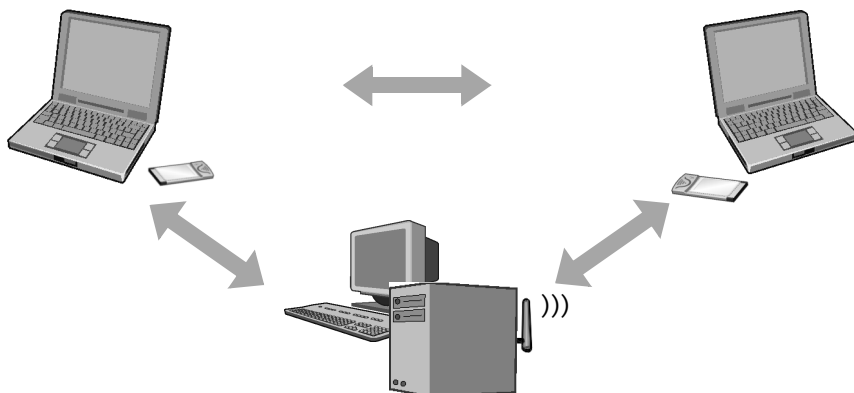


Connecting PCs simply and quickly

2. Printers, Internet connections or other resources like files on an already installed PC are to be used from other PCs.



3. Several users would like to play a PC game together.



Requirements

The following requirements have to be met if you want to set up an ad-hoc network:

- ◆ Wireless network adapters such as the Gigaset PC Card 54 or Gigaset PCI Card 54 have to be installed in all the PCs that will be communicating with each other. Please read the relevant operating instructions on how to install these adapters.
- ◆ The IP addresses of the PCs must be static.

The IP address is used for the unique identification of a network component. IP addresses can be assigned on a static or dynamic basis. This is determined during the network configuration of the PCs. In many cases the IP addresses are defined as dynamic and so can change every time a network connection is established.

Depending on the operating systems used in your network, ad-hoc mode may lead to communications problems if dynamic IP addresses are used. Therefore you should assign static IP addresses. You can find further information about this in the appendix on page 117.

Setting network adapters for ad-hoc mode

For ad-hoc mode you have to reconfigure your Gigaset PC Card 54 or Gigaset PCI Card 54. You can do this using the Gigaset WLAN adapter monitor.

To configure the ad-hoc mode on your PC:

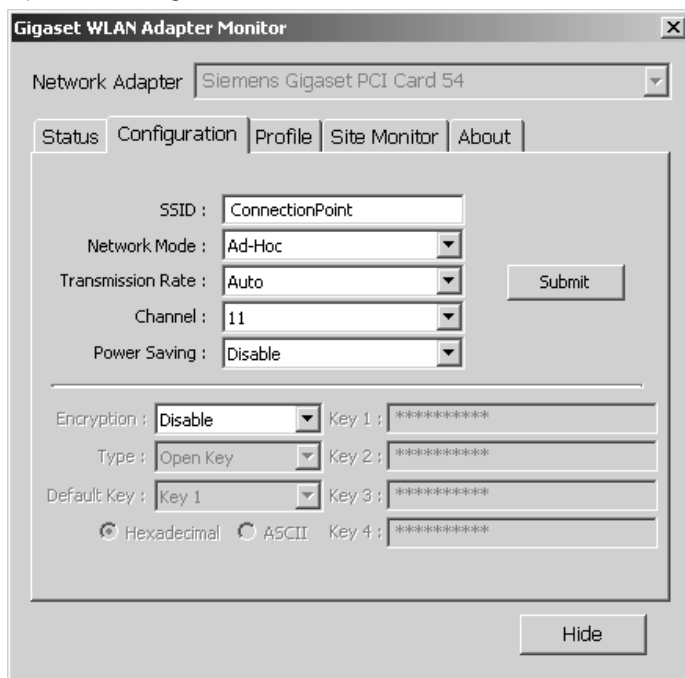
- ◆ Start the Gigaset WLAN adapter monitor by double clicking on the icon in the taskbar.



The *Gigaset WLAN adapter monitor* is displayed.

Connecting PCs simply and quickly

- ◆ Open the **Configuration** tab.



The screenshot shows the 'Gigaset WLAN Adapter Monitor' window with the 'Configuration' tab selected. The 'Network Adapter' dropdown is set to 'Siemens Gigaset PCI Card 54'. The 'Status' tab is also visible. The configuration fields are as follows:

Field	Value
SSID	ConnectionPoint
Network Mode	Ad-Hoc
Transmission Rate	Auto
Channel	11
Power Saving	Disable
Encryption	Disable
Type	Open Key
Default Key	Key 1
Key 1	*****
Key 2	*****
Key 3	*****
Key 4	*****

Buttons: Submit, Hide.

- ◆ In the **Network mode** list, select the entry **ad-hoc**.



Make sure that all the PCs involved have the same values for **Channel**, **SSID** and **Encryption**!

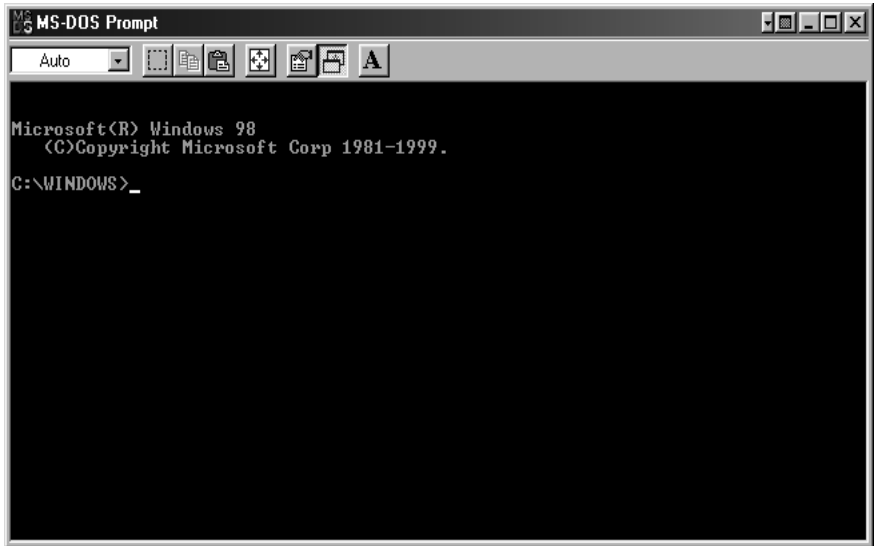
- ◆ Click **Submit**.
- ◆ Click **Hide** to close the window.

Checking the connection

Once you have completed the steps described in Section "Setting network adapters for ad-hoc mode" for each PC in the ad-hoc network, you can check whether a connection has been established.

This can be done as follows:

- ◆ Open the **command prompt**. This can be done by clicking **Start – Programs – command prompt**.



- ◆ Then for each PC to be linked enter a `ping` command. To do this you will need the name of the PC on the network or its IP address.

Example:

You want to connect three PCs in your ad-hoc network. You have assigned the IP addresses 192.168.5.1 (PC 1), 192.168.5.2 (PC 2) and 192.168.5.3 (PC 3) for the PCs.

Enter in the command prompt on PC 1:

`ping 192.168.5.2` (checks whether data exchange with PC 2 is possible)

`ping 192.168.5.3` (checks whether data exchange with PC 3 is possible)

Apply the same procedure on the other PCs.



If you have forgotten which IP addresses you assigned, you can find the IP address on each PC by using the command `ipconfig`.

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

If the command does not return any statistics, but ends with a time-out, then this means that the components cannot communicate with each other. Reboot the PCs and check that you have carried out all the steps in the Section "Setting network adapters for ad-hoc mode" correctly.

- ◆ You can close the command prompt window by entering the `exit` command.

Restricting access to the Internet

The default setting in your router is that all PCs registered with the router can use all Internet services and access all Internet pages. For security and cost reasons many users attach great importance to controlling access to the Internet. Particularly for parents, for example, it is important that their children cannot access certain Internet pages or that their children's PCs cannot access the Internet at all.

You can use the filter function to determine which PCs may use which services and block access to various Internet addresses. Once the filter function is enabled, only those PCs that are in the table can connect to the Internet. All the other PCs are completely cut off from the Internet.

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

- ◆ Filtering of services (see page 22)

Here you can define which PCs are to have access to the Internet and which Internet services can be called from which PC.

- ◆ URL filtering and domain blocking (see page 27)

This allows you to prevent the displaying of a particular website with a particular URL address or the Web pages of a particular domain.

Example:

- Blocking the URL `http://www.abcd.com` means that none of the Web pages of the domain `www.abcd.com` can be displayed.
- Blocking the URL `http://www.abcd.com/products` means that precisely the `http://www.abcd.com/products` and subsequent pages cannot be displayed.

Requirements

You always define a services filter for a given PC. A defined filter can only be assigned properly if the PC can be identified uniquely. There are two ways of ensuring this:

1. Via the registration to the router

This is only possible for PCs that obtain their IP address via the router's DHCP server and are registered with the router. These PCs are shown in a selection list and you can define a filter for them without any further information.

2. Via the MAC address

You can use this when a PC does not obtain its IP address via the router's DHCP server or the PC does not happen to be registered with the router.

The MAC address is the hardware address of the network adapter use for connecting to the router. It is fixed and cannot be changed.

If you want to set filter functions using MAC addresses, you have to know the PC's MAC address. Open the **MS-DOS prompt** on the PC in question and enter the command `ipconfig /all`. This command returns detailed information about the network adapters. You will find the MAC address of each installed network adapter under **Physical address**. If there are several network adapters in the PC, make sure you use the right address.



Please bear in mind that changing the network adapter will negate the PC's registration as the new adapter will have a different MAC address.

Configuring the filter

The example configuration on the following pages is based on the following assumptions:

- ◆ Unrestricted Internet access for PC "My_PC".
- ◆ Peter's PC is to have access to a particular service, "SuperService".
- ◆ Anna's PC is to have Internet access, i. e. access to HTTP service.
- ◆ A number of Web addresses (URLs) are to be blocked.
- ◆ All the other PCs are to be completely cut off from the Internet. This is done automatically once you enable the filter.

To set up this configuration:

1. Create a filter table with
 - an entry for the PC "My_PC" with unrestricted access (see page 23),
 - an entry for Peter's PC with access to "SuperService" (see page 24),
 - an entry for Anna's PC with access to the HTTP service (see page 25).
2. Define the URL blocks you want (see page 27).

Starting filter configuration

To start filter configuration:

- ◆ Launch your Web Browser.
- ◆ Enter the router IP address in the Web Browser address bar. If you have not configured the router with a different IP address, this will be `http://192.168.2.1`
You will then see a login window:
- ◆ If a password has already been assigned, enter it and click **LOGIN**.
- ◆ After logging in, select **Advanced Setup**.
- ◆ Open the **Filter** menu.

Providing and restricting access to Internet services

If you want to provide or restrict access to Internet services, you have to define a filter table. Open the **Filter** window.

- ◆ Select in the left-hand pane the entry **Filter – Internet services**.

Internet Services

Disabling the WAN port ping replay makes your router more secure against possible attacks from external hosts. For the PC's in your local network you can define services the PC can use in the internet. Other services are filtered. The table can have up to 16 entries.

WAN Port Ping Replay :
☒ Disabled ☐ Enabled

List Use (Filter Type) :
☐ Use the list to allow the access to the internet ☒ Do not use the list

How do you define the service :
☒ Select predefined services from the list
☐ Define service manually

Select the service you want to filter :

Predefined services

Protocol

Port

HTTP

TCP

80

Select PC >>

Allowed service		This service is allowed for		Details	Delete
Name	Port	PC Name			
No filter defined yet !					

The filter's default setting is disabled, i. e. all the PCs connected have access to all services. You have to set up a filter table before activating the filter function. Each entry in the filter table assigns a particular service to a given PC. You can make up to 16 entries.

All the PCs you include can use the Internet services assigned to them. PCs not in the table cannot connect to the Internet.

!

If you block the Internet access for the PC you are using you will no longer have any access to your Gigaset Router user interface because you have to enter an http address to open it and thus use an Internet service. The access block applies once you activate the filter. If you have accidentally blocked access to the user interface, you will have to reset the router. This can be done by switching the router off, pressing the reset button on the back and switching the router on again while keeping the reset button pressed. Please bear in mind that this will restore **all** configuration settings to the factory settings.

22

Permitting all services for a PC

You want to add a PC to the filter table with the name "My_PC" with full Internet access rights. The PC has already been registered with the router.

This can be done as follows:

- ◆ Open the **Predefined services** selection list and select the entry **ALL**.

Select the service you want to filter :

Predefined services: ALL Protocol: ALL Port: 0-0

Select PC >>

- ◆ Click **Select PC>>**

WAN Port Ping Replay : ☒ Disabled ☐ Enabled

List Use (Filter Type) : ☒ Use the list to allow the access to the internet ☐ Do not use the list

How do you define the PC: ☒ Select the PC from the list.
☐ Select PC manually

These PC's are active booked in.

Select the PC: My_PC 00:90:96:4b:d6:93

<< Back Add to List >>

- ◆ Select the appropriate PC from the list of registered PCs.
- ◆ Click **Add to list**.
- ◆ Click **APPLY**.

Allowed service		This service is allowed for	Details	Delete
Name	Port	PC Name		
ALL	0-0	My_PC	Detail	Delete

The PC has now been added to the table.

Permitting non pre-defined services for a PC

Peter's PC is to be permitted to access a particular service available on the Internet under the name "SuperService". This will require certain information about the service, e. g. the protocol and the port number(s) that the service uses.

Peter's PC is not connected to the router at the moment so it will have to be registered manually.

- ◆ Select **Define service manually**.

How do you define the service :	☐ Select predefined services from the list ☒ Define service manually	
Select the service you want to filter :	Service name	SuperService
	Protocol	☒ TCP ☐ UDP
	Port	1704
		Select PC >>

- ◆ Again enter the name of the service.
- ◆ Select the protocol the service uses.
- ◆ Enter the port number(s) used by the service for communication. You can enter a block of port numbers with a hyphen (1230-1239) or different port numbers separated by commas.
- ◆ Click **Select PC>>**
- ◆ As the PC is not registered at the moment, you will have enter it manually. Select **Select PC manually**.

How do you define the PC:	☐ Select the PC from the list. ☒ Select PC manually	
Select thePC:	PC Name (optional)	Peters_PC
	MAC-Address	00 : 93 : c5 : f0 : 42 : 5a
		<< Back Add to List >>

- ◆ Enter a name for the PC so that you can find it more easily in the table in future. You can assign any name you want.
- ◆ Enter the PC's MAC address (see page 20).
- ◆ Click **Add to list**.
- ◆ Click **APPLY**.

Allowed service		This service is allowed for	Details	Delete
Name	Port	PC Name		
ALL	0-0	My_PC	Detail	Delete
SuperService	1704	Peters_PC	Detail	Delete

The PC has now been added to the list.

Permitting pre-defined services for a PC

Now we need an entry for Anna's PC. She is to have restricted Internet access, i. e. she must be assigned the HTTP service.

- ◆ Select the entry **HTTP** in **Predefined services**.

How do you define the service :

☒ Select predefined services from the list
☐ Define service manually

Select the service you want to filter :

Predefined services

Protocol

Port

HTTP

TCP

80

Select PC>>

- ◆ Click **Select PC>>**

WAN Port Ping Replay : ☒ Disabled ☐ Enabled

List Use (Filter Type) : ☒ Use the list to allow the access to the internet ☐ Do not use the list

How do you define the PC:

☒ Select the PC from the list.
☐ Select PC manually

These PC's are active booked in.

- ◆ Select the appropriate PC from the list of registered PCs.
- ◆ Click **Add to list**.
- ◆ Click **APPLY**.

Restricting access to the Internet

Allowed service		This service is allowed for	Details	Delete
Name	Port	PC Name		
ALL	0-0	My_PC	Detail	Delete
SuperService	1704	Peters_PC	Detail	Delete
HTTP	80	Annas_PC	Detail	Delete

The PC has now been added to the table.

Activating the filter

Once you have added all the entries you want to the filter table, you have to activate the table.

WAN Port Ping Replay :	☒ Disabled ☐ Enabled		
List Use (Filter Type) :	☒ Use the list to allow the access to the internet ☐ Do not use the list		
How do you define the service :	☒ Select predefined services from the list ☐ Define service manually		
Select the service you want to filter :	Predefined services HTTP	Protocol TCP	Port 80
			Select PC >>

- ◆ Activate the filter.
- ◆ Click **APPLY**.



No new entries can be made to the list while it is active.

Blocking access to certain Internet pages

All we have to do now is set up the URL filter for blocking Internet pages.



Please bear in mind that the assigned URL filter applies for **all the PCs**.

- ◆ Select in the left-hand pane the entry **Filter – URL filter**.
Initially the list is empty.
- ◆ Enter the URL you want to block. The specified domain or Internet page and all the subsequent pages will be blocked.

URL filter :		☒ Enabled ☐ Disabled
Select the URL you want to block:	http://www.supergame.com	Add to the list
URL		Delete
No URL added yet !		

- ◆ Click **Add to list**.

URL filter :		☒ Enabled ☐ Disabled
Select the URL you want to block:		Add to the list
URL		Delete
www.supergame.com		Delete

- ◆ Add any further URLs to the list.

URL		Delete
www.supergame.com		Delete
www.eroticnet.de		Delete
www.gewalt.de		Delete

- ◆ Click **APPLY**.

This permanently blocks the specified Internet pages.

Configuring security features

You should make the following settings for the greatest possible security in your local network:

- ◆ Protect your router configuration with a password (see page 30).
This will prevent users on your network from changing your router's settings, especially the security settings themselves.

For wireless networks you should also:

- ◆ Change the SSID (Service Set ID) (see page 31).
Change the factory-set SSID **ConnectionPoint** to a new secret password, preferably a combination of numbers, letters and special characters. Only those who know the SSID can log in to your router in wireless mode. Avoid proper names or words that your neighbour for example could easily guess.
- ◆ Disable the broadcast function for the SSID (see page 31).
Then the router will no longer transmit the new SSID and it can no longer be "read" by eavesdroppers.
- ◆ Activate WEP encryption (see page 33).
This will apply 64- or 128-bit encryption to the data sent over the network and thus prevent eavesdropping.
- ◆ Create an access table (MAC access table, see page 36)
This determines which PCs have wireless access to your router. All the others will be excluded.

i

- ◆ Remember that the SSID and the WEP key have to be the same on all the wireless components.
- ◆ Before you change your Gigaset SE505 dsl/cable settings, we recommend that you back up the current functioning state of the router first!
To do this select in Advanced Setup **Administration -Backup and Restore**. Click **Backup**, follow the dialogue that appears and save your settings.

The Gigaset SE505 dsl/cable has a security setup that guides you step by step through the most important configuration actions for router security. This can also be done via Advanced Setup. Here we will describe configuration using Security Setup with appropriate references to the corresponding functions in Advanced Setup.

Launching Security Setup

To launch Security Setup:

- ◆ Launch your Web Browser.
- ◆ Enter the router IP address in the Web Browser address bar. If you have not configured the router with a different IP address, this will be
`http://192.168.2.1`
You will then see a login window:
- ◆ If a password has already been assigned, enter it and click **LOGIN**.
- ◆ After logging in, select **Security Setup**.

Security Setup takes you through the following steps:

1. Assign configuration password (see page 30)
2. Change the router's SSID (see page 31)
3. Set WEP encryption (see page 33)
4. Set up access control (see page 36)
5. Back up the configuration (see page 39)

Protecting your configuration with a password

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

Step 1 of 5: Set Login-in password

You may set a login password to protect your router configuration. Enter a password (max.32 characters, valid characters: A-Z, a-z, 0-9) and confirm the new password. If you don't want to use a password, keep this input boxes empty.

Please keep the password in mind.

Enter new password:

Confirm new password:

- ◆ Enter a password in the **Enter new password** box and repeat it in the box underneath.
The password must be between 3 and 32 characters long. It is not case sensitive. Avoid names and all too obvious words. Mix letters and numbers.

i

Remember the password that you have assigned. If you ever forget the password you will have to reset your router. This can be done by switching the router off, pressing the reset button on the back and switching the router on again while keeping the reset button pressed. Please bear in mind that this will restore **all** the settings to the factory configuration. No password will be active either.

- ◆ To apply the settings click **NEXT**.

i

Use the following function in Advanced Setup if you want to change the password later on:
Administration – Management

Changing the SSID and disabling Broadcast

A wireless network is defined by giving all the components an identical SSID (Service Set ID). The factory setting for the router's SSID is **ConnectionPoint**. You should change this setting to make sure that nobody can log in to the network unnoticed. You should also prevent the SSID being included in the data packets sent over the network. This could allow persons eavesdropping on the data traffic to gain unauthorised access to your network.

Carry out the following steps:

1. Change the SSID on your router and define that it should no longer be visible.
2. Change the SSID accordingly for all wireless network adapters on all PCs (see page 40).

You will be changing your router's SSID in the next step of Security Setup.

Step 2 of 5: Wireless Network ID (SSID)

You may change the SSID to distinguish your wireless router from others. Max. 32 characters (A-Z,a-z,0-9).

If you change the SSID you have to reconnect your PCs to your wireless router.

Wireless Network ID (SSID) :

You need the SSID, when you connect your PCs to your wireless router.

SSID invisible means, that your router does not broadcast its SSID. Therefore you have to know your SSID if you want to establish a connection to your network.

SSID visibility

☐ visible ☒ invisible

If you set the SSID invisible, keep the SSID in mind !

- ◆ Enter an SSID of your choice. It can be up to 32 alphanumeric characters long. Avoid names and all too obvious words. Mix letters and numbers.

Configuring security features

- ◆ In the **SSID visible** row, select the option **invisible**. This disables the broadcast function for the SSID.
- ◆ To apply the settings click **NEXT**.

i

Use the following function in Advanced Setup if you want to change the SSID later on:

Wireless settings – Basic settings

Once you have completed Security Setup, you have to change the SSID on the wireless network adapters of the connected PCs as well, otherwise they will no longer have access to the router's wireless network. How to do this for a Siemens Gigaset PC Card 54 or Siemens Gigaset PCI Card 54 is described on page 40.

Sending encrypted data

Wireless networks are exposed to the risk of eavesdropping even more than wired networks are. Given the typical ranges of network adapters all the intruder needs is a laptop or PDA (Personal Digital Assistant) with an appropriately configured network card to listen in on any communications over a nearby wireless LAN.

To plug this security gap, WLAN Standard IEEE 802.11 specified an encryption mechanism called **WEP** (Wired Equivalent Privacy) for data encryption and device authentication to a base station (e. g. the Gigaset SE505 dsl/cable).

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



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

To activate WEP encryption on your wireless network components:

1. Activate Web encryption on your Gigaset SE505 dsl/cable and enter a 64- or 128-bit key.

Remember the key you entered!

2. Activate Web encryption on the wireless network adapters and enter the same 64- or 128-bit key (see page 41).

In the following steps we assume that your wireless network has already been set up and is functioning properly.

64- and 128-bit key

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

Setting WEP encryption on the router

In the next step of the Security Setup you will set the WEP encryption on your router.

Step 3 of 5: Set WEP - Key (Wired Equivalent Privacy)

A WEP - Key protects your wireless network against unauthorised access. It's recommended to use a WEP - Key.

Select WEP-Mode ☐ WEP Key 128 Bit ☐ WEP Key 64 Bit ☒ Do not use a WEP Key

Please note: We recommend to use a WEP Key !

- ◆ Select the encryption mode: 64 or 128-bit.

The Web page then has an added section where you can enter the key.

The following illustration shows the page after selecting a 128-bit key.

A WEP Key protects your wireless network against unauthorised access. It's recommended to use a WEP Key.

Select WEP-Mode ☒ WEP Key 128 Bit ☐ WEP Key 64 Bit ☐ Do not use a WEP Key

Enter Input-Mode ☒ Numbers and characters(Hexadecimal) ☐ Characters (ASCII)

Valid characters: 0-9, A-F, 26 characters. This key is needed, when you connect your wireless computers to your router.

Enter WEP-Key

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

If you choose **hexadecimal**, you can use characters **0** to **9** and **A** to **F**.

- With an encryption depth of 64 bits, the key is exactly 10 characters long. An example of a valid key would be: 1234567ABC.
- With an encryption depth of 128 bits, the key is exactly 26 characters long. An example of a valid key would be: 234567ABC8912345DEF1234567.

If you choose **ASCII**, you can use characters **0** to **9** and **A** to **F** and the special characters of the ASCII character set.

- With an encryption depth of 64 bits, the key is exactly 5 characters long.
An example of a valid key would be: GIGA1.
- With an encryption depth of 128 bits, the key is exactly 13 characters long.
An example of a valid key would be: GIGASET_SE505.



- ◆ It is very **important** to make a note of the key you enter. You will need this information to configure the wireless network adapters properly.
- ◆ Do not use the values in this example for your configuration.

- ◆ To apply the settings click **NEXT**.



Use the following function in Advanced Setup if you want to change the WEP key later on:

Wireless settings – WEP mode

Once you have completed Security Setup, you have to change the WEP encryption on the wireless network adapters of the connected PCs as well, otherwise they will no longer have access to the router's wireless network. How to do this for a Siemens Gigaset PC Card 54 or Siemens Gigaset PCI Card 54 is described on (see page 41).

Setting up access control

In the next step of Security Setup you can decide which PCs are to have wireless access to your router and thus to your local network. Access is controlled via the MAC addresses of the PCs' network adapters. These MAC addresses are entered in a MAC access table. Once the access control is activated, only those PCs that are in the table can connect to the Internet. The table can hold up to 16 entries.



If you intend to activate MAC access control, you should enter at least the PC you want to use for configuring the router. Otherwise you will no longer have any access to the router's user interface. You will receive a warning message to that effect.

If you accidentally exclude all PCs from accessing the router, there are two options available:

- ◆ You can completely reset the router. This can be done by switching the router off, pressing the reset button on the back and switching the router on again while keeping the reset button pressed. Please bear in mind that this will restore all configurations to the factory settings.
- ◆ You can connect a PC to the router via one of the LAN sockets. As MAC access control only applies for PCs connected in wireless mode, you can then use the PC for changing the router's configuration.

The default setting for access control is deactivated. That means all the PCs using the correct SSID can register. To retain this setting click **NEXT**.

Step 4 of 5: MAC Access Control

You can define the PCs, which are admitted to your wireless network. The PCs are identified by their MAC-address, which is a unique identifier of the wireless network adapter. For that use the MAC access control list, otherwise don't use it.

MAC access control list: ☒ enable ☐ disable

To activate access control :

- ◆ Select **MAC access table**. The last defined access table will be shown and activated. Only these PCs can now register with the router.
If you are using this function for the first time, you will have to define a MAC access table.

Add A Member To The List :

The new entry will be defined through
☒ List of active booked in devices ☐ MAC Address
Active PC

Device Name	MAC Address	Delete
No member added yet !		

You can do this in two different ways:

◆ Using the list of registered PCs

Use this option if the IP addresses on the local network are assigned by the router's DHCP server and the corresponding PCs are registered.

- In this case, check the **List of active booked in devices** option.
- Then select from the list all the PCs that are to have access and then click **Add to list**.



If you want to add PCs to the table that are not registered at the moment, first deactivate the MAC access table, register all the PCs you want to include in the table with your router and then reactivate the MAC access table.

◆ By direct entry of the MAC address

Use this option if the IP addresses are not assigned by your router's DHCP server but are static or if the PCs you want to include are not registered with the router at the moment.



You can find the MAC addresses of the PCs' wireless network adapters using **MS-DOS prompt** with the command `ipconfig /all` on the PCs in question.

- In this case, check the **MAC address** option.

Configuring security features

The new entry will be defined through

☐ List of active booked in devices ☒ MAC Address

Add A Member To The List :

00 : 90 : 96 : 49 : 3d : ad MAC-Address

my_PC Name (optional)

Add to list

Device Name	MAC Address	Delete
No member added yet !		

- Enter all the MAC addresses of the PCs that are to have access. The table is easier to handle if you assign a name to the PC and then click **Add to list**.

The new entry will be defined through

☐ List of active booked in devices ☒ MAC Address

Add A Member To The List :

: : : : : : : MAC-Address

 Name (optional)

Add to list

Device Name	MAC Address	Delete
my_PC	00:90:96:49:3d:ad	Delete

- ◆ To delete an entry from the table, click **delete** in the right-hand column of the table entry.
- ◆ To apply the settings click **NEXT**.



Use the following function in Advanced Setup if you want to add or change the access control later on:

Wireless settings – Access control

Backing up the configuration

In the final stage of Security Setup you can back up your router settings to a file and store it on your PC or other data medium. All the current settings are backed up, including those you made before e. g. in Basic Setup or Advanced Setup. If needed, you can use this file to restore the current configuration of your router. Backed-up data can be restored using the **Administration – Backup and Restore** menu item in Advanced Setup.

Step 5 of 5: Save Setting

You can save your settings on your PC. If you have in future any problems with your router configuration, you can transfer this configuration file to your router. This function is provided in the advanced configuration menu, backup&restore.

☐ Save configuration to PC

You find further security features, like filter, port forwarding in the advanced setup.

If you have changed the SSID or WEP Key you will now loose the connection to the router. You have to enter the same settings in the utility tool of your wireless connected PC.

- ◆ If you want to back up the current settings, enable **Save configuration to PC**. If you do not want to back up the current configuration, disable this option.
- ◆ Click **FINISH** to close Security Setup.
If you have enabled **Save configuration to PC**, the file download window will appear in your Browser. Enter where you want to save the file.

The Security Setup settings are now active on your router.



Use the following function in Advanced Setup if you want to back up the configuration settings later on:

Administration – Backup and Restore

Security configuration on the network adapters

You now have to configure the factory-set SSID and– if activated–the WEP key for the wireless network adapters in your PCs. Only then can you register with the router again.

Changing the SSID on network adapters

You can use the **Gigaset WLAN adapter monitor** to change the SSID on all wireless network adapters (Gigaset PC Card 54 or Gigaset PCI Card 54)

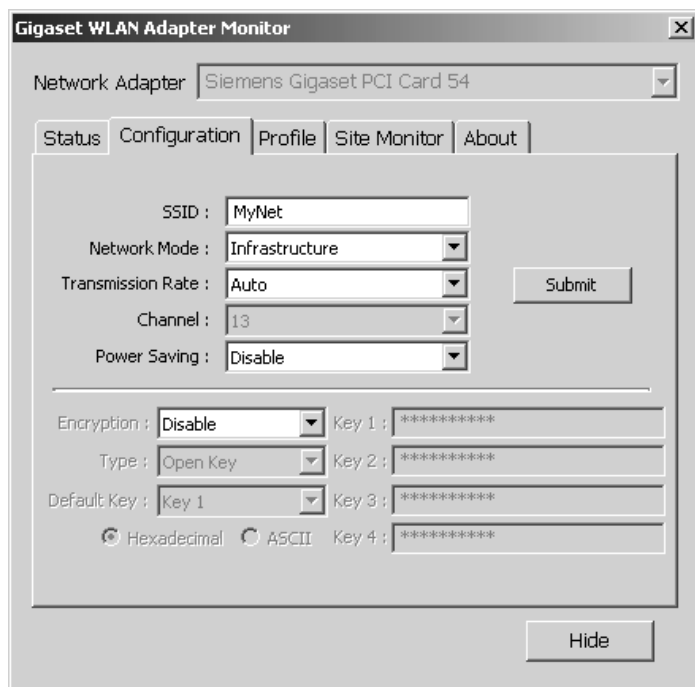
Carry out the following steps:

- ◆ Start the Gigaset WLAN adapter monitor by double clicking on the icon in the taskbar.



The **Gigaset WLAN adapter monitor** is displayed.

- ◆ Open the **Configuration** tab.



- ◆ Enter the same value for the SSID as you assigned to the router.
- ◆ Click **Submit**. This will restore the connection to the router.
- ◆ Click **Hide** to close the window.

Setting WEP encryption on the network adapters

You have to enter the same key as on the router on all the network adapters that will communicate with each other via the Gigaset SE505 dsl/cable.

You can configure the Gigaset PC Card 54 or Gigaset PCI Card 54 using the **Gigaset WLAN adapter monitor**.

To enter the WEP key:

- ◆ Start the Gigaset WLAN adapter monitor by double clicking the icon in the taskbar.



The **Gigaset WLAN adapter monitor** is displayed.

- ◆ Open the **Configuration** tab.

The screenshot shows the 'Gigaset WLAN Adapter Monitor' window with the 'Configuration' tab selected. The 'Network Adapter' dropdown is set to 'Siemens Gigaset PCI Card 54'. The configuration fields are as follows:

- SSID: MyNet
- Network Mode: Infrastructure
- Transmission Rate: Auto
- Channel: 13
- Power Saving: Disable
- Encryption: 128 Bit
- Type: Open Key
- Default Key: Key 1
- Radio buttons: ☒ Hexadecimal, ☐ ASCII
- Key 1, Key 2, Key 3, and Key 4: All set to asterisks (*****).

Buttons: 'Submit' and 'Hide'.

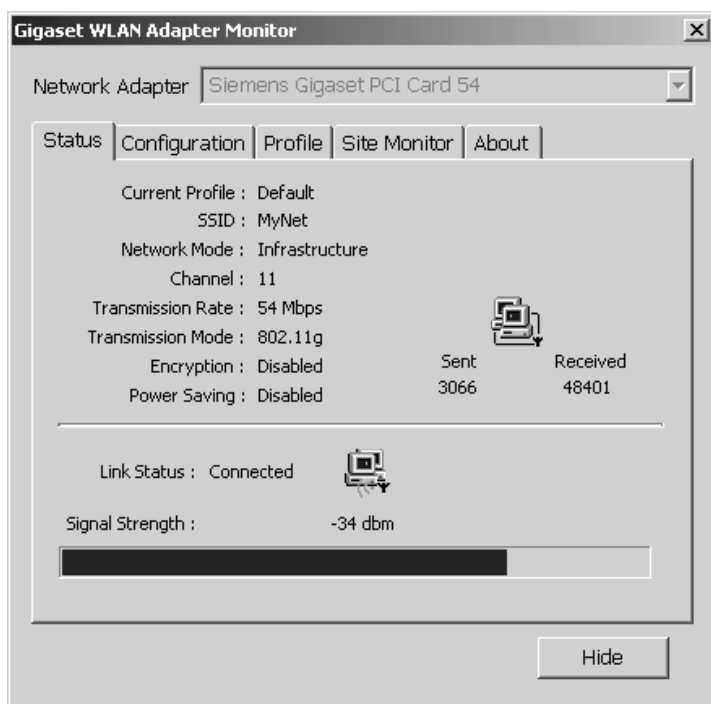
Configuring security features

- ◆ Select from the **Encryption** menu the encryption mode you want (in our example 128 bit). The selection must be the same as on the router.
- ◆ Select one of the four keys as the **default key**.
- ◆ Choose whether you want to assign a hexadecimal or ASCII key. The selection must be the same as on the router.
- ◆ Enter the key you noted when configuring the router in the field for the **default key** you selected.
- ◆ Click **Submit**.



After transmission, the connection may be interrupted for a short time.

- ◆ The **Status** tab will tell you when the connection has been restored.



- ◆ Click **Hide** to close the window.

You have now successfully set up WEP encryption for your network!



If the key you entered on the network adapters does not match the router key, the network adapters will no longer be able to send or receive data to or from the router. If you forgot to make a note of the generated key, for example, you can:

- ◆ Reset the router. This can be done by switching the router off, pressing the reset button on the back and switching the router on again while keeping the reset button pressed. Please bear in mind that this will restore all configurations to the factory settings. Then disable encryption for the network adapter as well and then start from the beginning again.
- ◆ Re-configure the WEP function via a PC with a cable connection to the router.

Internet games

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

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

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

Some applications, such as games on the Internet, require several links, i.e. several ports, so that the players can communicate with each other. In addition, these applications must also be permitted to send requests from other players on the Internet to the player on the local network. These applications cannot work if NAT is active. If you want to use such applications nevertheless, then you will have to set up Port Forwarding for them.

With Port Forwarding (directing requests to certain ports) you order the router to send requests from the Internet for a particular service, in this case a game, to the appropriate port(s) on the PC running the game.

Starting configuration

To start configuration:

- ◆ Launch your Web Browser.
- ◆ Enter the router IP address in the Web Browser address bar. If you have not configured the router with a different IP address, this will be
`http://192.168.2.1`

You will then see a login window:

- ◆ If a password has already been assigned, enter it and click **LOGIN**.
- ◆ After logging in, select **Advanced Setup**.
- ◆ Open the **Virtual server** menu.
- ◆ Select **Virtual server – Port Forwarding**.

Setting up Port Forwarding for games

The following example describes the Port Forwarding configuration for

- ◆ the game "MSN-GAMING-ZONE" on PC "My_PC". The configuration of this game has been predefined and only needs to be applied. The PC must be registered with the router.
- ◆ the game "My_Game" on PC "My_GamesPC". The configuration for this game has not been predefined and so you will have to configure it yourself. The PC is currently not registered with the router.

Setting up Port Forwarding for MSN-GAMING-ZONE

Port-Forwarding

Forwarding is used to provide external access to your local machines. If you want to run a server software on a PC of your local network, you have to forward the according service to that PC.

Port-Forwarding :	☒ Enabled ☐ Disabled			
How do you define the service:	☒ Select predefined services from the list ☐ Define service manually			
Select the service you want to forward:	Predefined services MSN-GAMING-ZONE	Protocol TCP	ext. Port 2300-2	int. Port 2300-2400
				Select PC >>

- ◆ Select **Select predefined services from the list**.
- ◆ Select the predefined game **MSN-GAMING-ZONE** from the selection list. The protocol and external/internal ports are entered automatically.
- ◆ Now select the PC running the game. To do this click **Select PC >>**.

Port-Forwarding :	☒ Enabled ☐ Disabled	
How do you define the PC:	☒ Select the PC from the list. ☐ Select PC manually	
Select the PC:	These PC's are active booked in. My_PC 00:90:96:4b:d6:93	
		<< Back Add to List >>

- ◆ Select **Select the PC from the list**.
- ◆ Select the PC from the list of registered PCs.
- ◆ Click **Add to list**.

Internet games

- ◆ Click **APPLY**. A new entry for the game and the PC will be displayed in the list.

Incoming service		The service will be forwarded to		Details	Delete
Name	ext. Port	PC Name	int. Port		
MAN-GAMING-ZONE	2300-2400	None	2300-2400	Detail	Delete

Setting up Port Forwarding for non predefined games



To configure Port Forwarding you will need the information about the protocol and external/internal ports the application uses. You will find this information in the game documentation or on the vendor's/provider's website.

- ◆ Select **Define service manually**.

Port-Forwarding :	☒ Enabled ☐ Disabled
How do you define the service:	☐ Select predefined services from the list ☒ Define service manually
Select the service you want to forward:	Service name My_Game Protocol ☒ TCP ☐ UDP ext. Port 2611-2612,6500 int. Port 2611-2612,6500 Select PC >>

- ◆ Enter the name of the game and select the protocol.
- ◆ Enter the external port via which messages for this game will be expected. You can specify a block of ports using a dash and several port numbers separated by commas.
- ◆ Enter the internal port(s) to which they are to be forwarded.
- ◆ Now select the PC running the game. To do this click **Select PC>>**.

Port-Forwarding :	☒ Enabled ☐ Disabled
How do you define the PC:	☐ Select the PC from the list. ☒ Select PC manually
Select the service you want to forward:	PC Name (optional) My_GamesPC MAC-Address 00 : 90 : 4d : 3a : 21 : b0 << Back Add to List>>

- ◆ Select **Select PC manually**.
- ◆ Enter the PC's name and MAC address.



You can find the MAC addresses of the PCs' wireless network adapters using **MS-DOS prompt** with the command `ipconfig /all` on the PCs in question.

- ◆ Click **Add to list**.
- ◆ Click **APPLY**. A new entry for the game and the PC will be displayed in the list.

Incoming service		The service will be forwarded to		Details	Delete
Name	ext. Port	PC Name	int. Port		
MAN-GAMING-ZONE	2300-2400	My_PC	2300-2400	Detail	Delete
My_Game	2611-2612,6500	My_GamesPC	2611-2612,6500	Detail	Delete

- ◆ Click **APPLY** again to confirm the new list.

Network conferences with MS Netmeeting

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

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

With Microsoft Netmeeting you can conduct network conferences via the Internet. MS Netmeeting is a complex application that uses several ports or port ranges, dynamically assigned ports and special protocols. In addition, this application must also be permitted to send requests from other participants on the Internet to those on the local network. These application cannot work if NAT is active.

If you want MS Netmeeting to work properly, you can disable the NAT function for this application by configuring the router as a virtual server. Externally the router takes on the role of the server. It receives the requests of remote Netmeeting users under its public IP address and automatically redirects them to the local Netmeeting users.

Starting configuration

To start configuration:

- ◆ Launch your Web Browser.
- ◆ Enter the router IP address in the Web Browser address bar. If you have not configured the router with a different IP address, this will be
`http://192.168.2.1`
You will then see a login window:
- ◆ If a password has already been assigned, enter it and click **LOGIN**.
- ◆ After logging in, select **Advanced Setup**.
- ◆ Open the **Virtual server** menu.
- ◆ Select **Virtual server – Port Forwarding**.

Setting up Port Forwarding for MS Netmeeting

Port-Forwarding :	☒ Enabled ☐ Disabled		
How do you define the service:	☒ Select predefined services from the list ☐ Define service manually		
Select the service you want to forward:	Predefined services	Protocol	ext. Port
	INETMEETING	TCP	1720
			int. Port
			1720
			Select PC >>

- ◆ Select **Select predefined services from the list**.
- ◆ Select the predefined service **NETMEETING** from the selection list. The protocol and external/internal ports are entered automatically.
- ◆ Now select the PC that will be running Netmeeting. To do this click **Select PC>>**.

Port-Forwarding :	☒ Enabled ☐ Disabled	
How do you define the PC:	☒ Select the PC from the list. ☐ Select PC manually	
Select the PC:	These PC's are active booked in.	
	my_PC 00:90:96:3d:a9:08	
	<< Back	Add to List>>

- ◆ Select **Select the PC from the list**.
- ◆ Select the PC from the list of registered PCs.

i

Remember that the PC must be registered with the router. If it is not registered, select **Select PC manually** and enter the PC's name and MAC address (see page 47).

- ◆ Click **Add to list**.

Network conferences with MS Netmeeting

- ◆ Click **APPLY**. A new entry for Netmeeting and the PC will be displayed in the list.

Incoming service		The service will be forwarded to		Details	Delete
Name	ext. Port	PC Name	int. Port		
NETMEETING	1720	my_PC	1720	Detail	Delete

- ◆ Click **APPLY** again to confirm the new list.

Offering your own server on the Internet

If you want to offer files or Web services that are on a PC in your local network to other Internet users, set the PC up as a server (e. g. as FTP or HTTP server). However the normal router configuration does not allow "external" access to PCs on the local network.

To make services available on the Internet from local PCs, you have to

- ◆ set up the router as a virtual server or
- ◆ set up a demilitarised zone (DMZ) for the PC making the service available.

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

If the WAN connection of your local network is supplied with dynamic IP addresses you have to make sure that the service you want to provide can always be reached at the same address on the Internet. This is handled by the dynamic DNS Service (DynDNS). You will find further information in the user guide on the CD-ROM.

Use the **Virtual server** menu to make the settings necessary for offering your services on the Internet. You can

- ◆ set up your router as a virtual server. To do this, you have to set up Port Forwarding (see page 52).
- ◆ open PCs on your local network for general access from the Internet. To do this, you have to set up a demilitarised zone (DMZ) for it (see page 56).

Starting configuration

To start configuration:

- ◆ Launch your Web Browser.
- ◆ Enter the router IP address in the Web Browser address bar. If you have not configured the router with a different IP address, this will be
`http://192.168.2.1`

You will then see a login window:

- ◆ If a password has already been assigned, enter it and click **LOGIN**.
- ◆ After logging in, select **Advanced Setup**.
- ◆ Open the **Virtual server** menu.
- ◆ Select the **Virtual server – Port Forwarding** entry for setting up Port Forwarding or **Virtual server – DMZ** for configuring a DMZ.

Setting up Port Forwarding for Internet servers

Port Forwarding (directing requests to particular ports) is needed if you want to run server services for the Internet on a PC on your local network. For example, you could use one of your PCs to operate a Web server that provides HTML pages. The router, which in this case functions as a virtual server, directs requests from the Internet for an HTML page to the appropriate PC running the Web server.

The following example describes the Port Forwarding configuration for

- ◆ a Web server (HTTP) on PC "My_WebServer". Requests for this service arrive via external port 80 (default port for http service) and are to be redirected to internal port 8080. PC "My_WebServer" is currently registered with the router and can be applied from the list.
- ◆ your own service called "My_Service" on PC "My_ServicePC". The service will be called from the Internet via external port 8181. This port number will also be used for the internal port. The PC "My_ServicePC" is not connected to the router at the moment so it will have to be registered manually.

Setting up Port Forwarding for a Web server

- ◆ Select in the left-hand pane the entry *Virtual server – Port Forwarding*.

Port-Forwarding

Forwarding is used to provide external access to your local machines. If you want to run a server software on a PC of your local network, you have to forward the according service to that PC.

Port-Forwarding :
How do you define the service:

Select the service you want to forward:

Port-Forwarding :
☒ Enabled ☐ Disabled

How do you define the service:
☒ Select predefined services from the list
☐ Define service manually

Predefined services

Protocol

ext. Port

int. Port

HTTP

TCP

80

80

Select PC >>

Incoming service		The service will be forwarded to		Details	Delete
Name	ext. Port	PC Name	int. Port		
No filter defined yet !					

- ◆ Select *Select predefined services from the list*.
- ◆ Select the predefined service **HTTP** from the selection list. The protocol and external port are entered automatically.

52

- ◆ Specify the internal port number to which requests for the service are to be directed. The Web server has been configured so that it reacts to requests on port 8080. The requests for Web pages however arrive on port 80 (default). If you now include the PC in the forwarding table and define port 80 as the external and port 8080 as the internal port, then all the requests from the Internet for the service with port number 80 will be redirected to the Web server of the PC you defined with port 8080.
- ◆ Now select the PC running the service. To do this click **Select PC>>**.

Port-Forwarding :	☒ Enabled ☐ Disabled
How do you define the PC:	☒ Select the PC from the list. ☐ Select PC manually
Select the PC:	These PC's are active booked in. My_WebServer 00:90:96:4b:d6:93 << Back Add to List >>

- ◆ Select **Select the PC from the list**.
- ◆ Select the PC from the list of registered PCs.
- ◆ Click **Add to list**.
- ◆ Click **APPLY**. A new entry for the service and the PC will be displayed in the list.

Incoming service		The service will be forwarded to		Details	Delete
Name	ext. Port	PC Name	int. Port		
HTTP	80	My_WebServer	80	Detail	Delete

Offering your own server on the Internet

Setting up Port Forwarding for your own services

- ◆ Select **Define service manually**

Port-Forwarding :	☒ Enabled ☐ Disabled
How do you define the service:	☐ Select predefined services from the list ☒ Define service manually
Select the service you want to forward:	Service name My_Service
	Protocol ☒ TCP ☐ UDP
	ext. Port 8181
	int. Port 8181
Select PC >>	

- ◆ Enter the name of the service, select the protocol and specify the external port on which messages for this service are expected and the internal port they are to be redirected to.



You can specify a block of ports using a dash (e. g. 8181-8185) and several port numbers separated by commas (e. g. 8181,8185).

- ◆ Now select the PC running the service. To do this click **Select PC>>**.

Port-Forwarding :	☒ Enabled ☐ Disabled
How do you define the PC:	☐ Select the PC from the list. ☒ Select PC manually
Select the service you want to forward:	PC Name (optional) My_ServicePC
	MAC-Address 00 : 90 : 3b : 5c : 41 : f0
<< Back Add to List >>	

- ◆ Select **Select PC manually**.

- ◆ Enter the PC's name and MAC address.



You can find the MAC addresses of the PCs' wireless network adapters using **MS-DOS prompt** with the command `ipconfig /all` on the PCs in question.

- ◆ Click **Add to list**.
- ◆ Click **APPLY**. A new entry for the service and the PC will be displayed in the list.

Incoming service		The service will be forwarded to		Details	Delete
Name	ext. Port	PC Name	int. Port		
HTTP	80	My_WebServer	80	Detail	Delete
My_Service	8181	My_ServicePC	8181	Detail	Delete

- ◆ Click **APPLY** again to confirm the new list.

Setting up demilitarised zones for servers

By default access from the Internet to PCs on the local network is not permitted. The router shields the local network with a firewall. Some applications cannot work properly behind a firewall. In this case you can open **one** PC for unrestricted Internet access in both directions. You define a so-called demilitarised zone (DMZ) for this PC. If you define a DMZ, all the requests from the Internet for a service will be redirected to that PC if the service in question has not already been redirected to another PC via Port Forwarding (see page 52).



A PC in such a demilitarised zone is freely accessible for the Internet and thus may constitute a security risk for your local network.

To set up a DMZ:

- ◆ Select in the left-hand pane the entry *Virtual server – DMZ*

DMZ (demilitarized zone)

If you define one PC as a DMZ - host, all ports are forwarded to this PC. If a port is already defined in the port forwarding, this port is forwarded to the PC defined in the forwarding list. Think about security, if you want to use DMZ.

DMZ :	☒ Enabled ☐ Disabled
How do you define the PC:	☒ Select the PC from the list. ☐ Select PC manually
Select the PC:	These PC's are active booked in. My_ServicePC 00:90:96:4b:d6:93 ▾ Add to List>>

Incoming service	The service will be forwarded to	Details	Delete
No List entry defined yet !			

- ◆ Select **DMZ**. If no DMZ has been defined (no entry in the table), you will now have to select a PC for the DMZ.
- ◆ Select the PC you want to use. There are two ways of doing this: You can
 - **Select the PC from the list**
 - **Select PC manually**

- ◆ Select one of the registered PCs from the list or enter the PC's name and MAC address.



You can find the MAC addresses of the PCs' wireless network adapters using **MS-DOS prompt** with the command `ipconfig/all` on the PCs in question.

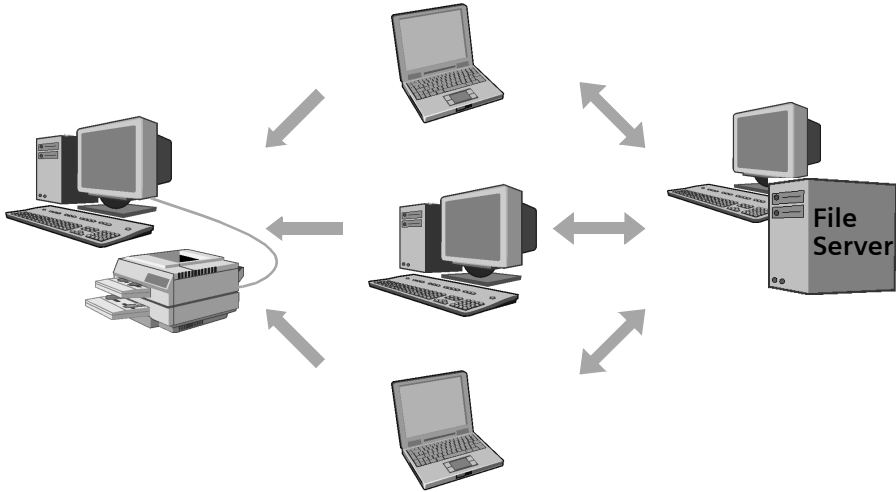
- ◆ Click **Add to list**. The entry for the PC will be shown in the table. Any existing entry will be overwritten by the new one.

Incoming service	The service will be forwarded to	Details	Delete
ALL	My_ServicePC	Detail	Delete

- ◆ Click **APPLY** if you want to apply these settings for the router configuration.

Sharing files and printers

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 the steps for sharing files or printers on the network. 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.
- ◆ Users who want to access the files or printer have to make them available on their PC.

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



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 of where you can find which information in this chapter.

	Windows 98	Windows XP	Windows 2000
Set up a network	page 59	page 80	page 98
Release your own files	page 68	page 86	page 106
Release your own printers	page 70	page 88	page 110
Set up user IDs	page 71	page 89	page 103
Use files on other PCs	page 74	page 92	page 111
Use printers on other PCs	page 77	page 95	page 115

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 59).
2. Select computer names and workgroup (see page 62).
3. Select type of access control (see page 62).
4. Set TCP/IP protocol (see page 63).
5. Install utilities for file and printer release (see page 66).
6. Release files and printer (see page 68).

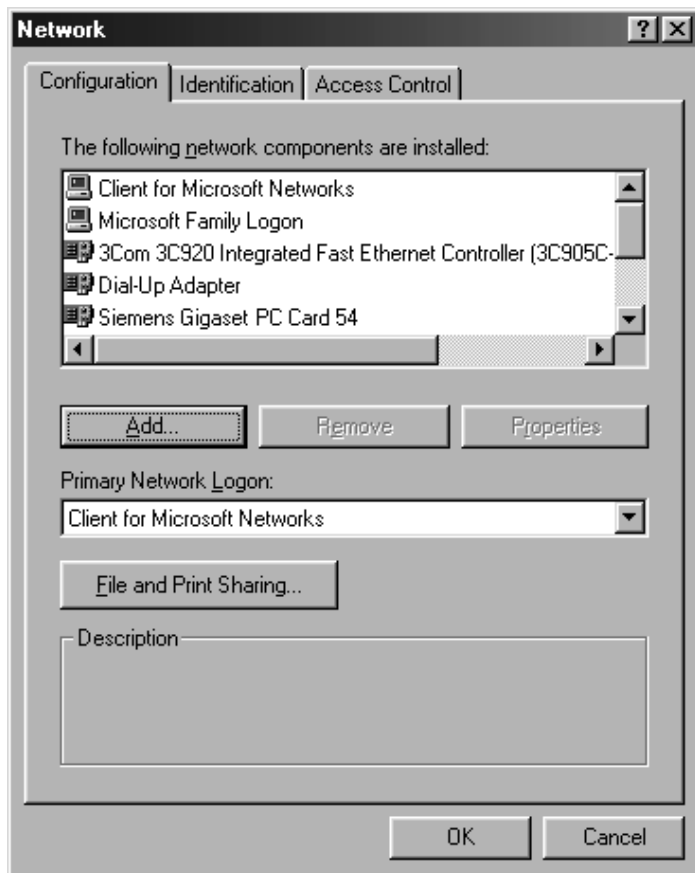
Setting up a PC as Client for Microsoft Networks

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**.

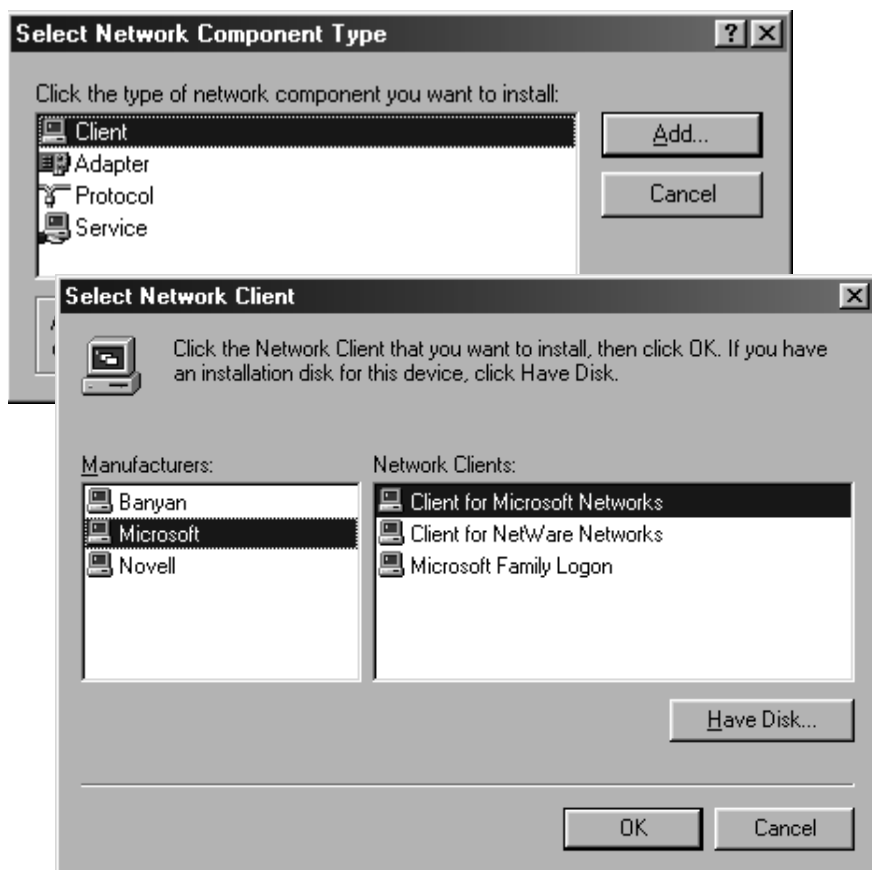
Sharing files and printers

- ◆ Check whether the list of components contains the entry **Client for Microsoft Networks**.



If the entry exists, please continue from page 62.

- ◆ 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

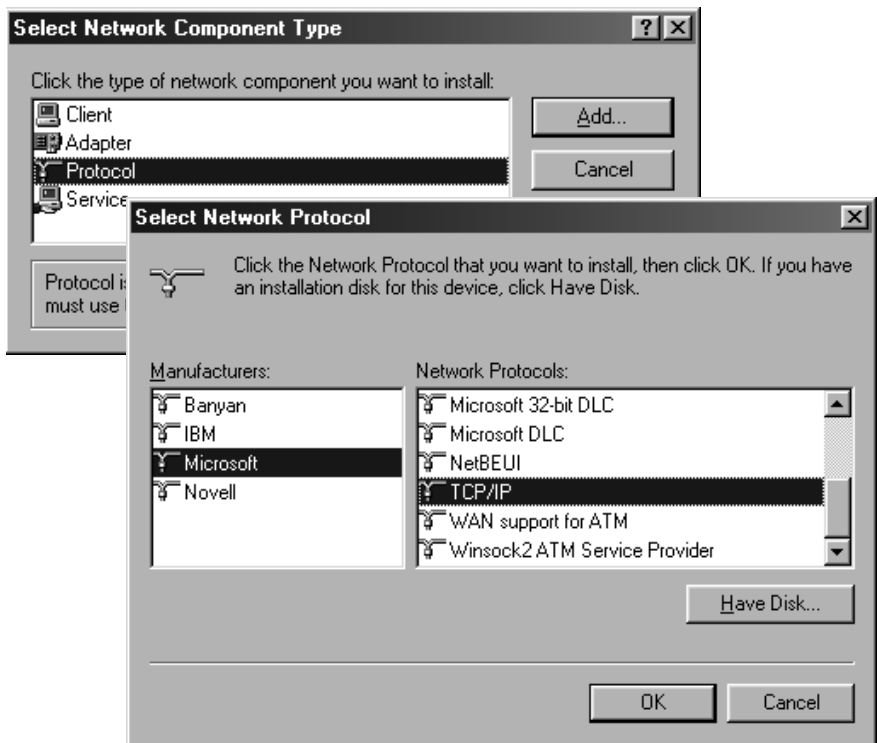
The TCP/IP protocol ensures that the PCs on the network can communicate with each other. This protocol requires certain settings which you will now make so that it can function smoothly.

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 PCI Card 54 as the wireless network adapter, the list must contain the entry **TCP/IP > Siemens Gigaset PCI Card 54**.

If the entry for your network card or network adapter is there, please turn to page 64.

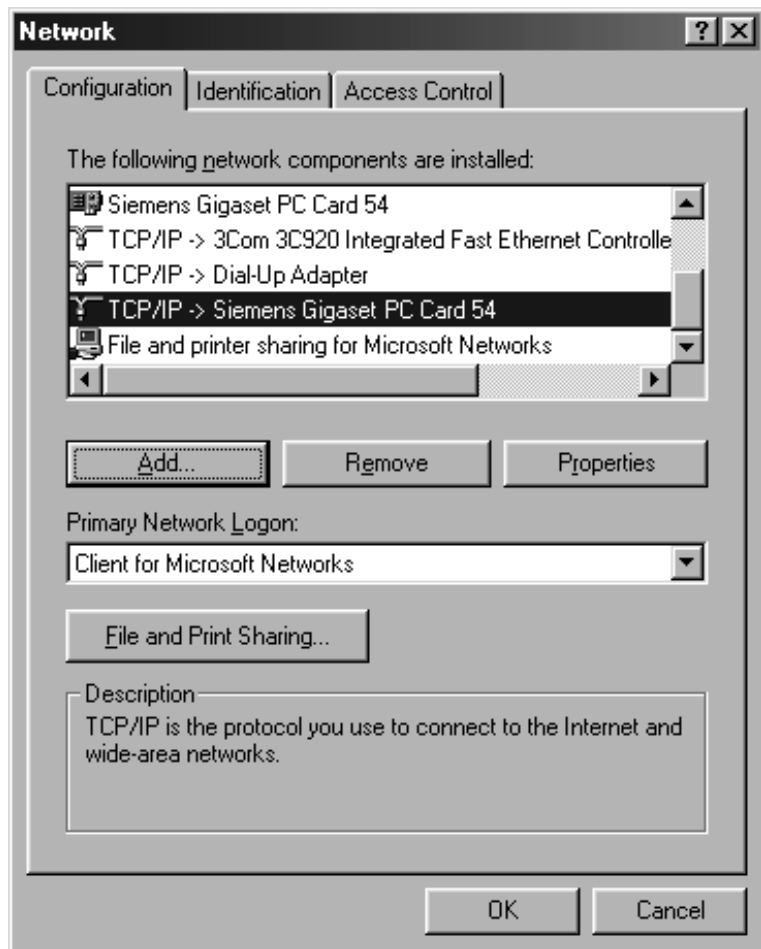
- ◆ If the entry does not exist, click **Add**.



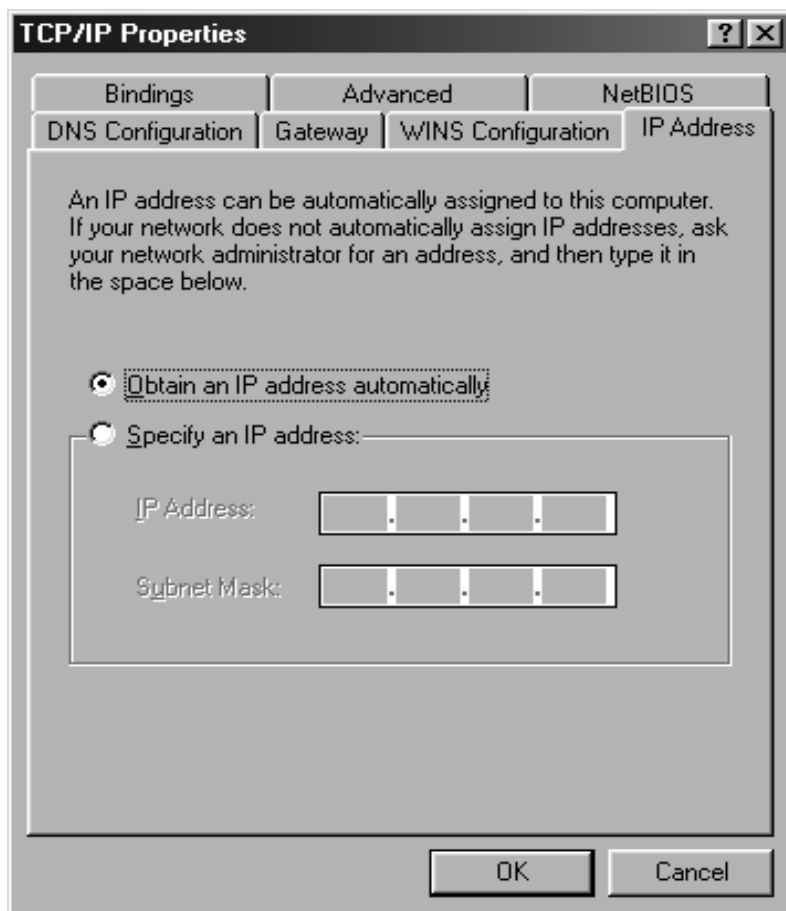
- ◆ Select as network component type **Protocol** and click **Add**.
- ◆ Select in **Manufacturers** the entry **Microsoft** and in **Network protocol** the entry **TCP/IP** before confirming with **OK**.

Setting the TCP/IP protocol

- ◆ 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**.



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 in the Appendix from page 117.

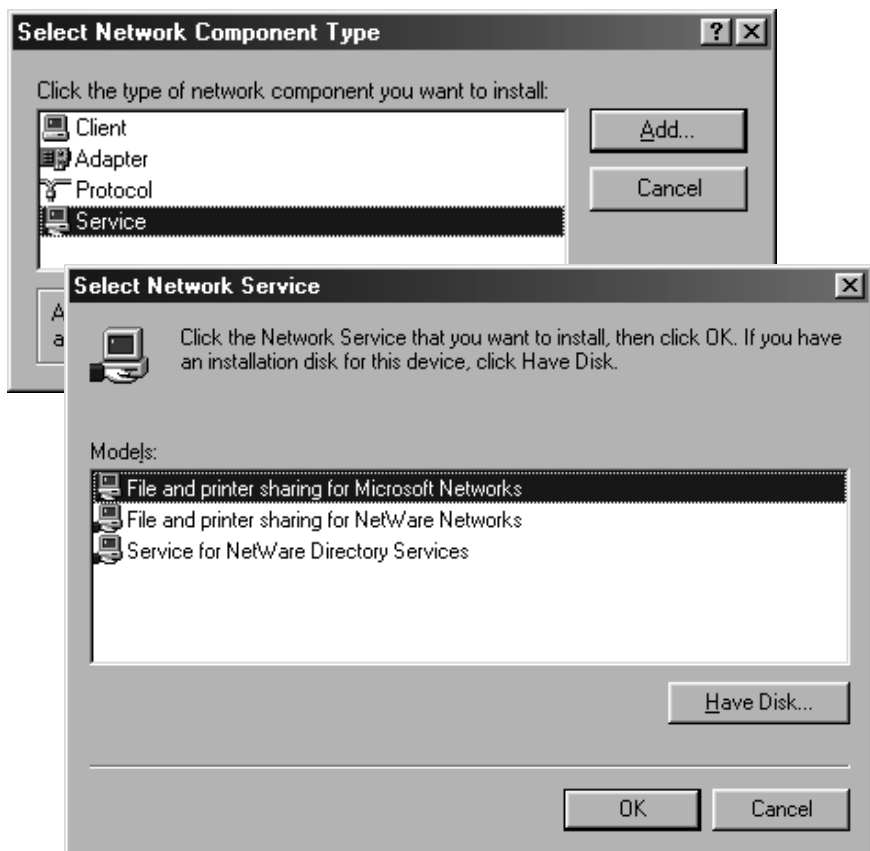
Installing utilities for file and printer release

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**.

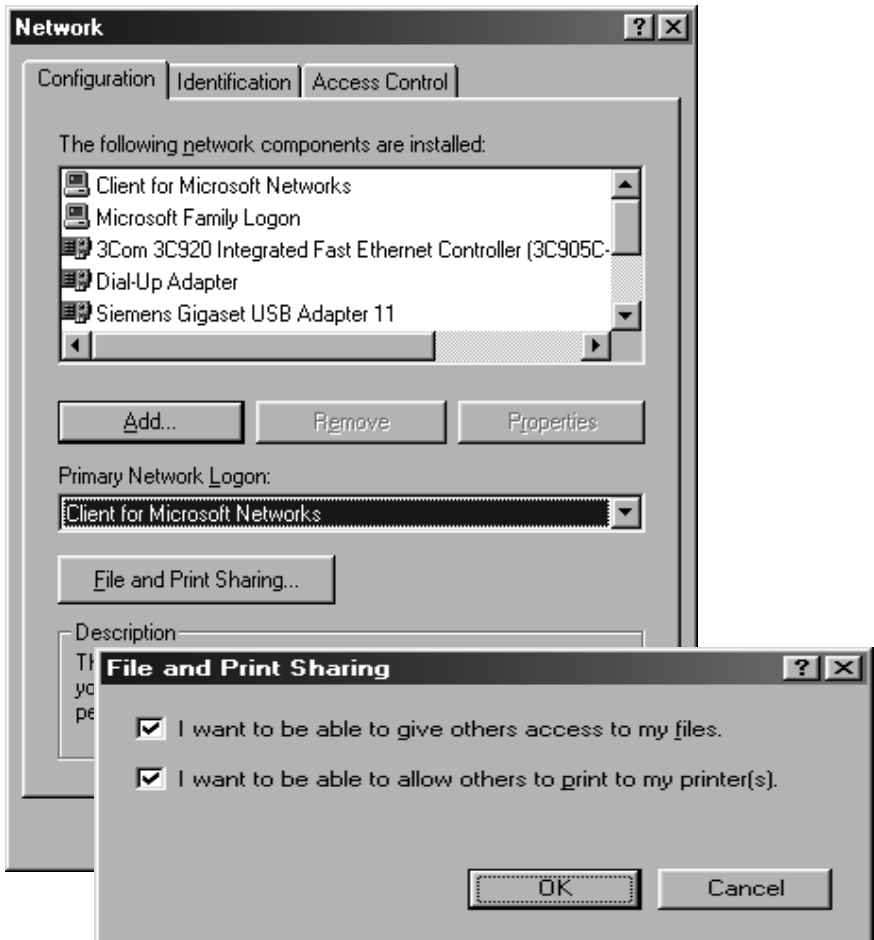
If the entry exists, please continue from page 67.

- ◆ 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**.

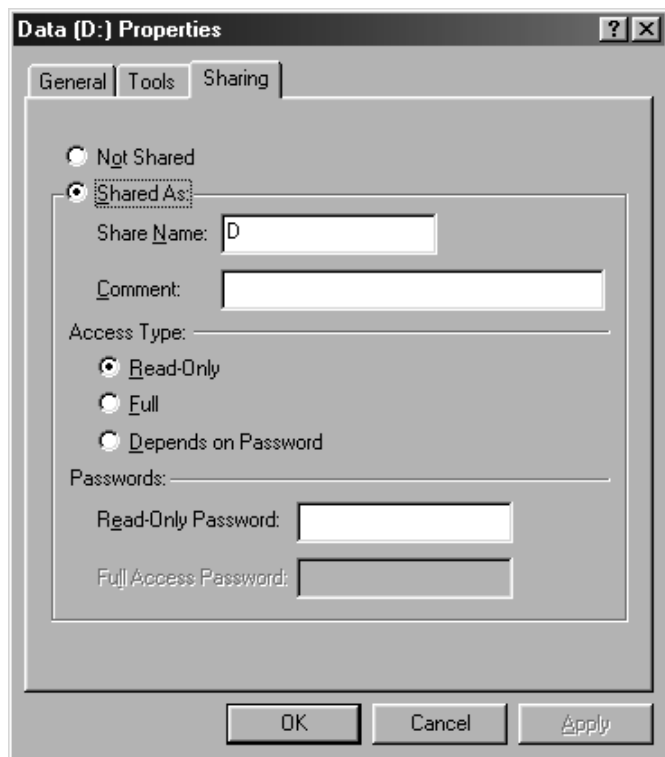
You will now need the Windows installation CD. Windows will copy some files from the installation CD before prompting you to reboot your computer. Then the network is ready for use.

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:

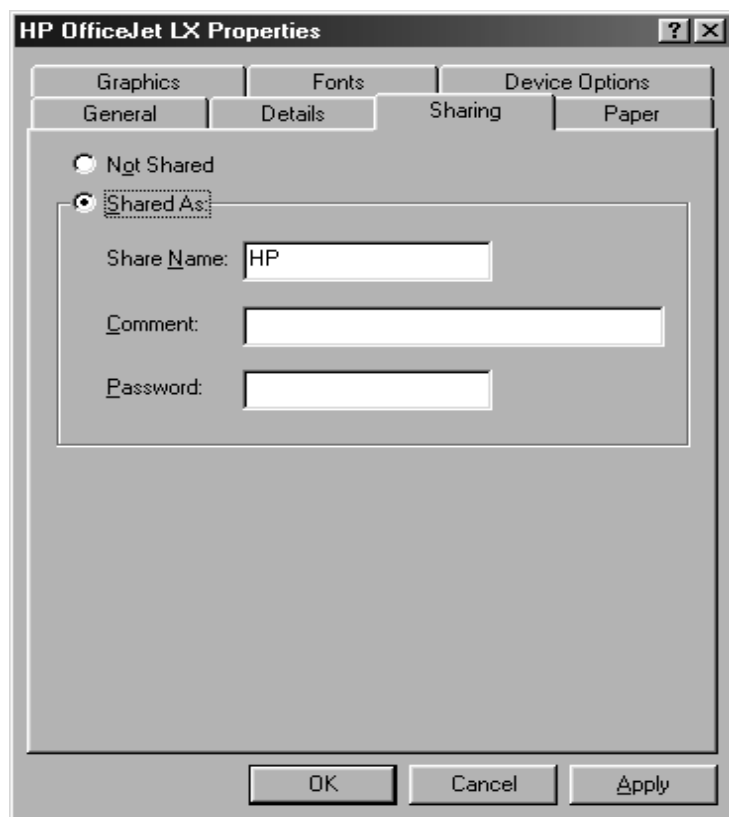
<i>Read only:</i>	If you want to allow other users to open and read documents but not edit or delete them.
<i>Full:</i>	If you want to allow other users to edit, add or delete files.
<i>Depends on password:</i>	If you want to grant various users different access rights.

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

Sharing files and printers

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.



- ◆ 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 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.

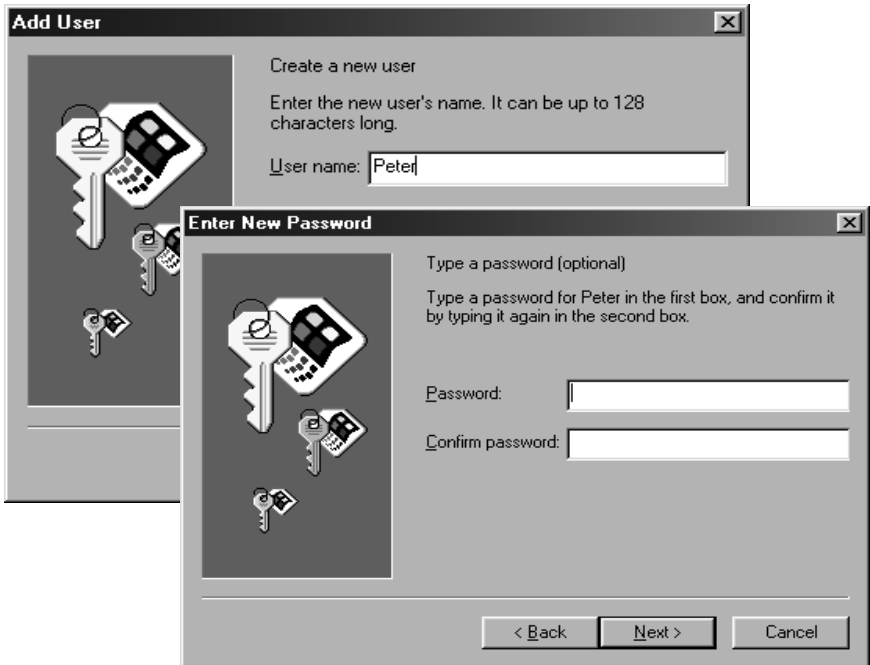


If the resource you want to use on your PC is on a Windows 2000 system then you have to set up user IDs for all the users who are to have access. The same user IDs have to be entered as on the releasing system.

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**.



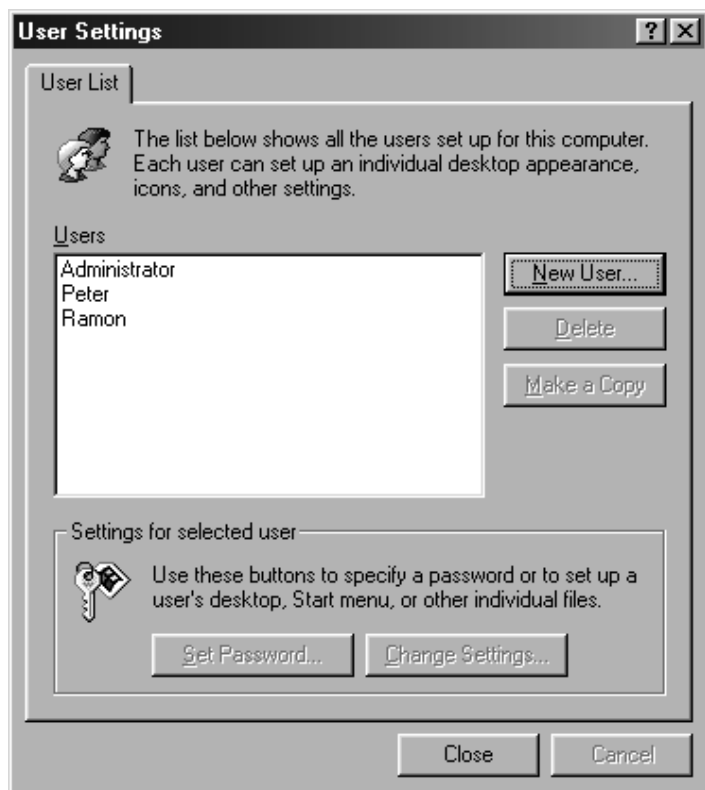
- ◆ Enter a user name and click **next**.
- ◆ Enter a password, repeat it and click **next**.

Sharing files and printers

- ◆ 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 75).
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 76).
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.

i

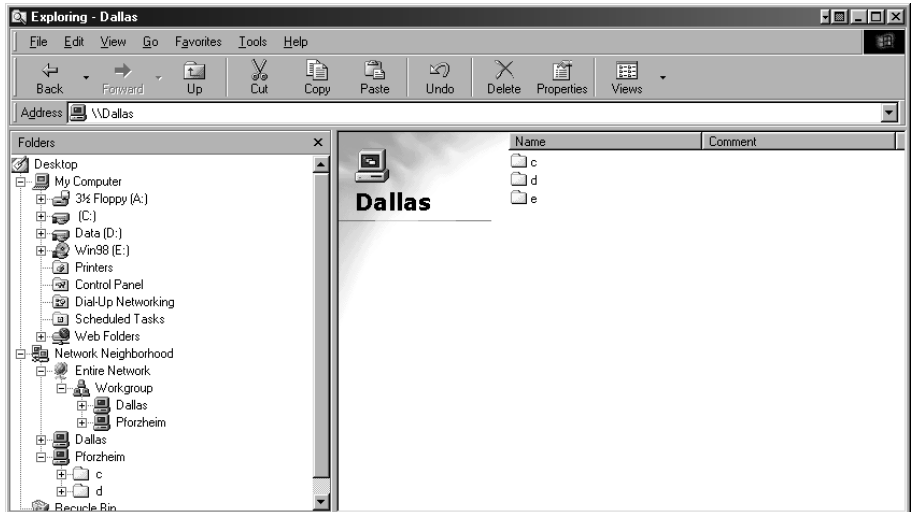
Please bear in mind that drives or folders can be hooked on to several PCs at the same time and thus accessed by other users. Most applications (e. g. word processing software) lock files once they have been opened. This prevents inconsistent data pools. If you cannot open a file because it is locked, 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:



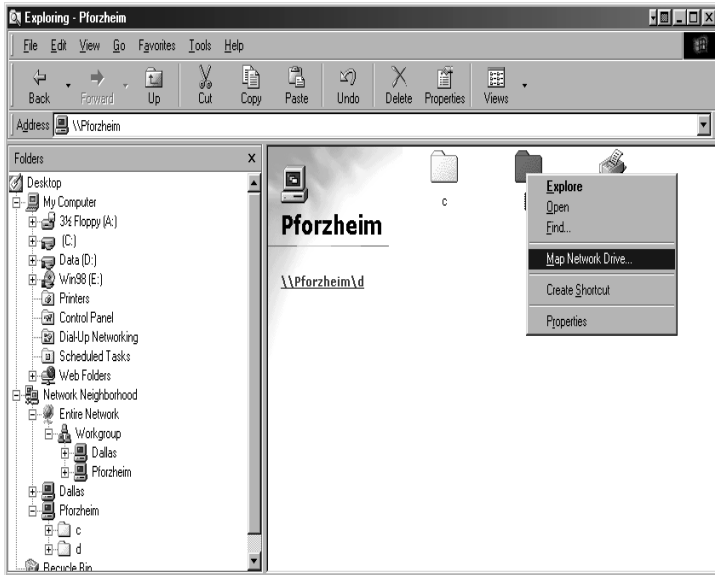
Clicking a PC name shows the released drives and folders on this PC under the name assigned when they were released. You can navigate through the file system in the usual Windows Explorer way by clicking a drive or folder and then opening other branches of the file tree.

Sharing files and printers

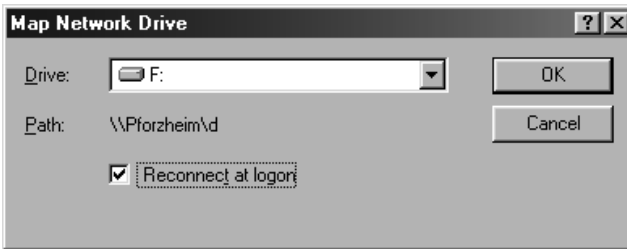
Hooking external files on to your own file system

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**.
- ◆ 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**.

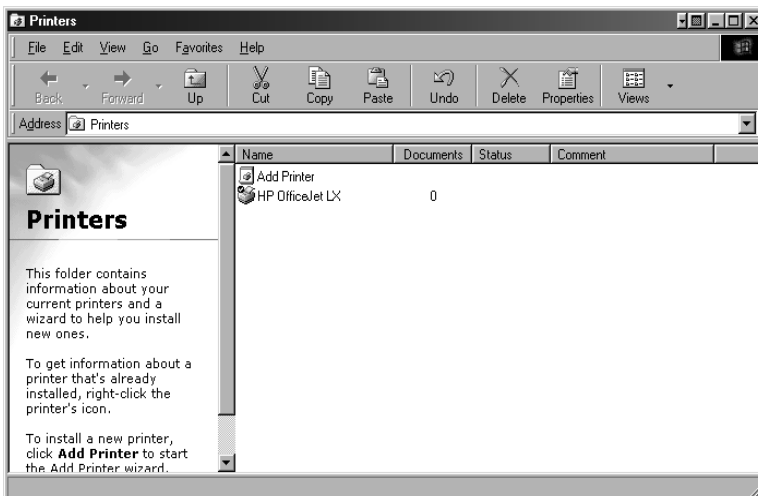


- ◆ Select the drive name under which the remote drive is to be hooked on to your PC. The next free drive will be prompted. If you select the option **Reconnect at login**, Windows will hook the drive on every time you start your PC, provided the remote PC is running.
- ◆ Now open the desktop. The remote 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:

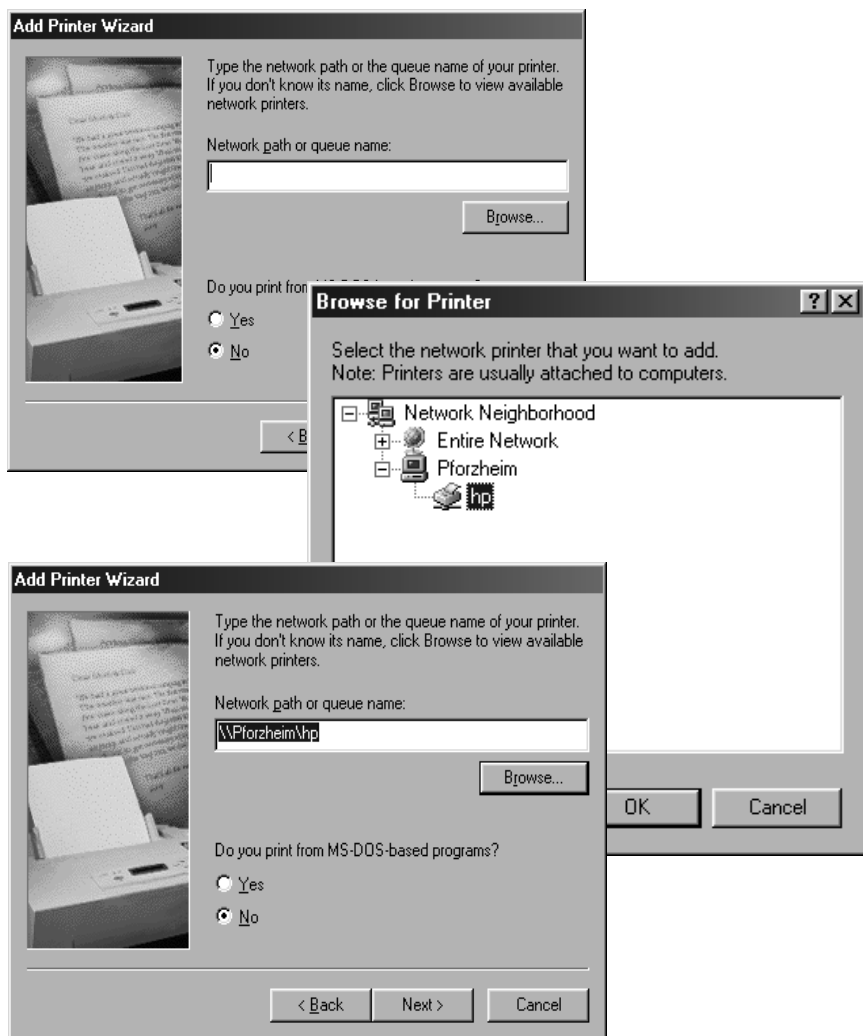
- ◆ Open the printer manager with **Start – Settings – Printers**



- ◆ Double-click the **Add printer** icon. This opens the printer installation wizard.
- ◆ Click **next**.

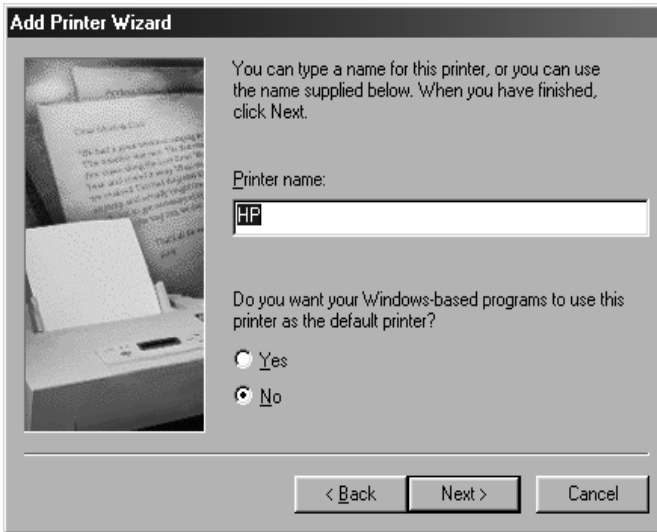
Sharing files and printers

- ◆ In the next window select **Network printer**.
- ◆ Click **next** again.
- ◆ 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**.

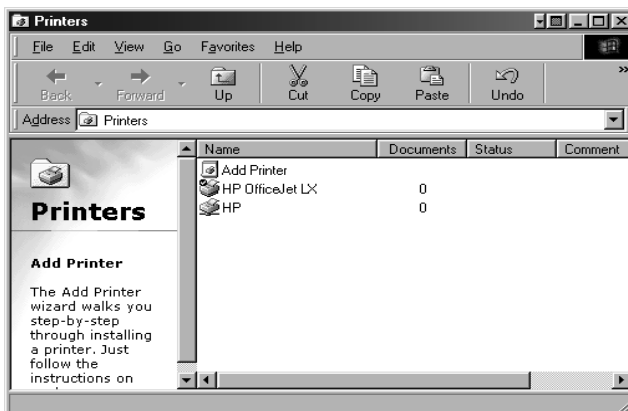


- ◆ The printer will now be displayed. Click **next**.

- ◆ 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.



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 83).
3. Accept network settings (see page 84).
4. Close installation procedures (see page 85).
5. Release files and printer (see page 86).

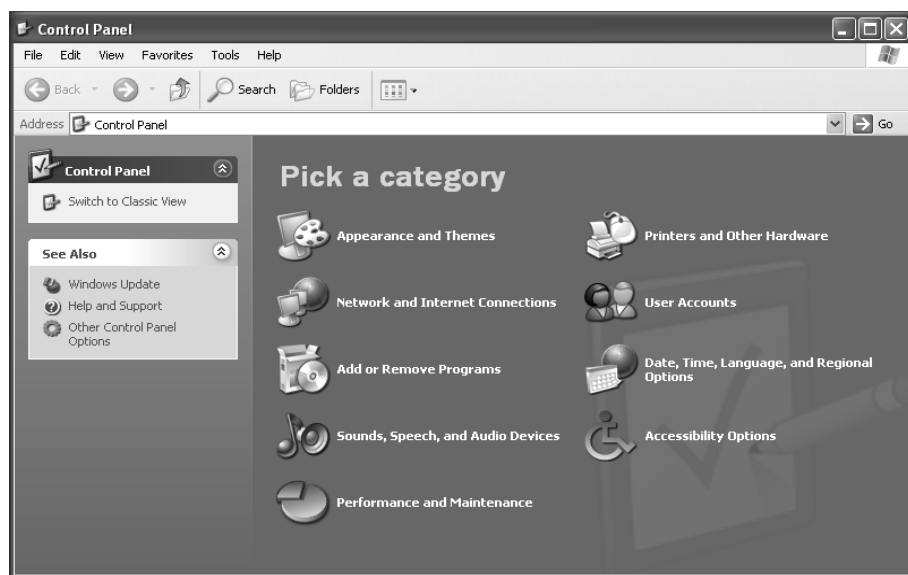
Configuring the network

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

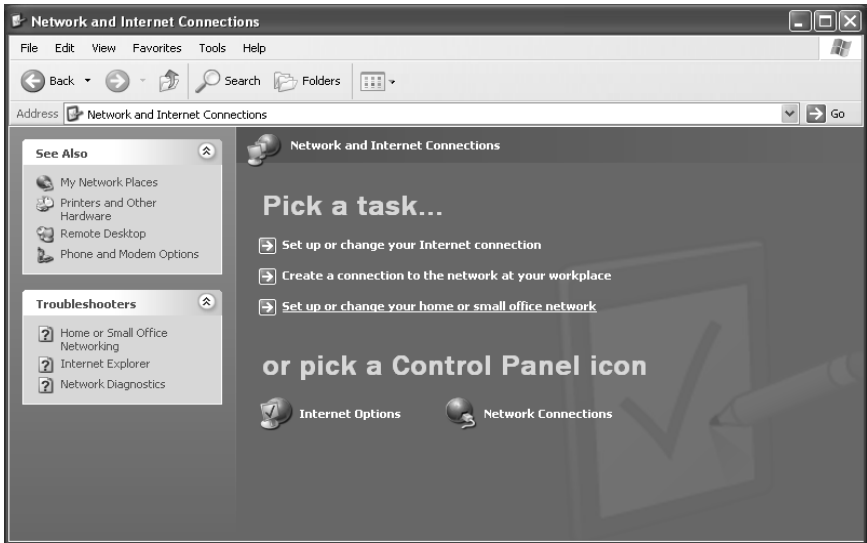
Launching the network wizard

Launch the network wizard as follows:

- ◆ Open the **Control Panel** and then **Network and Internet Connections**.



- ◆ 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 computer is to belong to. This name must be identical for all the PCs on 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...
Learn more...

Network Setup Wizard

Name your network.

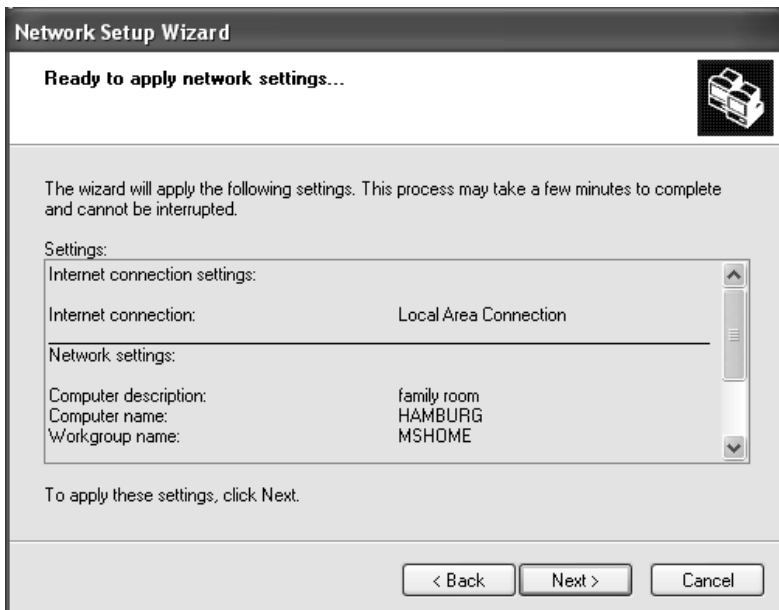
Name your network by specifying a workgroup name below. All computers on your network should have the same workgroup name.

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 this your "home network" will have been installed.

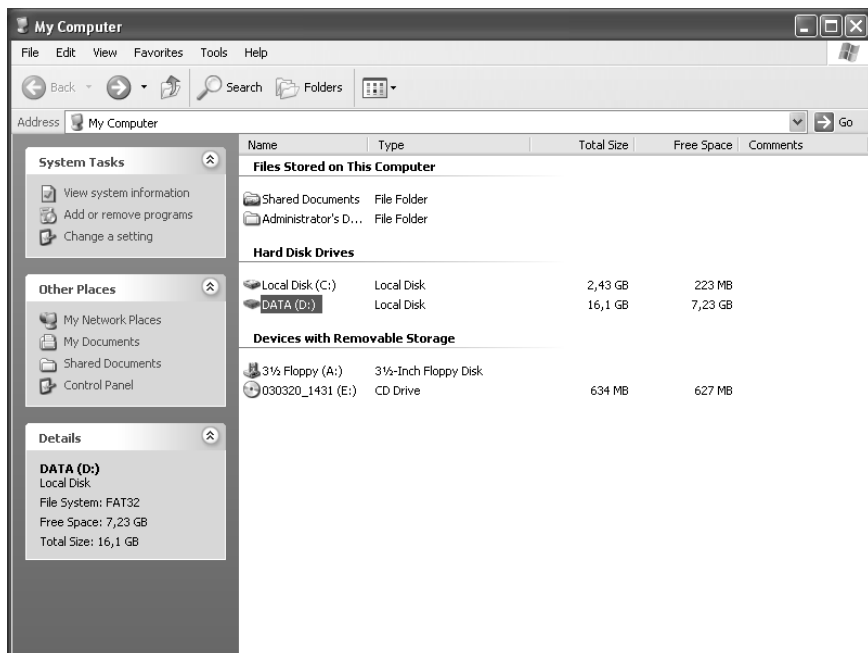
To set up the network on the other PCs with the same settings, insert the disk in the drive and run ***Netsetup*** with a double click.

Releasing files and printers

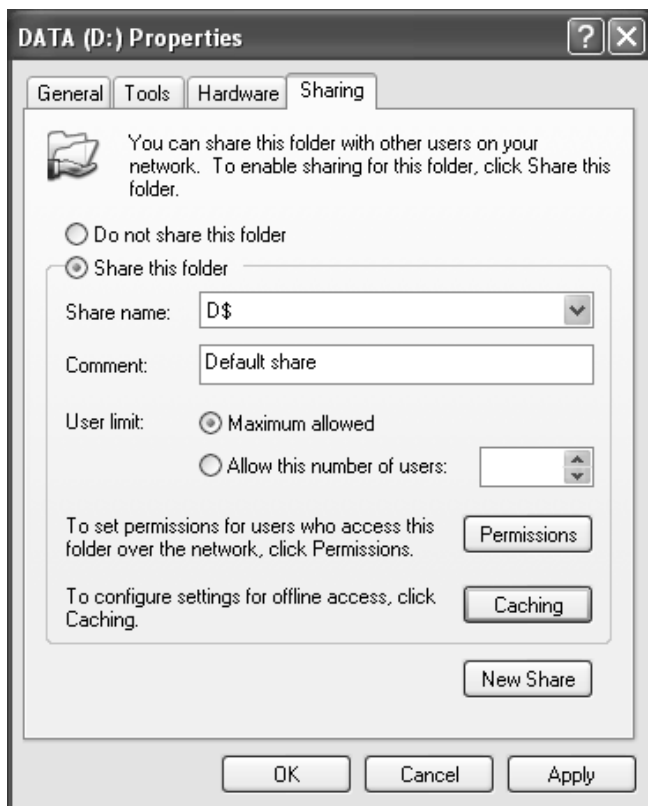
You can now release files and printers on your PC for other users on the network.

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**.



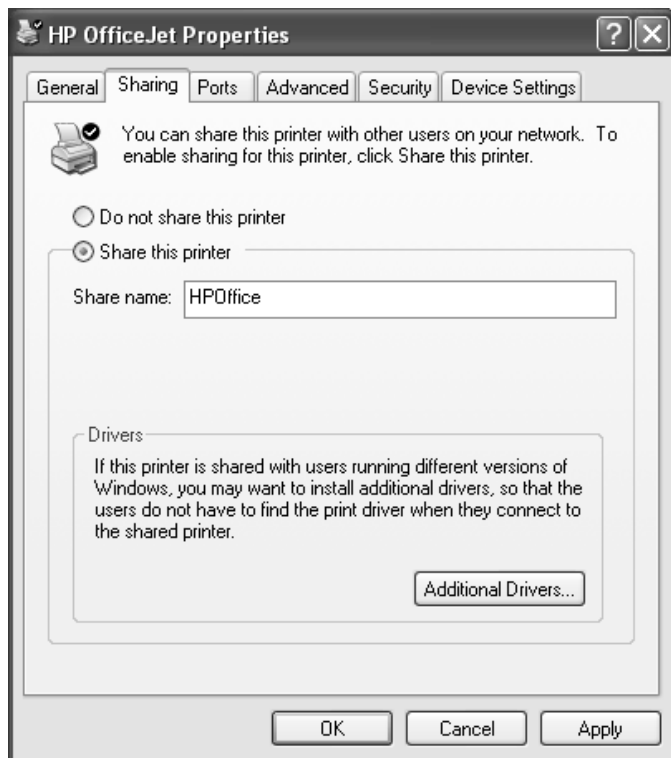
- ◆ Finally assign a **Share name**. From now on, your drive or folder will appear on the network under this name.
- ◆ Use **Apply** to save the current settings. Click **OK** to close release configuration. If a hand now appears below your folder or drive on the Desktop then you have configured everything correctly.

Sharing files and printers

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.

Using files and printers on the network (Windows XP)

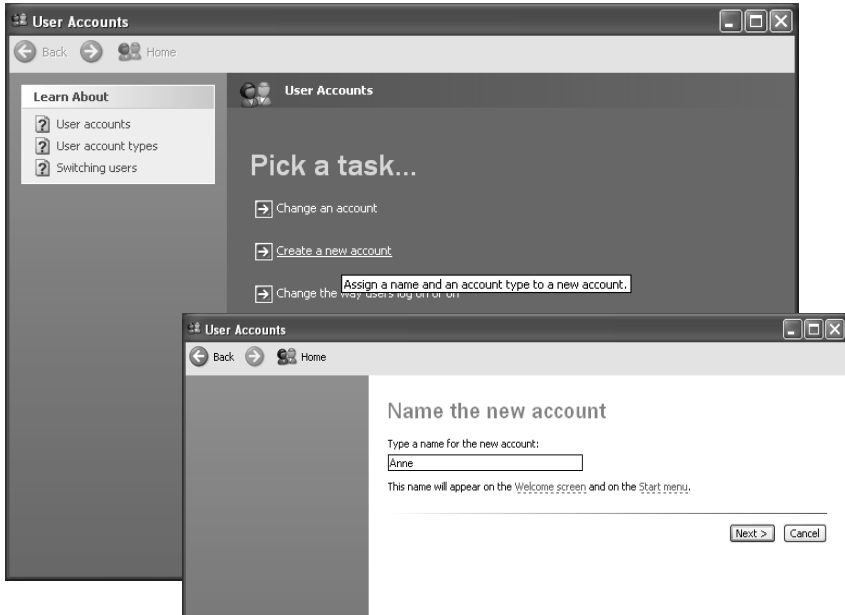
You can use resources on your PC such as files and printers that have been made available by other PCs.

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:

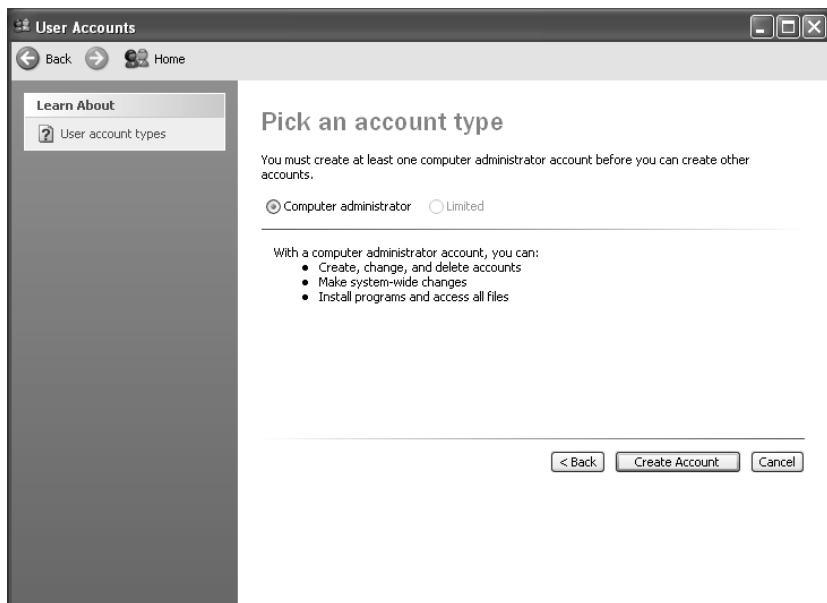
- ◆ Open the **Control Panel** and then **User accounts**.



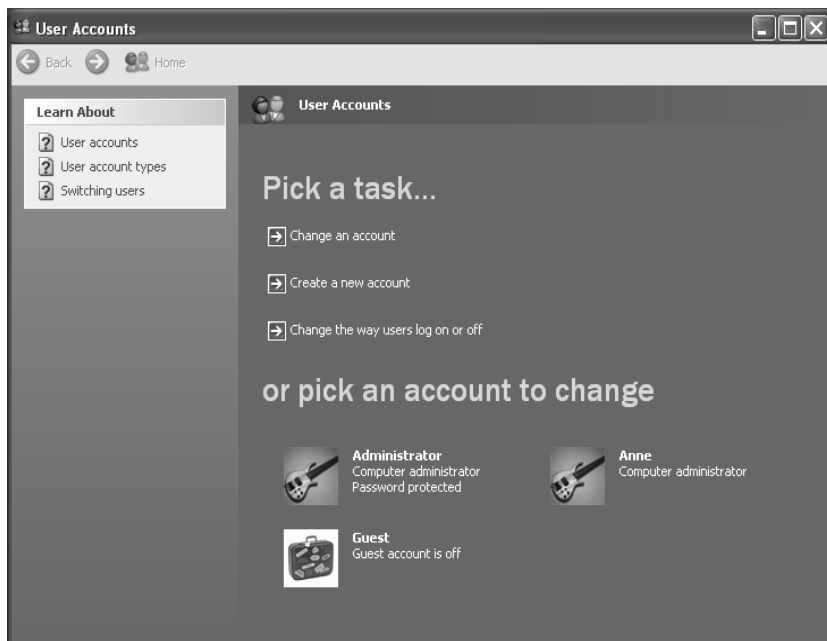
- ◆ Select **Create new account**.
- ◆ Enter a name for the user.
- ◆ Click **next**.

Sharing files and printers

- ◆ 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.



- ◆ 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 'Back' and 'Home' buttons. 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 EFS-encrypted files, personal certificates, and stored passwords for Web sites or network resources.**' followed by 'To avoid losing data in the future, ask Anne to make a password reset floppy disk.' There are two password input fields: 'Type a new password:' and 'Type the new password again to confirm:'. Both fields show six dots. Below them is a note: 'If the password contains capital letters, they must be typed the same way every time.' Then there is a 'password hint' field with the text 'Type a word or phrase to use as a password hint:'. At the bottom right are 'Create Password' and 'Cancel' buttons.

- ◆ 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:

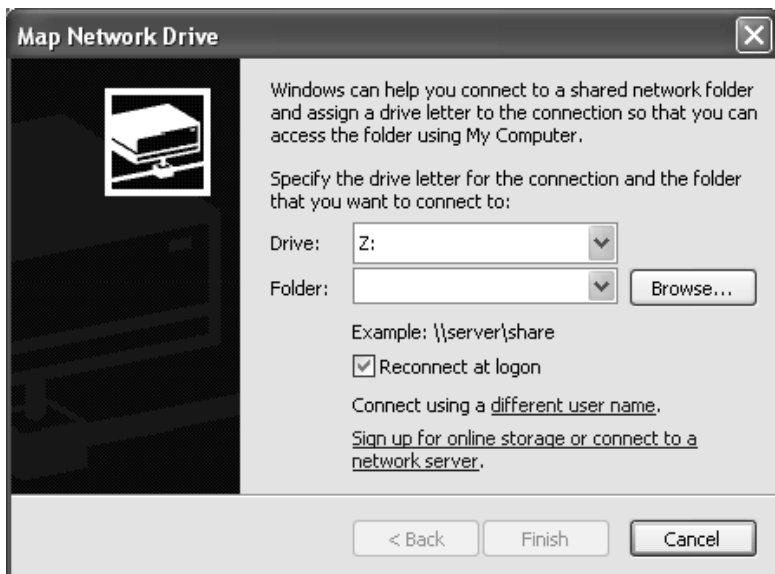
- ◆ via the My NetworkPlaces of your PC (see page 75).
You should choose this alternative if for example you want to copy files or folders from another PC to your own or vice versa.
- ◆ by hooking on to your PC's file system (see page 93).
You should choose this alternative if you want to work directly 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.

i

Please bear in mind that drives or folders can be hooked on to several PCs at the same time and thus accessed by other users. 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**.

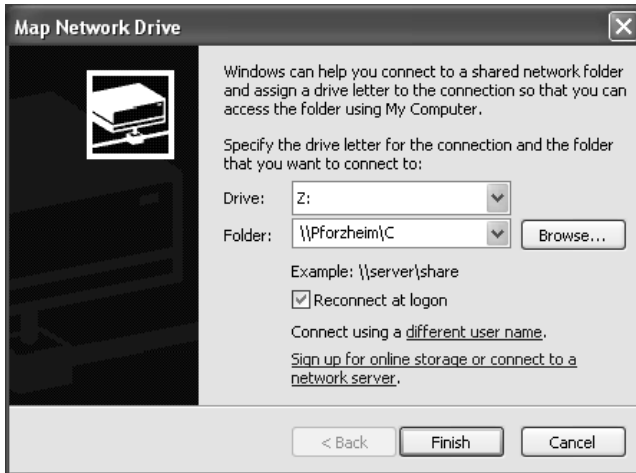


- ◆ Select the drive name under which the remote drive is to be hooked on to your PC.
- ◆ Enter a name under which the drive or folder is to be released for the network. To do this click **Browse**. This will open a screen in which you can search the network environment.



Sharing files and printers

- ◆ 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:

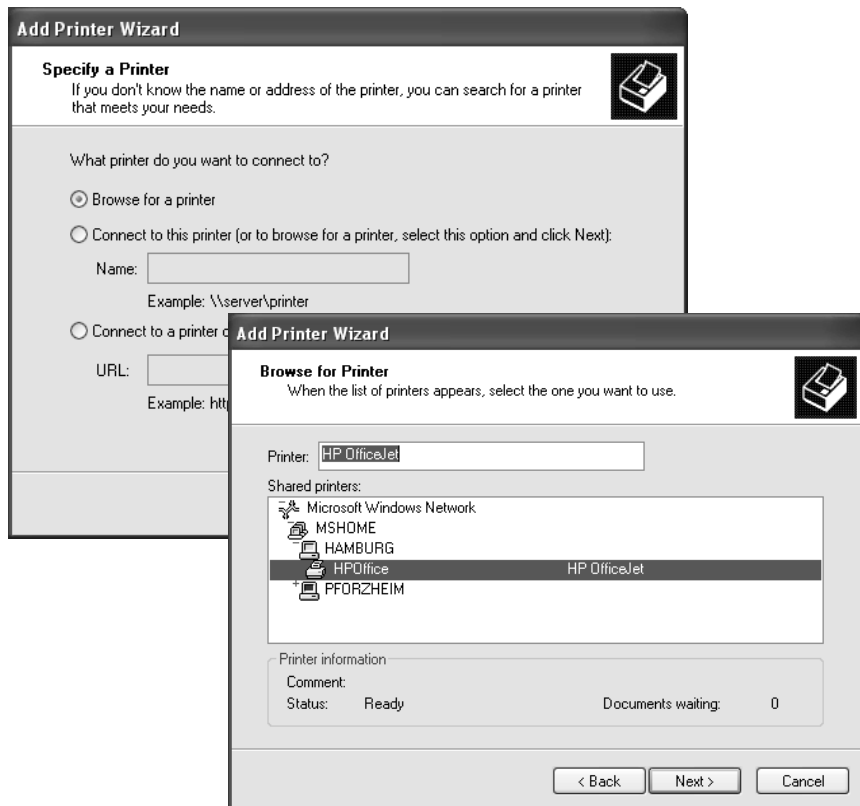
- ◆ Open the printer manager with **Printers and Faxes** in the Start menu.



- ◆ 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.

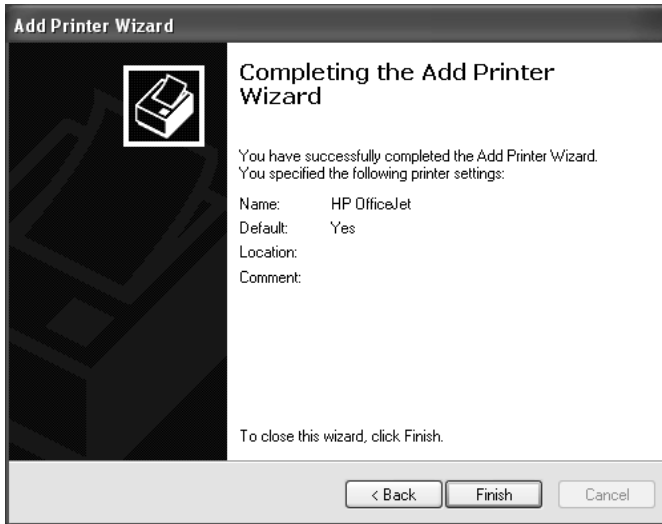
Sharing files and printers

- ◆ Select **Browse for a printer** to look for the printer on the network.
- ◆ 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.

Making your own files and printers available (Windows 2000)

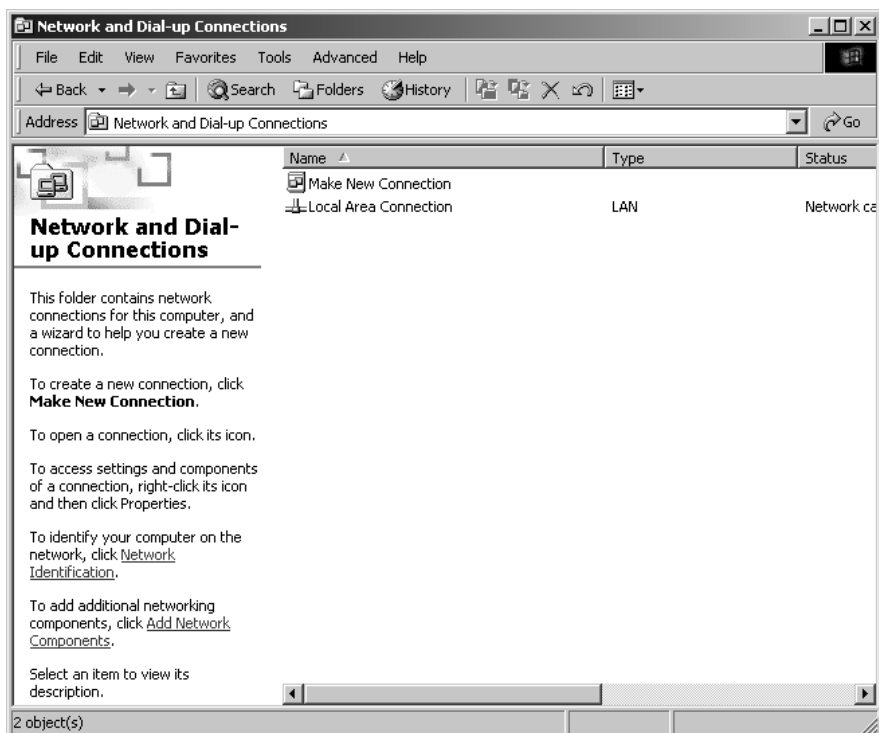
To release files or printers on a PC with Windows 2000 for other users on the network:

1. Install the network services (see below).
2. Select computer names and workgroup (see page 100).
3. Set TCP/IP protocol (see page 101).
4. Set up users (see page 103).
5. Release files and printer (see page 106).

Installing network services

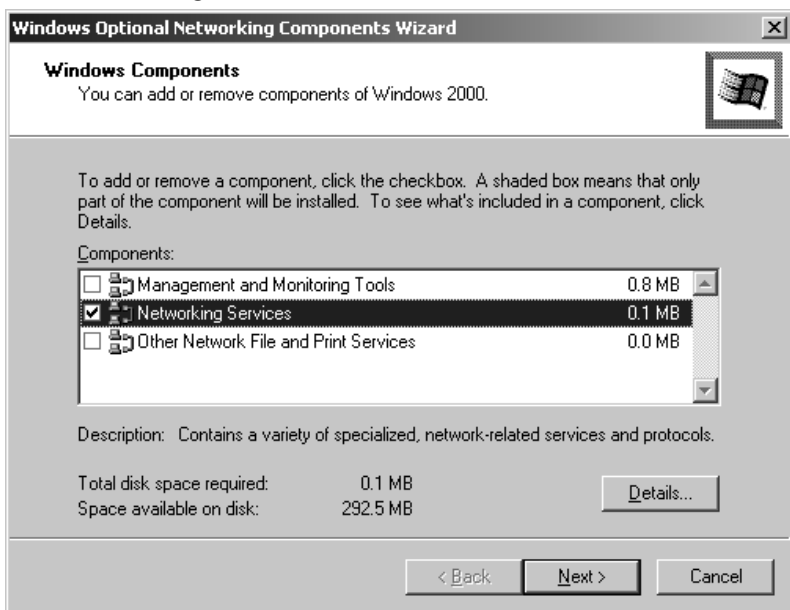
You have to install the network services before the PCs in your network can access shared resources. Have your Installation CD to hand. Then:

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

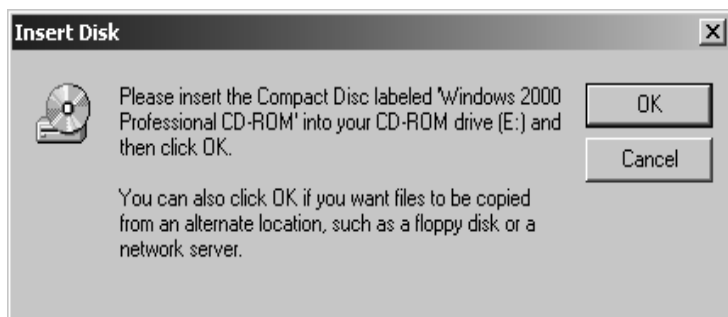


- ◆ Select in the left-hand pane the entry **Add network components**.

- ◆ Select **Networking services** and click **next**.



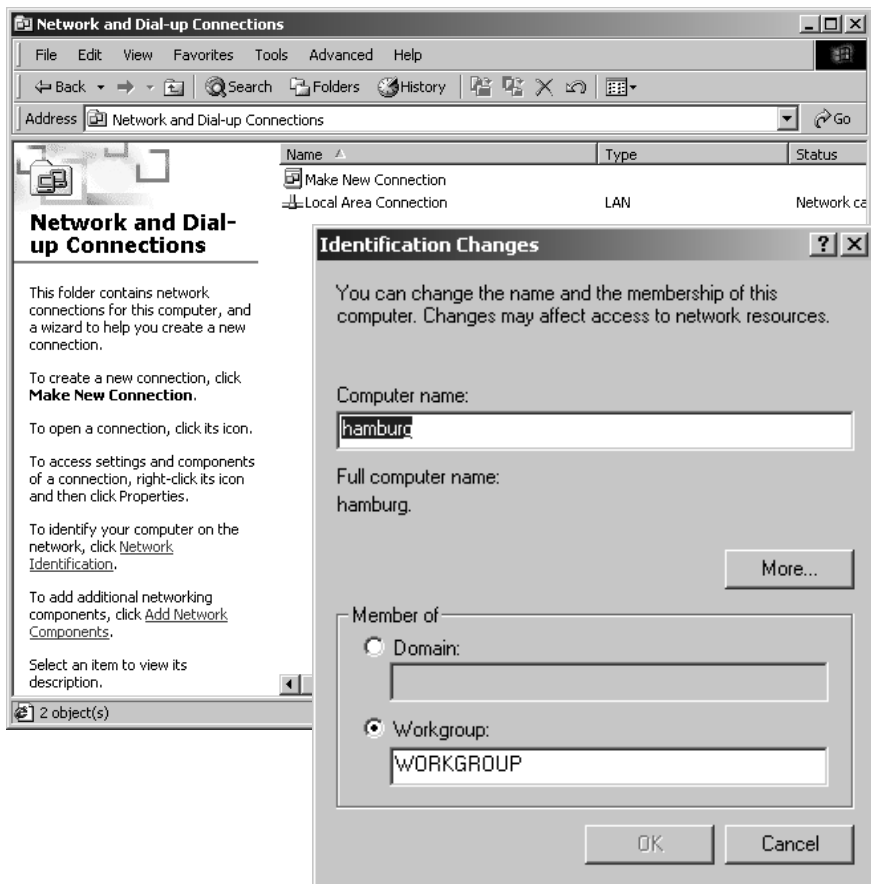
- ◆ Insert the WIN2000 CD and click the **OK** button to install all the required components.



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**.

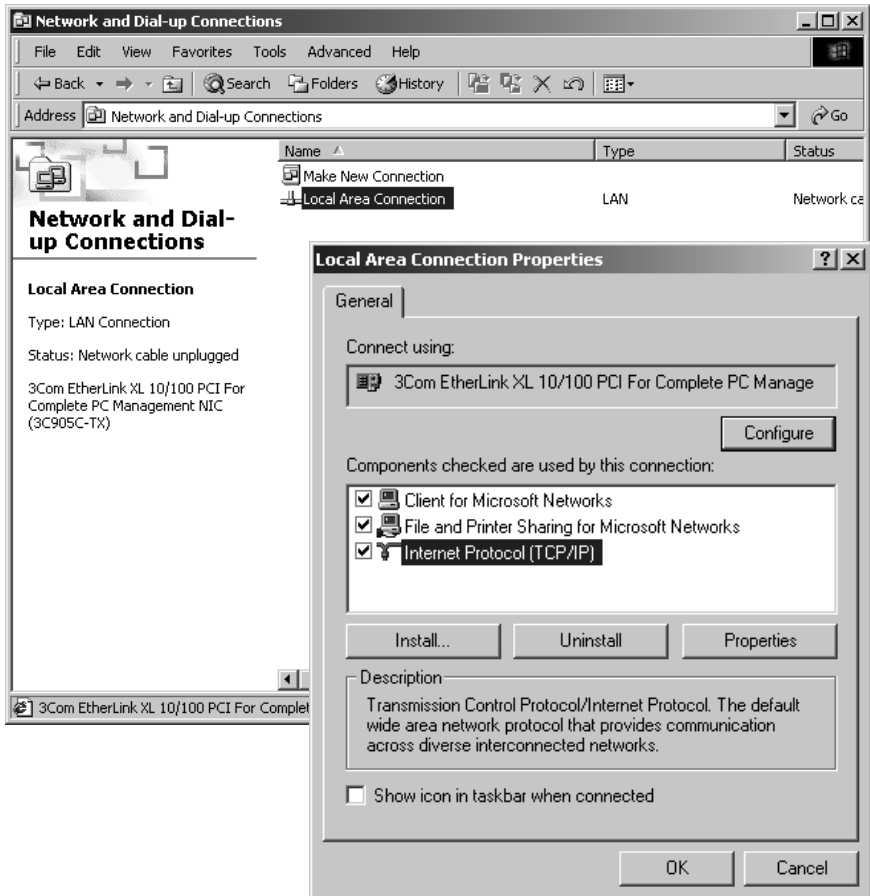


- ◆ In the **Computer name** box, enter the name the PC is to appear under on the network. This name must be unique within the network.
- ◆ In the **Workgroup** box, enter a name for the workgroup. This name must be the same for all the PCs on the network.
- ◆ Confirm this with **OK**.

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.

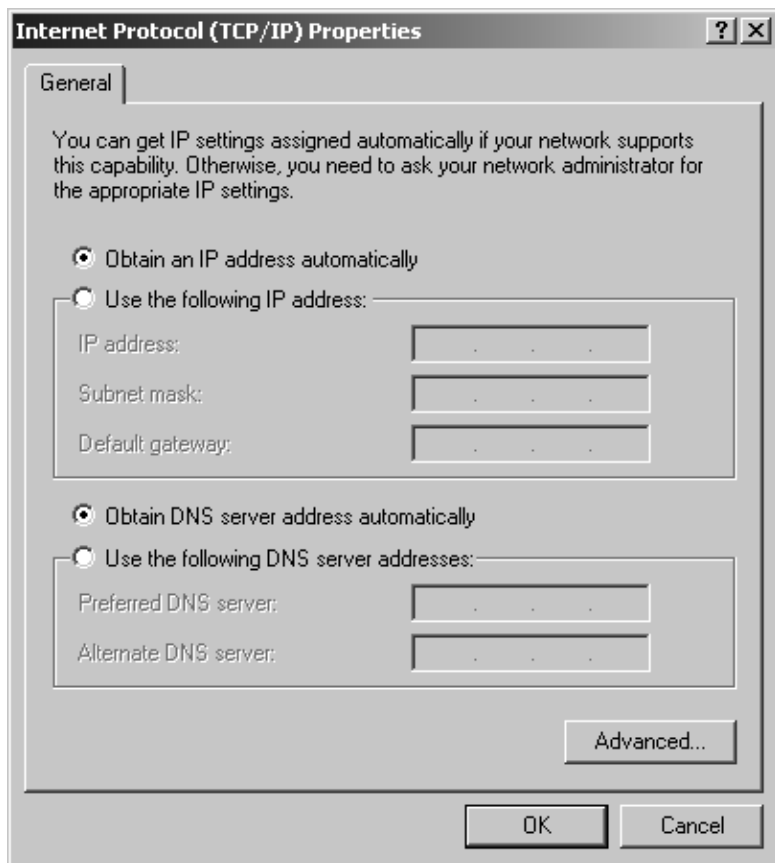
- ◆ Right click to open **Local Area Connection**. In the next window click **Properties**.



- ◆ 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**.

Sharing files and printers

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



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

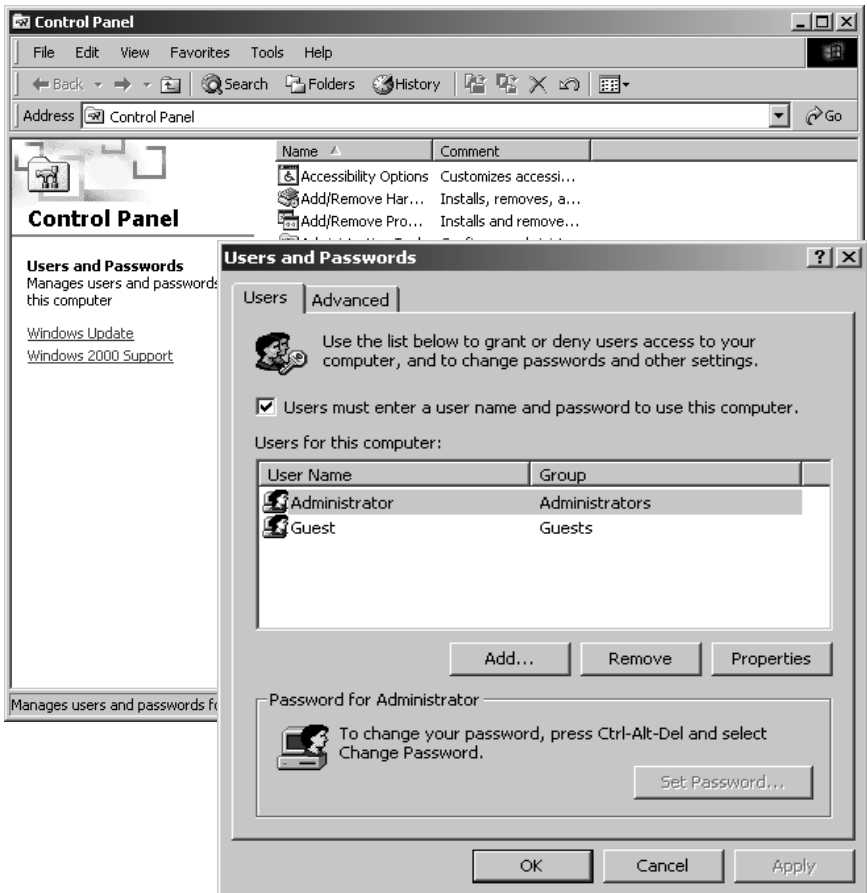
i

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 in the Appendix on page 117.

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**.

Sharing files and printers

- ◆ 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. On the left is a dark area with a white icon of a computer monitor with a plus sign. The main area is light gray and contains the text 'Enter the basic information for the new user.' Below this are three text input fields: 'User name:' with 'Anny' entered, 'Full name:' with 'Anny Gray' entered, and 'Description:' which is empty. Below the 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, Step 2. The left side is the same as the previous window. The main area is light gray and contains the text 'What level of access do you want to grant this user?'. There are three radio button options: 'Standard user (Power Users Group)' with a description 'Users can modify the computer and install programs, but cannot read files that belong to other users.', 'Restricted user (Users Group)' with a description 'Users can operate the computer and save documents, but cannot install programs or make potentially damaging changes to the system files and settings.', and 'Other: Administrators' which is selected. Below the 'Other' option is a description 'Administrators have complete and unrestricted access to the computer/domain'. 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**.

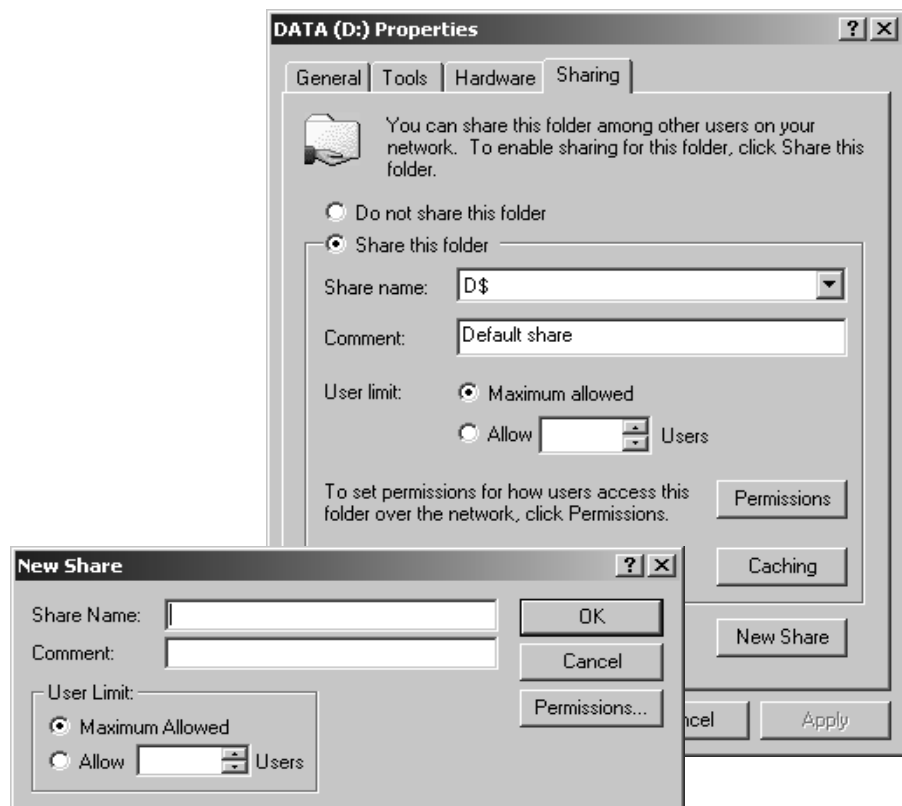


Releasing files and printers

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

Releasing files

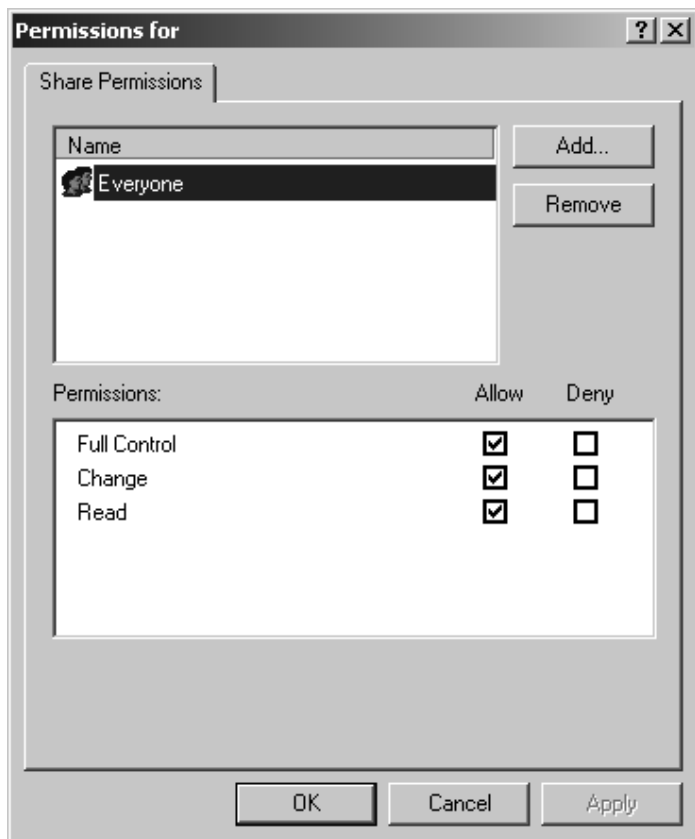
- ◆ Open the **Desktop** and right click the folder or drive you want to release.
- ◆ Now select the entry **Share** with the left-hand mouse button from the pop-up menu.



- ◆ 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**.

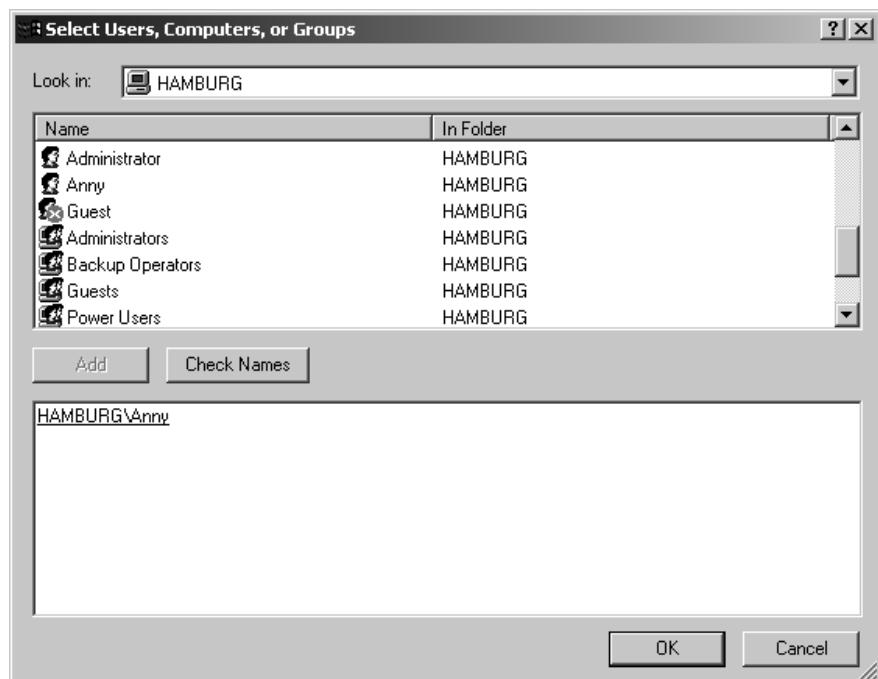
Now you can assign user rights to the registered users.

- ◆ Click **Add**.



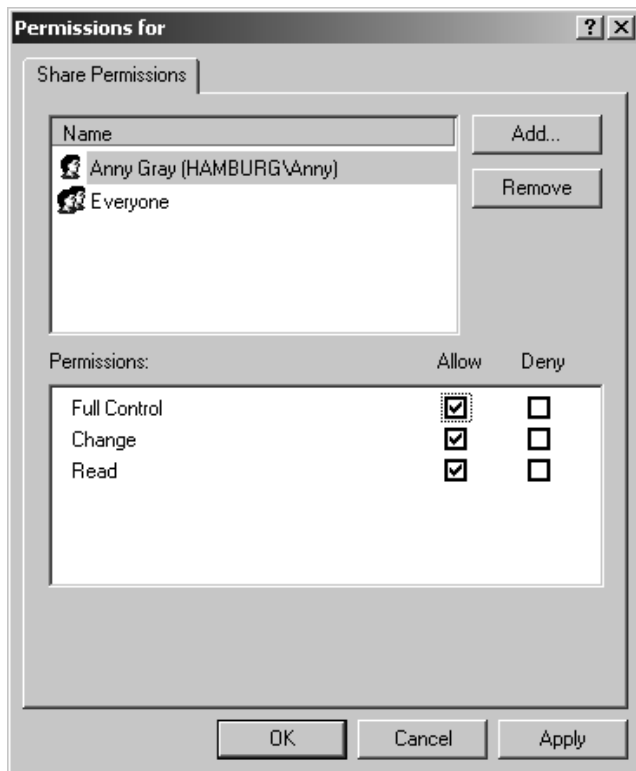
Sharing files and printers

- ◆ 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.

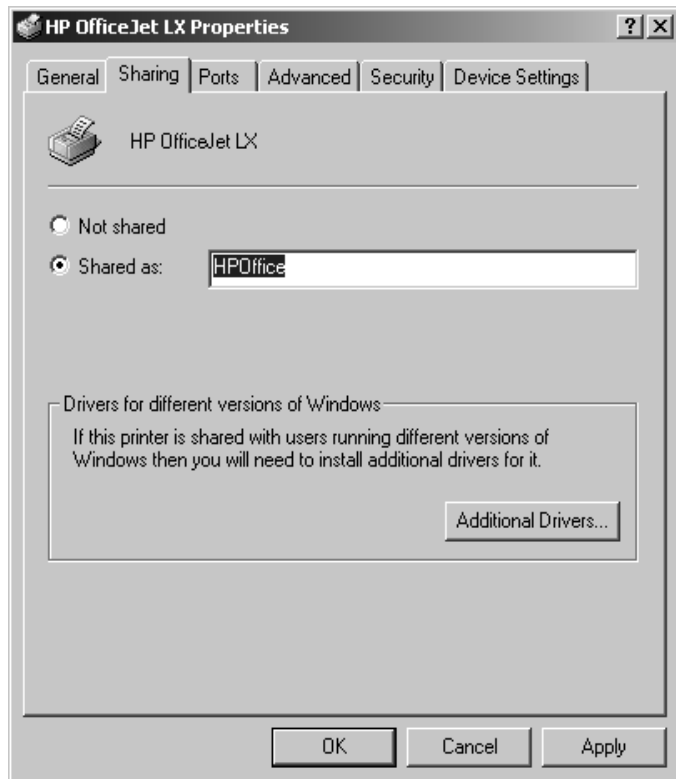


- ◆ To save the settings you have made, click **Apply** and **OK**. Close the next window as well with **OK**. Close the properties window with **OK**.

Sharing files and printers

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.

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.

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 75).
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 112).
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.

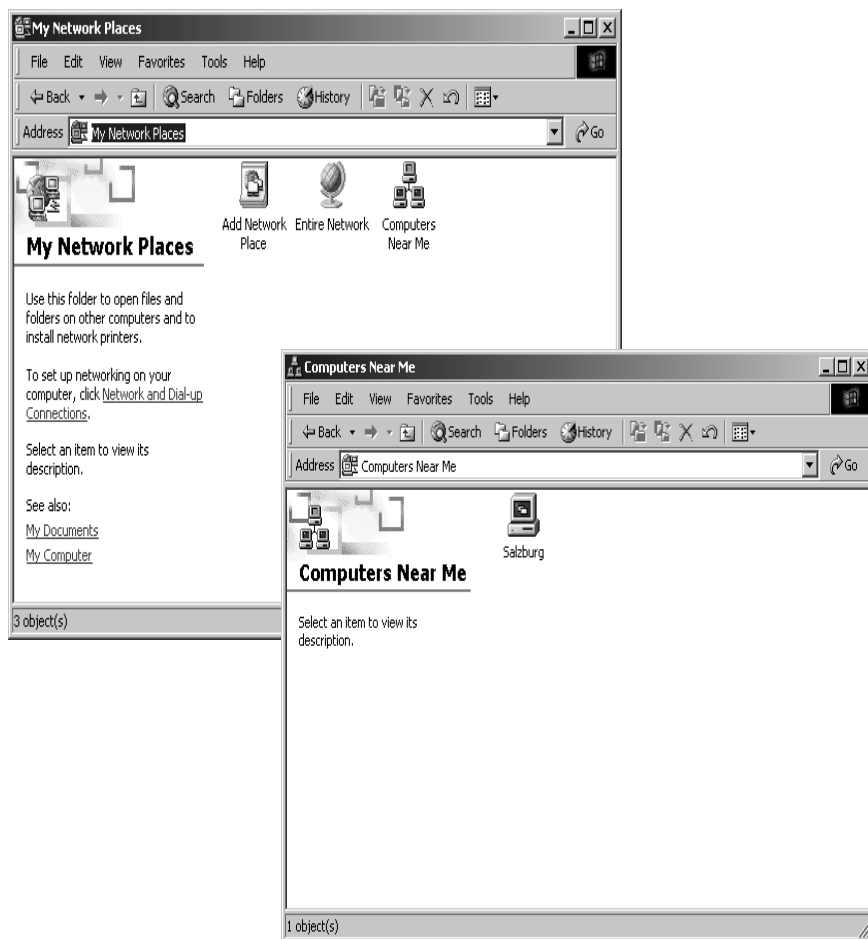


Please bear in mind that drives or folders can be hooked on to several PCs at the same time and thus accessed by other users. Most applications (e. g. word processing software) lock files once they have been opened. This prevents inconsistent data pools. If you cannot open a file because it is locked, you will normally see a message to that effect.

Sharing files and printers

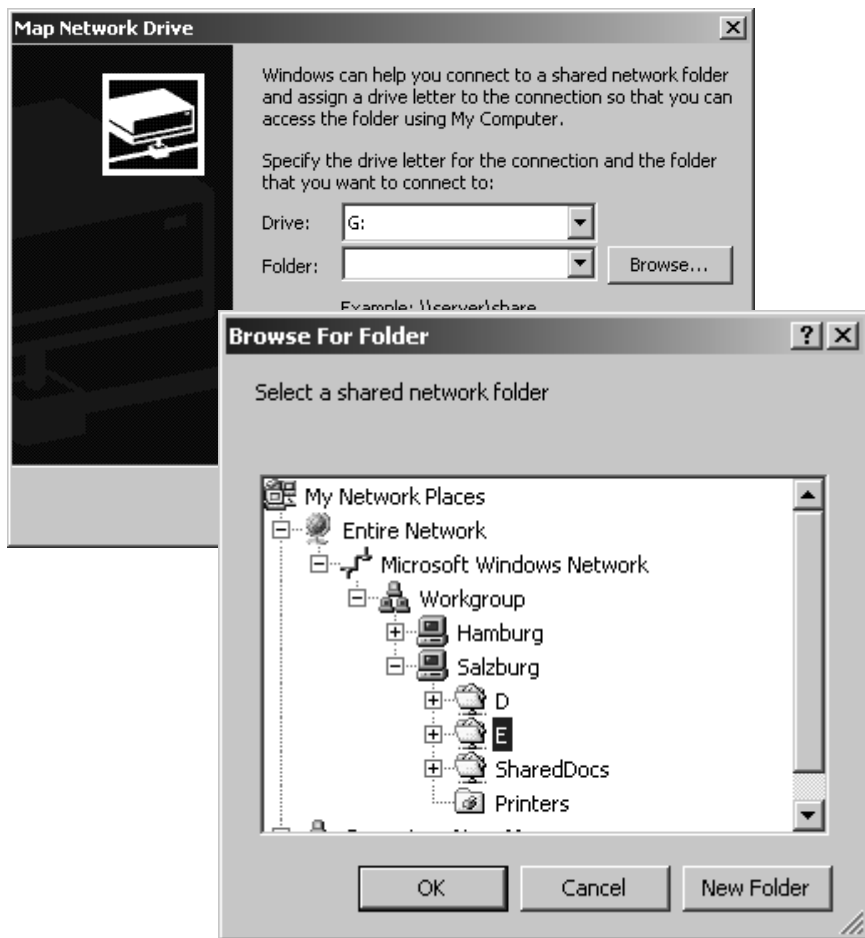
To hook up network drives:

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

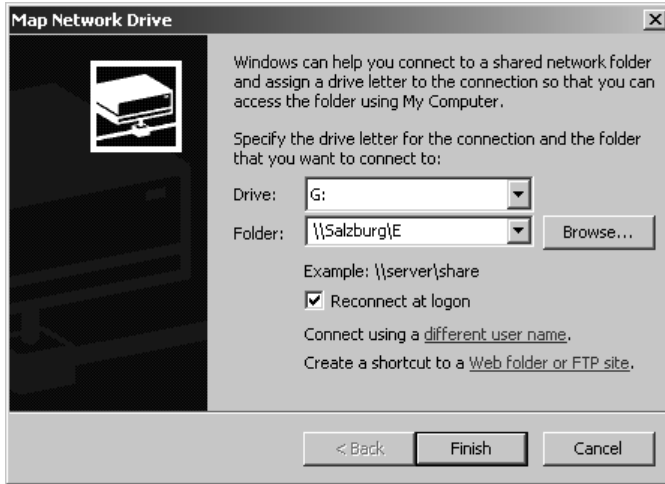


- ◆ Open the PC containing the resources you want to access with a double click. You will now see the shared resources on that PC.

- ◆ 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**.

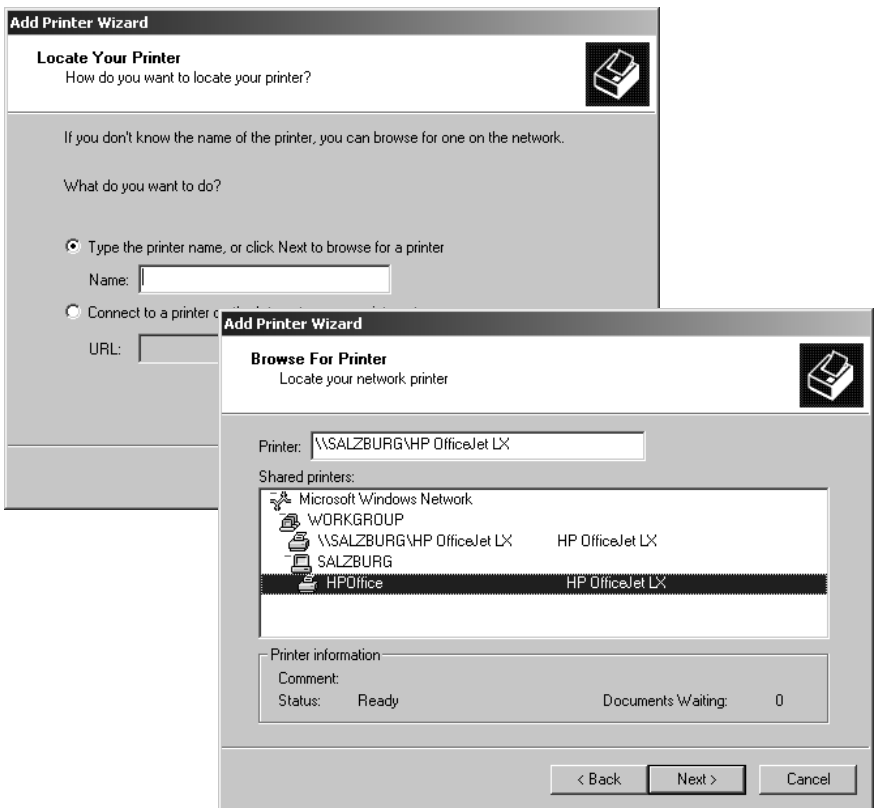


- ◆ If you select the option **Reconnect at logon**, Windows will hook the drive on every time you start your PC, provided the remote PC is running.
- ◆ Click **Finish**.
- ◆ Now open the **Desktop**. The remote drive is now available as the network drive. You can access the files as if they were on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



Sharing files and printers

- ◆ 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.

Appendix: 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 118, for Windows XP from page 122 and for Windows 2000 from page 126.

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.



Make sure that 255.255.255.0 is used as the subnet mask. 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

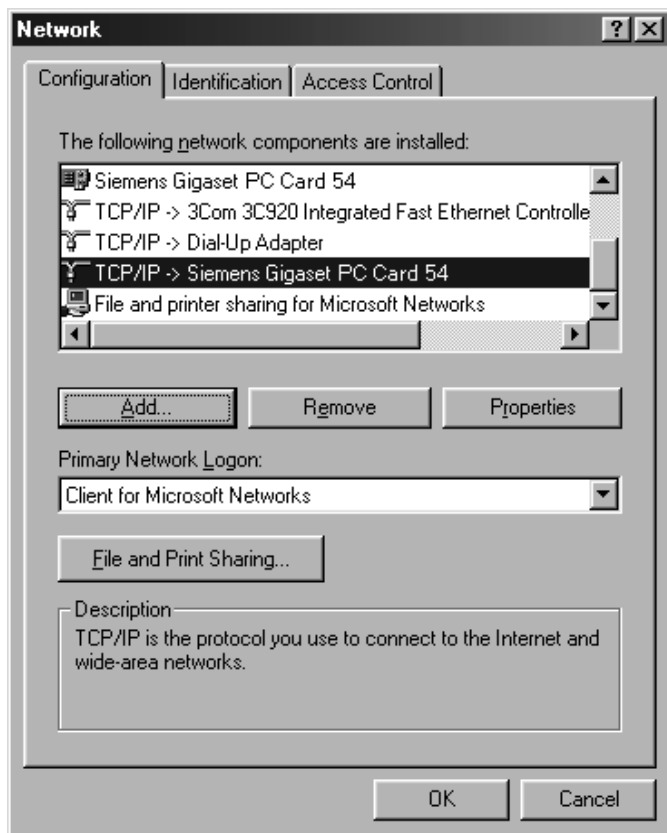
PC 1: 192.168.3.2

PC 2: 192.168.4.3

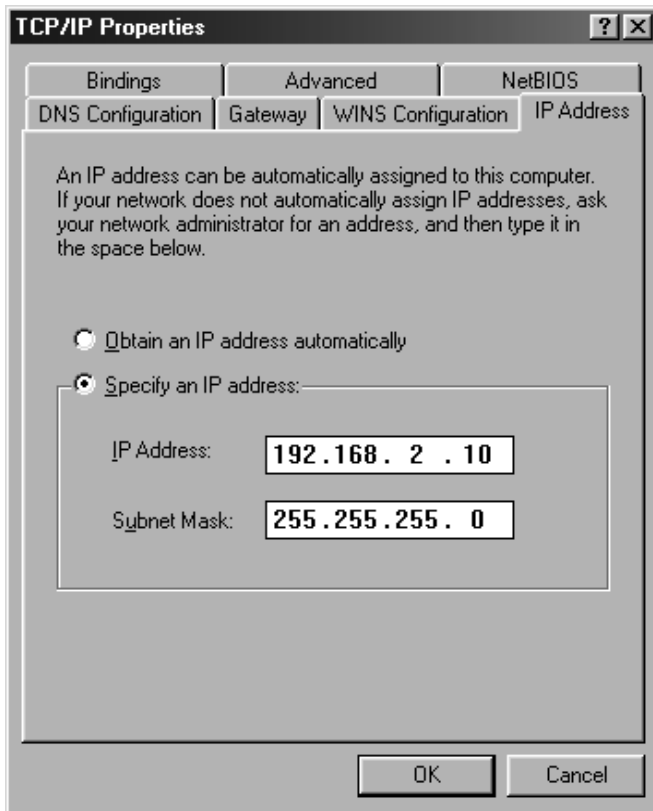
Windows 98

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.



- ◆ Click **Properties**.



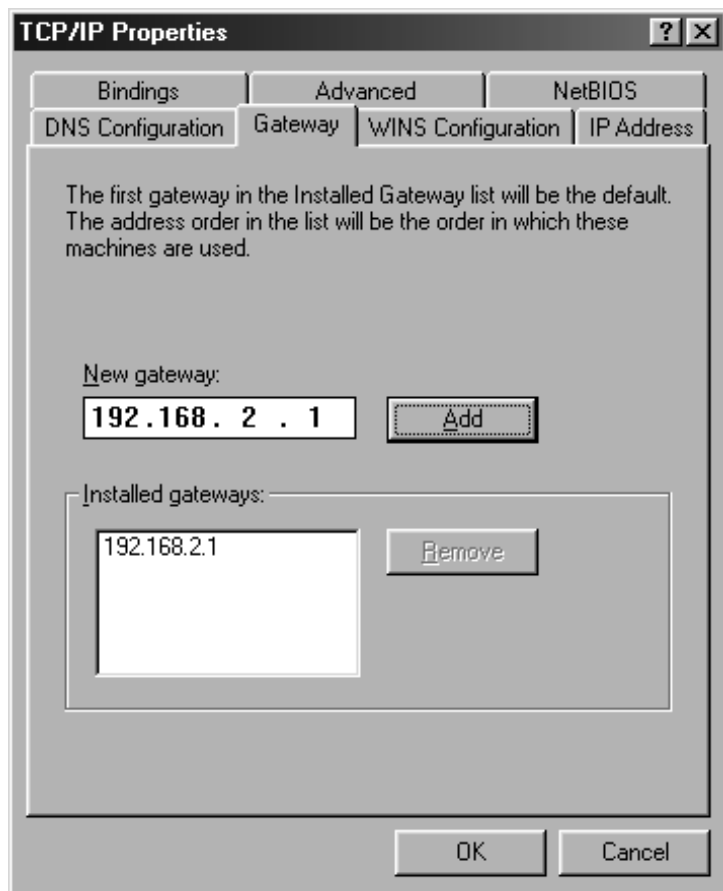
- ◆ Click the **IP address** tab and check the **Specify an IP address** option.
- ◆ Enter the IP address for the PC in the **IP address** box. Please bear in mind the information on page 117.
- ◆ Enter the subnet mask 255.255.255.0 in the box **Subnet Mask**.



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.

Appendix: Defining IP addresses

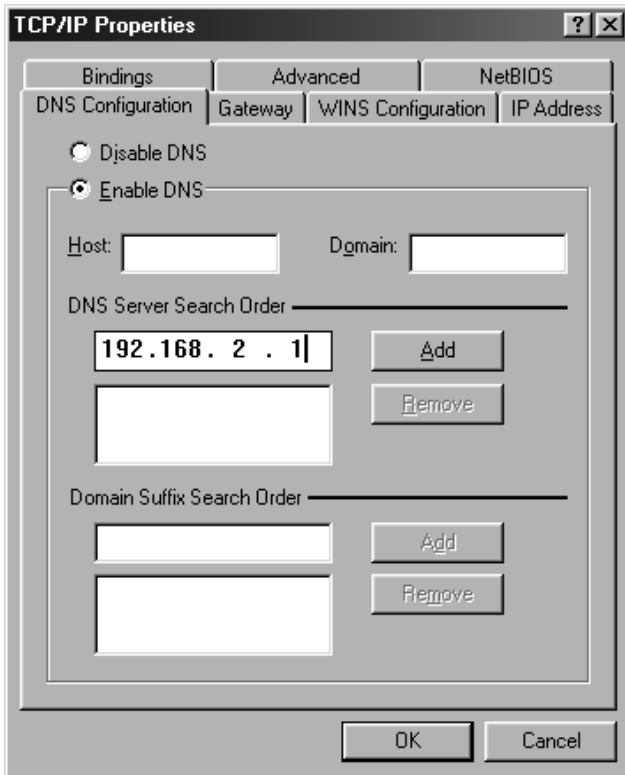
- ◆ Open the **Gateway** tab.



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**.

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



- ◆ Select **Enable DNS**.



DNS (Domain Name System) permits the assigning of IP addresses to computer 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

i

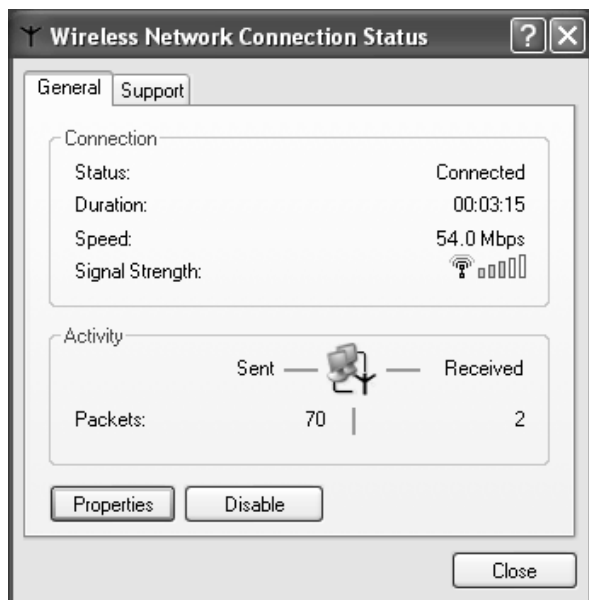
If you have a wireless connection between the router and PC: Make sure that the **Use Windows to configure the settings** function has been disabled.

This can be done as follows:

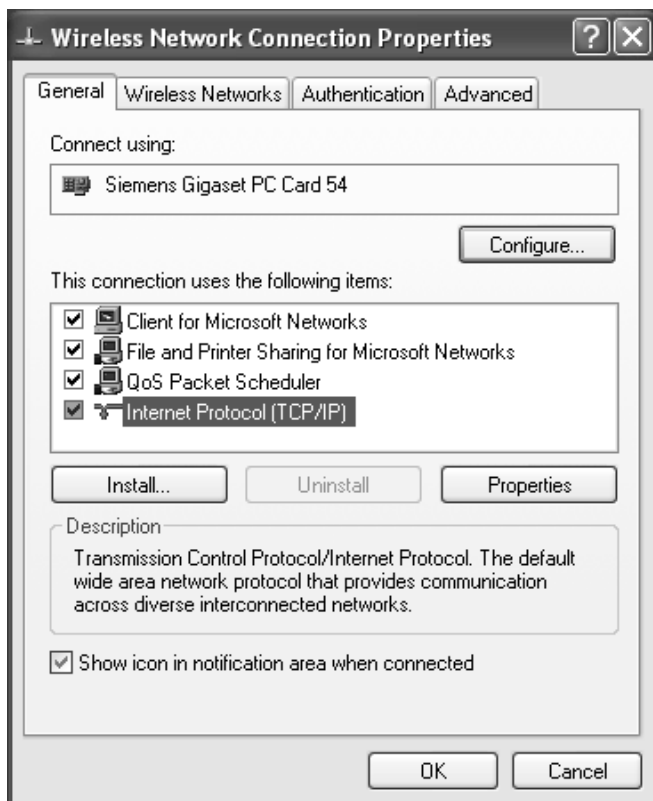
1. Click **Start – Control Panel – Network and Internet Connections – Network Connections – LAN or high-speed Internet**.
2. In the **General** tab click **Properties**.
3. Deactivate the **Use Windows to configure the settings** option in the **Wireless networks** tab.

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.



- ◆ In the **General** tab click **Properties**.



Appendix: Defining IP addresses

- ◆ 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 117.



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 **Default gateway** box.



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**.



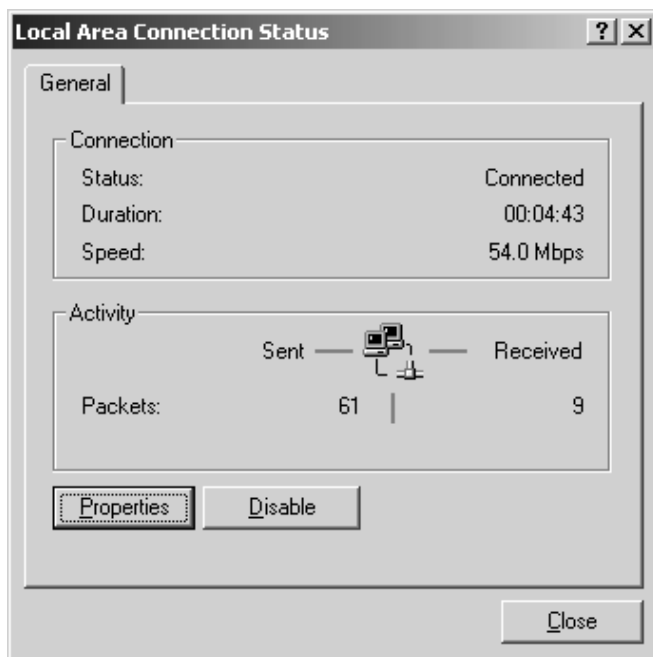
DNS (Domain Name System) permits the assigning of IP addresses to computer or domain names.

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

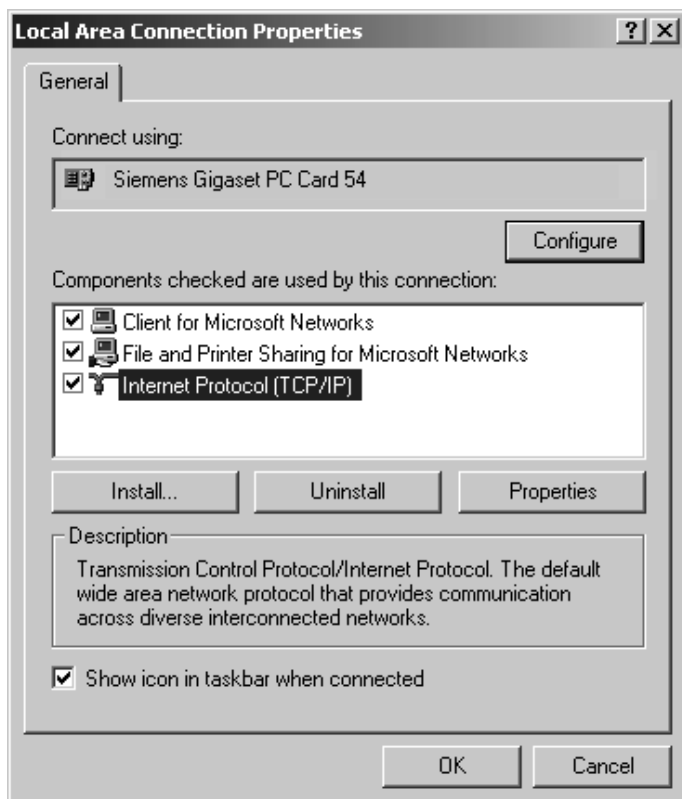
Windows 2000

To set a static IP address for your PC:

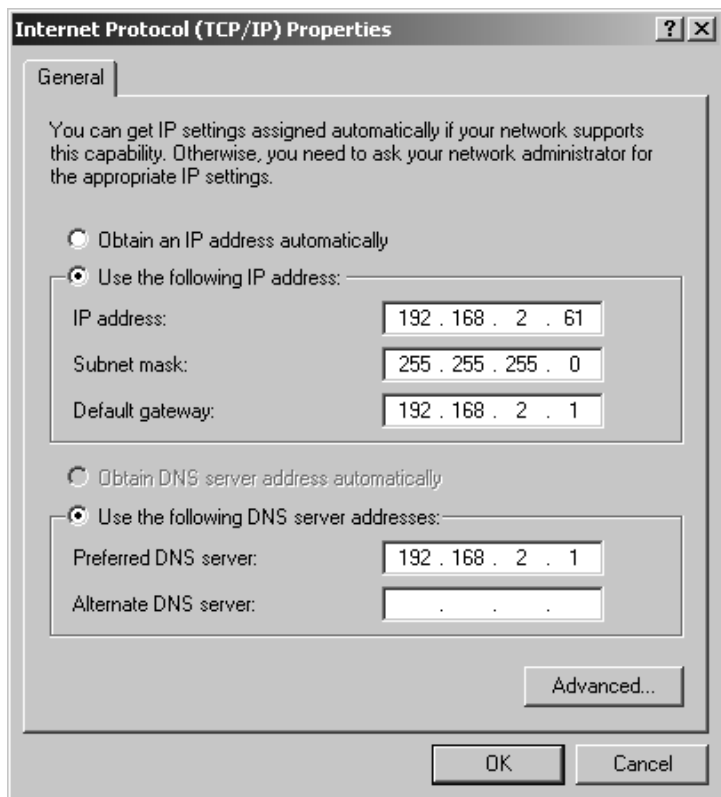
- ◆ Click **Start – Settings – Control Panel**.
- ◆ Double click the **Network and Dial-up Connections** icon and then **Local Area Connection**.



- ◆ In the **General** tab click **Properties**.



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



- ◆ 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 117.



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 **Default gateway** box.



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**.



DNS (Domain Name System) permits the assigning of IP addresses to computer 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 SE505 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 SE505 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 SE505 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 SE505 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**.

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.

Glossary

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 addresses. For Dynamic IP addresses 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 SE505 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)

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).

Glossary

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 SE505 dsl/cable has a **Private IP address** and a **Public IP address**.

IP address pool

The Gigaset SE505 dsl/cable's IP address pool defines a range of **IP addresses** that the router's **DHCP Server** can use to assign **Dynamic IP addresses**.

IPSec

Internet Protocol Security

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

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

ISP

Internet Service Provider see **Internet Service Provider**

L2TP

Layer Two Tunneling Protocol

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

LAN

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

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 be transported over the network at a time.

NAT

Network Address Translation

NAT is a method for implementing IP addresses (mostly **Private IP addresses**) in a network on one or more **Public IP addresses** on the **Internet**. With NAT several network components in a **LAN** can share the router's public IP address to connect to the Internet. The network components of the local network are hidden behind the router's IP address registered on the Internet. As a result of this security function NAT is frequently used as part of the network **Firewall**. If you want to make services on a PC on the local network available on the Internet despite NAT, you can configure the Gigaset SE505 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 54 and Gigaset PCI Card 54.

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 SE505 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**

Glossary

PPPoE

Point-to-Point Protocol over **Ethernet**

PPPoE is a **Protocol** for connecting network components in a local Ethernet network to the **Internet** via a modem.

PPTP

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 SE505 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 SE505 dsl/cable, have a public and a **Private IP address**.

Remote Management

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

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 packets from one local network (**LAN**) to another via the fastest route. A Router permits the connecting of network with different network technologies. For example, it can link a local network with **Ethernet** or **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 SE505 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.

Subnetwork

A subnetwork divides a network into smaller units.

Switch

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

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

TCP

Transmission Control Protocol

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

See also: **UDP**

TCP/IP

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

Tunneling

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

Glossary

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 SE505 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 SE505 dsl/cable complies with Standard 802.11g.

Index

Numerics

128-bit encryption	34
128-bit key	33
64-bit encryption	34
64-bit key	33

A

Access control	
activating the	36
at release level	62
at user level	62
changing in Advanced Setup	38
defining (Windows 98)	62
Access control to the router	36
Access point	8, 130
Address block for IP addresses	117
Ad-hoc mode	7, 130
configuring the network adapter	15
Ad-hoc network	7, 13
requirements	15
Advanced Setup	
launching	21, 29, 44, 48, 51
ASCII key	35
Assigning static IP addresses	
Windows 2000	126
Windows 98	118
Windows XP	122
Auto-Reconnect	130

B

Base station	8
Bridge	130
Broadcast	130
BSSID	130

C

Change user passwords	
Windows 2000	105
Checking network settings	
(Windows XP)	84
Client	130
Command	
exit	18
ipconfig	18
ipconfig /all	20, 37, 47, 55, 57

ping	17
Command prompt	
closing the	18
opening the	17
Configuration	
backing up	28, 39
backing up in Advanced Setup	39
restoring	39
Connecting network drives	
Windows 2000	113
Windows 98	76
Windows XP	93
Connection	
checking a	17
statistics	18
Connection method	82
ConnectionPoint (SSID)	31

D

Data encryption	33
Define computer name	
Windows 2000	100
Windows 98	62
Windows XP	83
Define workgroup	
Windows 2000	100
Windows 98	62
Windows XP	83
Demilitarised zone	56
DHCP	131
Digital Subscriber Line see DSL	
DMZ	56, 131
DNS	131
DNS Server	37, 121, 131
Domain name	131
Domain Name Service see DNS	
DSL	131
Dynamic DNS Service see DynDNS	
Dynamic Host Configuration Protocol	
see DHCP	
dynamic IP address	132
DynDNS	51, 132

E

Encryption	132
Encryption mode	

- selecting for network adapters 42
- selecting for router 34
- Entering a gateway
 - Windows 2000 129
 - Windows 98 120
 - Windows XP 125
- Ethernet 6, 8, 132
- Ethernet network
 - linking with a wireless network. . . . 9
- exit command. 18
- Extending the range 5

F

- Files
 - shared use in a network 58
- Filter
 - activating the 26
 - for Internet services 19
 - for URL addresses. 19
 - starting configuration 21
- Filter function. 19
- Filter table 22
- Firewall 56, 132
- Flat rate 132
- Full duplex 132

G

- Games
 - non pre-defined. 46
 - predefined configuration 45
- Games on the Internet 44
- Gateway 120, 125, 129, 132
- Gigaset PC Card 54 5, 7
- Gigaset PCI Card 54. 5, 7
- Gigaset Router see Router
- Gigaset SE505 dsl/cable. 5, 6
- Gigaset WLAN adapter monitor
 - changing the SSID 40
 - launching the 15, 40, 41
 - setting the ad-hoc mode 15
 - setting WEP encryption 41
- Global IP address see public IP address

H

- Half duplex 132
- Hexadecimal key 34
- Home network 5
- HTTP proxy 132
- Hub 133

I

- IEEE. 133
- Infrastructure mode. 8, 133
- Infrastructure network 8
- Institute of Electrical and Electronic Engineers see IEEE
- Internet. 8, 133
- Internet access. 5
 - restricting. 22
 - unrestricted 56
- Internet Protocol see IP Protocol
- Internet service
 - filtering 19, 22
 - non pre-defined 24
 - permitting an 23
 - pre-defined 25
 - restricting access 22
- Internet Service Provider 6, 133
- IP address 15, 117, 134
 - Address block 117
 - dynamic. 132
 - private 117, 136
 - public. 51, 136
 - static 15, 137
- IP address pool. 134
- IP protocol 133
- ipconfig. 18
- ipconfig /all 20, 37, 47, 55, 57
- IPSec. 134
- ISP see Internet Service Provider

K

- Key length
 - 128-bit (ASCII) 35
 - 128-bit (hexadecimal). 34
 - 64-bit (ASCII) 35
 - 64-bit (hexadecimal). 34

L

- L2TP 134
- LAN. 9, 134
- Launch
 - Advanced Setup . . . 21, 29, 44, 48, 51
 - command prompt. 17
 - Gigaset WLAN adapter
 - monitor 15, 40, 41
 - network wizard. 80
- Launch network wizard (Windows XP) 80
- Layer Two Tunneling Protocol see L2TP

List of registered PCs . 23, 37, 45, 49, 53
 Local IP address see private IP address
 Local network 134

M

MAC access table. 36
 MAC address 20, 37, 134
 Making drives available
 Windows 2000. 111
 Windows 98. 74
 Windows XP. 92
 Making files available
 Windows 2000. 111
 Windows 98. 74
 Windows XP. 92
 Making folders available
 Windows 2000. 111
 Windows 98. 74
 Windows XP. 92
 Making printers available
 Windows 2000. 115
 Windows 98. 77
 Windows XP. 95
 Maximum Receive Unit see MRU
 Maximum Transmission Unit see MTU
 Mbps 135
 Microsoft Network. 59
 Mobile network. 7, 13
 MRU 135
 MTU 135

N

NAT 44, 48, 135
 NAT function
 disabling for MS Netmeeting 48
 Netmeeting
 enabling 48
 setting up a virtual server. 48
 Network 135
 ad-hoc. 7
 infrastructure. 8
 wired. 6
 wireless. 7
 Network adapter 135
 changing the SSID 40
 configuring in ad-hoc mode 15
 Ethernet 6
 hardware address. 20
 setting WEP encryption 41

 wireless 7
 Network Address Translation see NAT
 Network Client
 setting up a (Windows 98). 61
 Network components
 mobile 7, 13
 Network configuration
 Windows 2000 98
 Windows 98 59
 Windows XP 80
 Network environment
 Windows 98 75
 Network service
 installing a (Windows 2000) 98

P

Parental control 19
 Password
 assigning a 30
 changing a 30
 changing in Advanced Setup 30
 forgotten 30
 Password for users
 Windows 2000 104
 Windows 98 71
 Windows XP 90

PC

 configuring as Microsoft Network
 Client 59
 defining a name (Windows 2000) . 100
 defining a name (Windows 98) . . . 62
 defining a name (Windows XP) . . . 83
 identification via MAC address. . . . 20
 putting in a DMZ. 56
 setting up as a server 51
 temporary integration in a network . 13
 unrestricted Internet access. 56
 PC game 14
 ping command. 17
 Point-to-Point Protocol over Ethernet
 see PPPoE
 Point-to-Point Tunneling Protocol
 see PPTP
 Port. 44, 135
 Port Forwarding. 52, 135
 for games. 44
 starting configuration 44, 48
 Port number 53, 135
 Possible uses 11

- PPPoE 136
- PPTP 136
- Printer
 - shared use in a network 58
- Private IP address 136
- Protection functions 19
- Protocol 44, 136
- Public IP address 136

- R**
- Releasing files
 - Windows 2000 106
 - Windows 98 68
 - Windows XP 86
- Releasing printers
 - Windows 2000 110
 - Windows 98 70
 - Windows XP 88
- Remote Management 136
- Rights for user access
 - (Windows 2000) 109
- Roaming 10, 136
- Router 5, 136
 - Access control 36
 - changing the SSID 31
 - for wired networks 6
 - protecting with a password 30
 - setting up as a virtual server 52
 - setting WEP encryption 34

- S**
- Security actions 28
- Security architecture, WEP 33
- Security risk 56
- Security Setup 28
 - launching 29
- Server 136
 - setting up a 51, 52
 - virtual 138
- Service
 - non pre-defined 54
 - pre-defined 52
 - providing on the Internet 51
- Service Set ID see SSID
- Service Set Identifier see SSID
- Setting the TCP/IP protocol
 - Windows 2000 101
 - Windows 98 64
- Setting up network printers
 - Windows 2000 115
 - Windows 98 77
 - Windows XP 95
- Setting up user IDs
 - Windows 2000 103
 - Windows 98 71
- Simple Mail Transfer Protocol see SMTP
- SMTP 136
- SSID 31, 137
 - changing a 31
 - changing in Advanced Setup 32
 - changing on the network adapter 40
 - changing on the router 31
 - ConnectionPoint 31
 - disabling broadcast 32
- Static IP address 137
- Subnet mask 119, 124, 128, 137
- Subnetwork 137
- Switch 137

- T**
- TCP 44, 137
- TCP/IP 137
- Transmission Control Protocol see TCP
- Transmission speed 135
- Tunnel 136
- Tunneling 137

- U**
- UDP 44, 138
- Universal Plug and Play see UPnP
- Universal Resource Locator see URL
- UPnP 138
- URL 138
- URL block see URL filter
- URL filter 27
- URL filtering 19
- User
 - settings for user interface
(Windows 98) 72
- User account
 - setting up a (Windows XP) 89
- User Datagram Protocol see UDP
- User list (Windows 98) 73
- User name
 - Windows 2000 104
 - Windows 98 71
 - Windows XP 89
- User password

Index

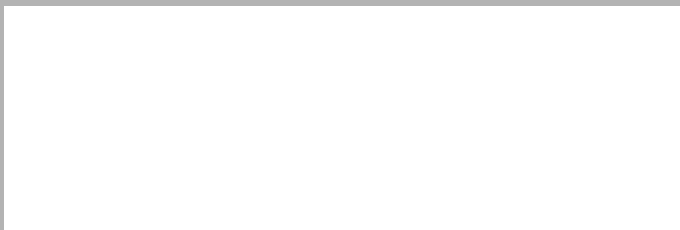
- Windows 2000. 104
- Windows 98. 71
- Windows XP. 90
- Utility
 - for file and printer release
 - (Windows 98) 66

V

- Virtual Private Network see VPN
- Virtual server 51, 52, 138
 - for Netmeeting 48
 - starting configuration 51
- VPN 138

W

- WAN. 138
- WAN interface. 5, 8
- WEP 138
- WEP encryption. 33
 - 128-bit 34
 - 64-bit 34
 - changing in Advanced Setup 35
 - setting on the network adapter. . . . 41
 - setting on the router 34
- Wide Area Network see WAN
- Wired Equivalent Privacy see WEP
 - and WEP encryption
- Wired network 6
- Wireless cell 139
- Wireless LAN see WLAN
- Wireless network. 139
 - ad-hoc mode 7
 - infrastructure mode 8
- WLAN. 7, 9, 139
 - Operating types 7
- WLAN adapter. 7



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

© Siemens AG 2003
All rights reserved.
Subject to availability.
Subject to change.
07/2003

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

Order No.: A31008-E105-B103-1-7619