Gigaset

EN Dear Customer,

Gigaset Communications GmbH is the legal successor to Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), which in turn continued the Gigaset business of Siemens AG. Any statements made by Siemens AG or SHC that are found in the user guides should therefore be understood as statements of Gigaset Communications GmbH.

We hope you enjoy your Gigaset.

DE Sehr geehrte Kundin, sehr geehrter Kunde,

die Gigaset Communications GmbH ist Rechtsnachfolgerin der Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), die ihrerseits das Gigaset-Geschäft der Siemens AG fortführte. Etwaige Erklärungen der Siemens AG oder der SHC in den Bedienungsanleitungen sind daher als Erklärungen der Gigaset Communications GmbH zu verstehen.

Wir wünschen Ihnen viel Freude mit Ihrem Gigaset.

FR Chère Cliente, Cher Client,

la société Gigaset Communications GmbH succède en droit à Siemens Home and Office Communication Devices GmbH & Co. KG (SHC) qui poursuivait elle-même les activités Gigaset de Siemens AG. Donc les éventuelles explications de Siemens AG ou de SHC figurant dans les modes d'emploi doivent être comprises comme des explications de Gigaset Communications GmbH.

Nous vous souhaitons beaucoup d'agrément avec votre Gigaset.

IT Gentile cliente,

la Gigaset Communications GmbH è successore della Siemens Home and Office Communication Devices GmbH & Co. KG (SHC) che a sua volta ha proseguito l'attività della Siemens AG. Eventuali dichiarazioni della Siemens AG o della SHC nei manuali d'istruzione, vanno pertanto intese come dichiarazioni della Gigaset Communications GmbH.

Le auguriamo tanta soddisfazione con il vostro Gigaset.

NL Geachte klant,

Gigaset Communications GmbH is de rechtsopvolger van Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), de onderneming die de Gigaset-activiteiten van Siemens AG heeft overgenomen. Eventuele uitspraken of mededelingen van Siemens AG of SHC in de gebruiksaanwijzingen dienen daarom als mededelingen van Gigaset Communications GmbH te worden gezien.

Wij wensen u veel plezier met uw Gigaset**.**

ES Estimado cliente,

la Gigaset Communications GmbH es derechohabiente de la Siemens Home and Office Communication Devices GmbH & Co. KG (SHC) que por su parte continuó el negocio Gigaset de la Siemens AG. Las posibles declaraciones de la Siemens AG o de la SHC en las instrucciones de uso se deben entender por lo tanto como declaraciones de la Gigaset Communications GmbH.

Le deseamos que disfrute con su Gigaset.

PT SCaros clientes,

Gigaset Communications GmbH é a sucessora legal da Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), que, por sua vez, deu continuidade ao sector de negócios Gigaset, da Siemens AG. Quaisquer declarações por parte da Siemens AG ou da SHC encontradas nos manuais de utilização deverão, portanto, ser consideradas como declarações da Gigaset Communications GmbH.

Desejamos que tenham bons momentos com o seu Gigaset.

DA Kære Kunde,

Gigaset Communications GmbH er retlig efterfølger til Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), som fra deres side videreførte Siemens AGs Gigaset-forretninger. Siemens AGs eller SHCs eventuelle forklaringer i betjeningsvejledningerne skal derfor forstås som Gigaset Communications GmbHs forklaringer.

Vi håber, du får meget glæde af din Gigaset.

FI Arvoisa asiakkaamme,

Gigaset Communications GmbH on Siemens Home and Office Communication Devices GmbH & Co. KG (SHC)-yrityksen oikeudenomistaja, joka jatkoi puolestaan Siemens AG:n Gigaset-liiketoimintaa. Käyttöoppaissa mahdollisesti esiintyvät Siemens AG:n tai SHC:n selosteet on tämän vuoksi ymmärrettävä Gigaset Communications GmbH:n selosteina.

Toivotamme Teille paljon iloa Gigaset-laitteestanne.

SV Kära kund,

Gigaset Communications GmbH övertar rättigheterna från Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), som bedrev Gigaset-verksamheten efter Siemens AG. Alla förklaringar från Siemens AG eller SHC i användarhandboken gäller därför som förklaringar från Gigaset Communications GmbH.

Vi önskar dig mycket nöje med din Gigaset.

NO Kjære kunde,

Gigaset Communications GmbH er rettslig etterfølger etter Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), som i sin tur videreførte Gigaset-geskjeften i Siemens AG. Eventuelle meddelelser fra Siemens AG eller SHC i bruksanvisningene er derfor å forstå som meddelelser fra Gigaset Communications GmbH.

Vi håper du får stor glede av din Gigaset-enhet.

EL Αγαπητή πελάτισσα, αγαπητέ πελάτη,

η Gigaset Communications GmbH είναι η νομική διάδοχος της Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), η οποία έχει αναλάβει την εμπορική δραστηριότητα Gigaset της Siemens AG. Οι δηλώσεις της Siemens AG ή της SHC στις οδηγίες χρήσης αποτελούν επομένως δηλώσεις της Gigaset Communications GmbH.

Σας ευχόμαστε καλή διασκέδαση με τη συσκευή σας Gigaset.

HR Poštovani korisnici,

Gigaset Communications GmbH pravni je sljednik tvrtke Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), koji je nastavio Gigaset poslovanje tvrtke Siemens AG. Zato sve izjave tvrtke Siemens AG ili SHC koje se nalaze u uputama za upotrebu treba tumačiti kao izjave tvrtke Gigaset Communications GmbH.

Nadamo se da sa zadovoljstvom koristite svoj Gigaset uređaj.

SL Spoštovani kupec!

Podjetje Gigaset Communications GmbH je pravni naslednik podjetja Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), ki nadaljuje dejavnost znamke Gigaset podjetja Siemens AG. Vse izjave podjetja Siemens AG ali SHC v priročnikih za uporabnike torej veljajo kot izjave podjetja Gigaset Communications GmbH.

Želimo vam veliko užitkov ob uporabi naprave Gigaset.

Issued by
Gigaset Communications GmbH
Schlavenhorst 66, D-46395 Bocholt
Gigaset Communications GmbH is a trademark licensee of Siemens AG

www.gigaset.com

Gigaset

CS

Vážení zákazníci,

společnost Gigaset Communications GmbH je právním nástupcem společnosti Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), která dále přejala segment produktů Gigaset společnosti Siemens AG. Jakékoli prohlášení společnosti Siemens AG nebo SHC, které naleznete v uživatelských příručkách, je třeba považovat za prohlášení společnosti Gigaset Communications GmbH.

Doufáme, že jste s produkty Gigaset spokojeni.

SK

Vážený zákazník,

Spoločnosť Gigaset Communications GmbH je právnym nástupcom spoločnosti Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), ktorá zasa pokračovala v činnosti divízie Gigaset spoločnosti Siemens AG. Z tohto dôvodu je potrebné všetky vyhlásenia spoločnosti Siemens AG alebo SHC, ktoré sa nachádzajú v používateľských príručkách, chápať ako vyhlásenia spoločnosti Gigaset Communications GmbH.

Veríme, že budete so zariadením Gigaset spokojní.

RO

Stimate client,

Gigaset Communications GmbH este succesorul legal al companiei Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), care, la rândul său, a continuat activitatea companiei Gigaset a Siemens AG. Orice afirmaţii efectuate de Siemens AG sau SHC şi incluse în ghidurile de utilizare vor fi, prin urmare, considerate a aparţine Gigaset Communications GmbH.

Sperăm ca produsele Gigaset să fie la înălţimea dorinţelor dvs.

SR

Poštovani potrošaču,

Gigaset Communications GmbH je pravni naslednik kompanije Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), kroz koju je nastavljeno poslovanje kompanije Gigaset kao dela Siemens AG. Stoga sve izjave od strane Siemens AG ili SHC koje se mogu naći u korisničkim uputstvima treba tumačiti kao izjave kompanije Gigaset Communications GmbH.

Nadamo se da ćete uživati u korišćenju svog Gigaset uređaja.

BG

Уважаеми потребители,

Gigaset Communications GmbH е правоприемникът на Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), която на свой ред продължи бизнеса на подразделението Siemens AG. По тази причина всякакви изложения, направени от Siemens AG или SHC, които се намират в ръководствата за потребителя, следва да се разбират като изложения на Gigaset Communications GmbH.

Надяваме се да ползвате с удоволствие вашия Gigaset.

HU

Tisztelt Vásárló!

A Siemens Home and Communication Devices GmbH & Co. KG (SHC) törvényes jogutódja a Gigaset Communications GmbH, amely a Siemens AG Gigaset üzletágának utódja. Ebből következően a Siemens AG vagy az SHC felhasználói kézikönyveiben található bármely kijelentést a Gigaset Communications GmbH kijelentésének kell tekinteni.

Reméljük, megelégedéssel használja Gigaset készülékét.

PL

Szanowny Kliencie,

Firma Gigaset Communications GmbH jest spadkobiercą prawnym firmy Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), która z kolei przejęła segment produktów Gigaset od firmy Siemens AG. Wszelkie oświadczenia firm Siemens AG i SHC, które można znaleźć w instrukcjach obsługi, należy traktować jako oświadczenia firmy Gigaset Communications GmbH.

Życzymy wiele przyjemności z korzystania z produktów Gigaset.

TR

Sayın Müşterimiz,

Gigaset Communications GmbH, Siemens AG'nin Gigaset işletmesini yürüten Siemens Home and Office Communication Devices GmbH & Co. KG (SHC)'nin yasal halefidir. Kullanma kılavuzlarında bulunan ve Siemens AG veya SHC tarafından yapılan bildiriler Gigaset Communications GmbH tarafından yapılmış bildiriler olarak algılanmalıdır.

Gigaset'ten memnun kalmanızı ümit ediyoruz.

RU

Уважаемыи покупатель!

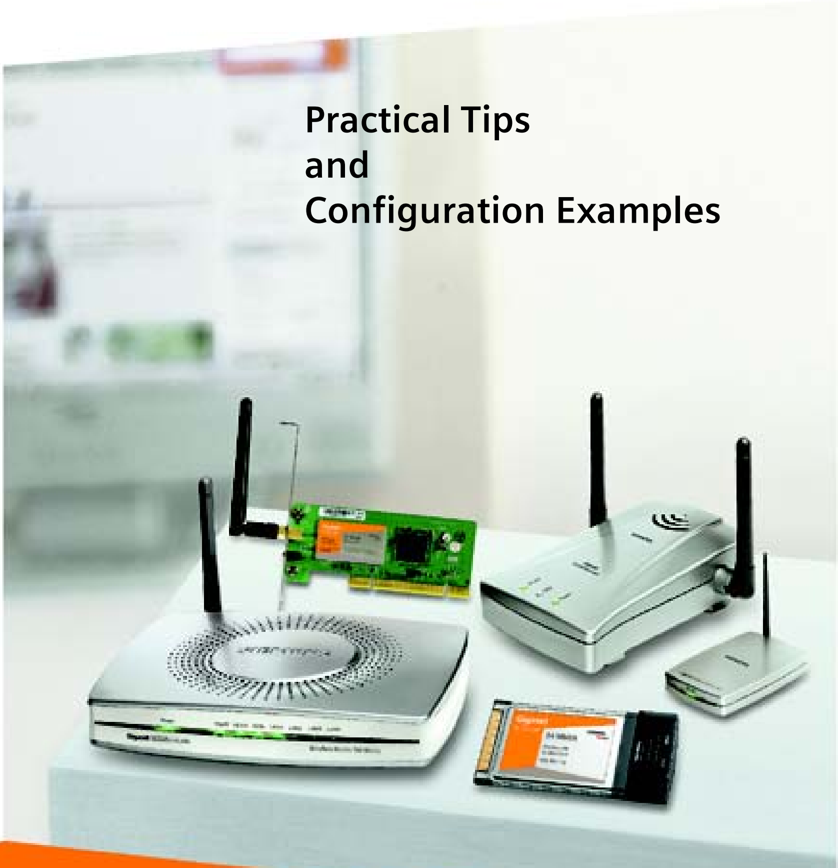
Компания Gigaset Communications GmbH является правопреемником компании Siemens Home and Office Communication Devices GmbH & Co. KG (SHC), которая, в свою очередь, приняла подразделение Gigaset в свое управление от компании Siemens AG. Поэтому любые заявления, сделанные от имени компании Siemens AG или SHC и встречающиеся в руководствах пользователя, должны восприниматься как заявления компании Gigaset Communications GmbH.

Мы надеемся, что продукты Gigaset удовлетворяют вашим требованиям.

Issued by
Gigaset Communications GmbH
Schlavenhorst 66, D-46395 Bocholt
Gigaset Communications GmbH is a trademark licensee of Siemens AG

www.gigaset.com

SIEMENS
mobile



Practical Tips
and
Configuration Examples

Gigaset SE505 dsl/cable
Gigaset PC Card 54
Gigaset PCI card 54
Gigaset USB Adapter 54
Gigaset WLAN Repeater

Gigaset

Contents

Introduction 4

Connecting PCs simply and quickly 14

Extending the network using repeaters 19

Restricting access to the Internet 28

Configuring security features 36

Introduction

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

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

Please note:

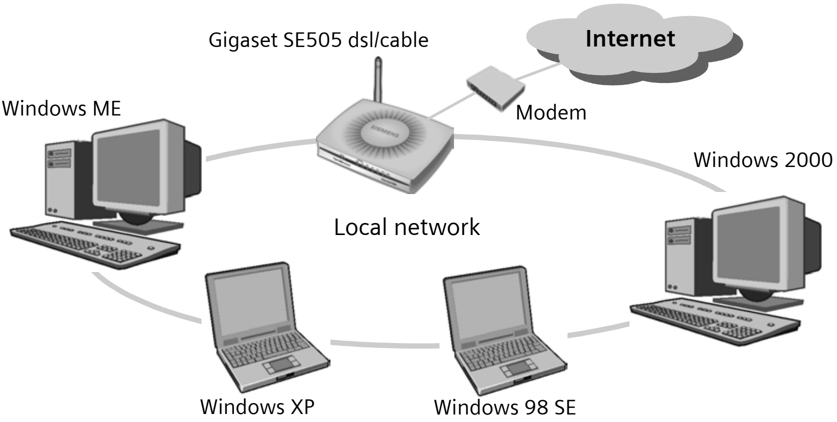
- The user interfaces depicted in this guide may differ from those on your screen because of the settings you have made. For Windows screens, the default state has been presented. There may also be minor differences due to different update cycles of user interface and this manual.
- In the examples we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

Trademarks

Microsoft, Windows 98, Windows 98 SE, Windows ME, Windows 2000, Windows XP, 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).

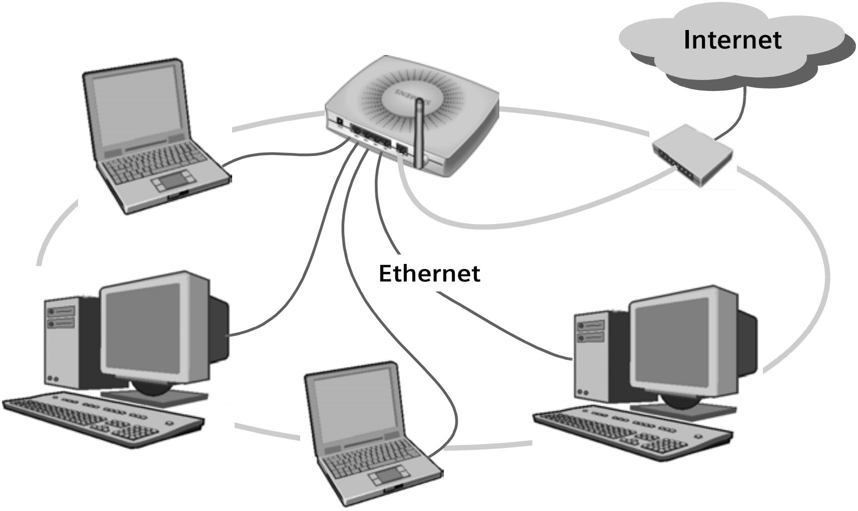


You can set up the network in a number of ways. You can

- 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 Gigaset PC Card 54, Gigaset PCI Card 54 wireless network adapters or a Gigaset USB Adapter to set up a wireless network without routers, i.e. connect PCs directly with each other (see page 7) or connect them to a Gigaset SE505 dsl/cable (see page 8).
- use one or more Gigaset WLAN Repeaters to extend the range of your wireless local network (see page 11).

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 WAN interface on the Gigaset SE505 dsl/cable allows all PCs in the network to access the Internet simultaneously. To use this feature you will need the access data from an Internet Service Provider, e. g. T-Online.

Wireless local network (WLAN)

The PCs must be equipped with a wireless network adapter (e.g. the Gigaset PC Card 54, Gigaset PCI Card 54 or Gigaset USB Adapter). The PCs must be equipped with a wireless network adapter (e.g. the Gigaset PC Card 54, Gigaset PCI Card 54 or Gigaset USB Adapter).

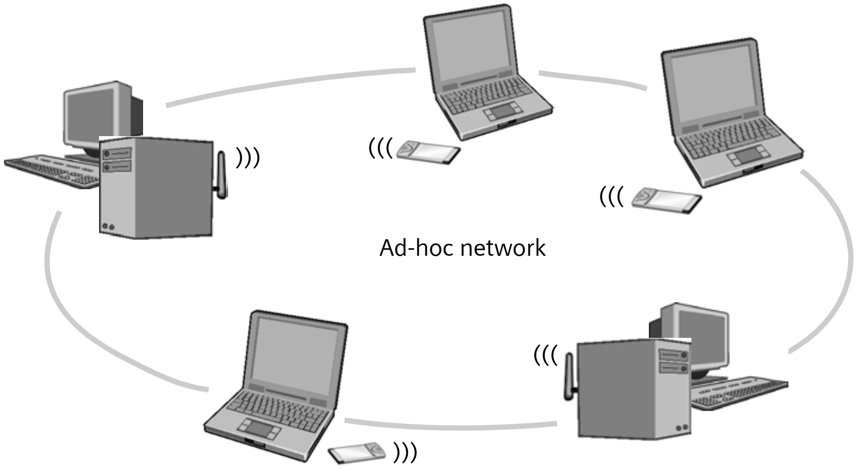
We generally differentiate between two types of wireless networks:

- ad-hoc mode
- infrastructure mode

Ad-hoc network

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

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



How to set up an ad-hoc network is described in Chapter "Connecting PCs simply and quickly" from page 14.

Infrastructure Network

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

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

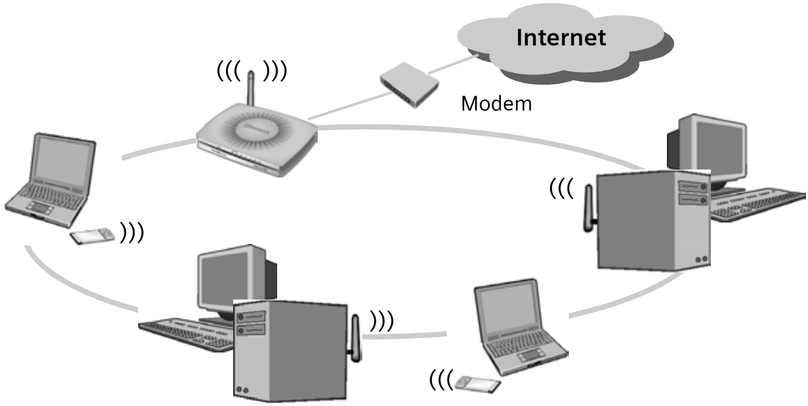
The Gigaset SE505 dsl/cable is such an access point. You can use it for connecting

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

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

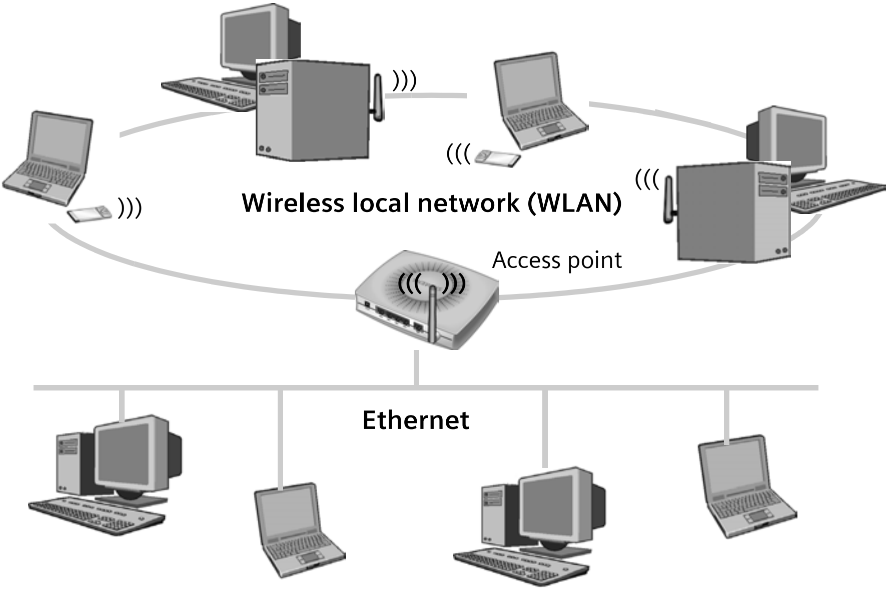
Connecting wireless networks to the Internet

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 a wired network (LAN)

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



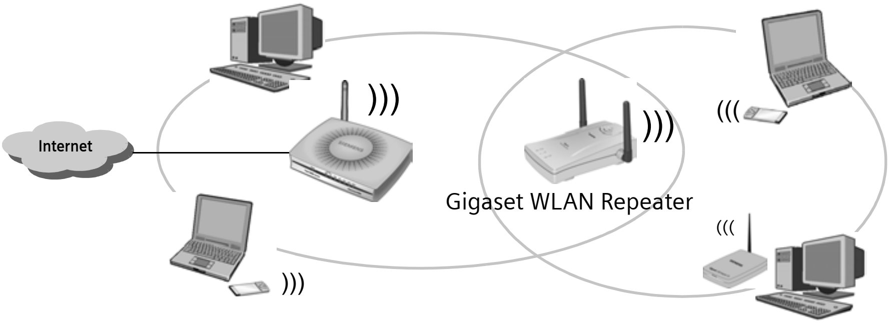
The Gigaset SE505 dsl/cable has four Ethernet interfaces (LAN ports). Up to four PCs can be connected directly to these LAN ports. These PCs also access the Internet via the Gigaset SE505 dsl/cable.

Please note:

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

Extending a wireless network using a repeater

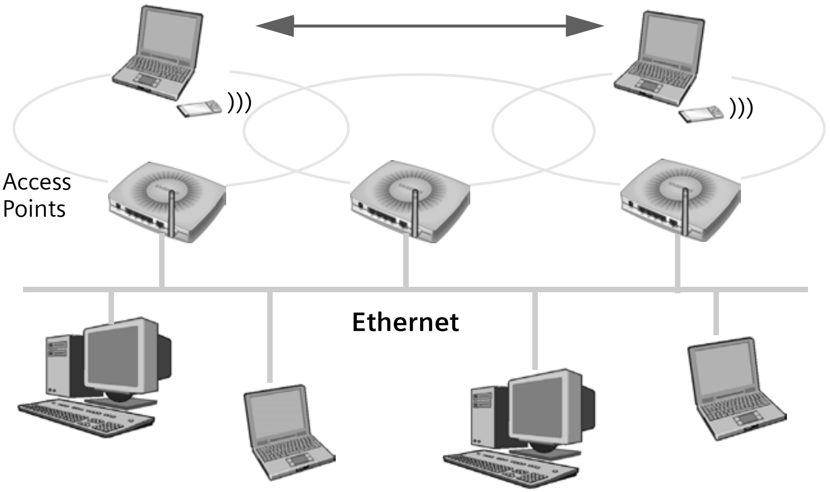
You can use a repeater, e.g. the Gigaset WLAN Repeater to extend the coverage of your wireless network. To do this, set it up at the limit of the range of your wireless network. The Gigaset WLAN Repeater will now transmit data traffic into its own wireless area. This technology allows you to set up wireless networks that cover a much larger area than would be possible with the Gigaset SE505 dsl/cable alone.



PCs that are to be integrated into a wireless local network using a Gigaset WLAN Repeater must be equipped with a wireless network adapter or a USB adapter. For details of how to enlarge your wireless network using a repeater, refer to "Extending the network using repeaters" on page 19.

Roaming

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



In a roaming network, all the users must use the same SSID (see page 38) and encryption (see page 39). The access point must be connected to a wired network (Ethernet). For details, refer to the operating instructions on the CD supplied.

Possible uses

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

- **Shared use of files**

  You can 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 79
  – for Windows XP from page 95
  – for Windows 2000 from page 115

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

  – for Windows 98, 98 SE, ME from page 83
  – for Windows XP from page 101
  – for Windows 2000 from page 120

- **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 80
  – for Windows XP from page 97
  – for Windows 2000 from page 119

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

  – for Windows 98, 98 SE, ME from page 86
  – for Windows XP from page 104
  – for Windows 2000 from page 124

- **Controlled access to the Internet**

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

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

  How to set up these control functions is described in Chapter "Restricting access to the Internet" from page 28.

- **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 36.

- **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 56 and "Network conferences with MS Netmeeting" from page 60.

- **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 63.

Connecting PCs simply and quickly

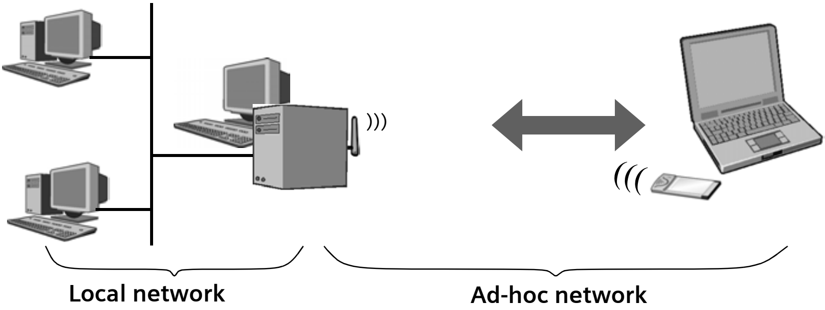
The easiest and fastest way of connecting two or more PCs is using an ad-hoc network (see also page 7). In an ad-hoc network all PCs have the same rights. Each PC can provide resources that can be used by users on the other PCs. This permits fast data exchange or shared use of files and printers (see also Chapter "Sharing files and printers" on page 69).

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 is that each PC to be included in the ad-hoc network is equipped with a wireless adapter, e.g. the Gigaset PC Card 54, Gigaset PCI Card 54 or a Gigaset USB Adapter.

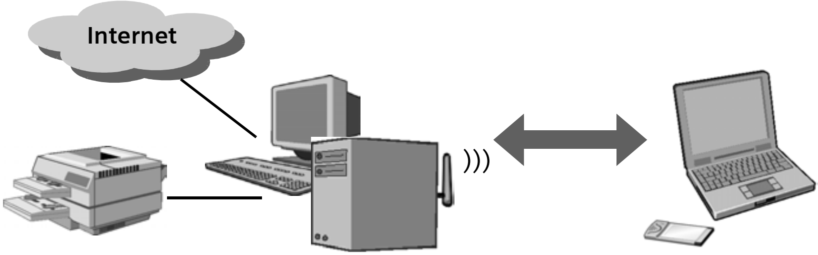
Using ad-hoc networks

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

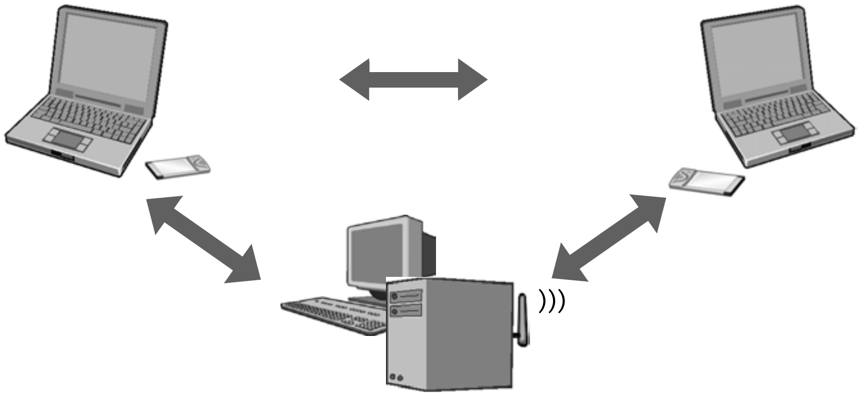
- You want to integrate your notebook into an existing local network temporarily to exchange files or programs for example.



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



- 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, the Gigaset PCI Card 54 or a Gigaset USB Adapter must be installed on all PCs that are to communicate with one another. 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.

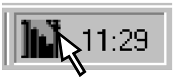
  Depending on the operating systems used in your network, ad-hoc mode may lead to communications problems if dynamic IP addresses are used. Therefore you should assign static IP addresses. You can find further information about this in the appendix on page 126.

Setting network adapters for ad-hoc mode

For ad-hoc mode, you must reconfigure your Gigaset PC Card 54, Gigaset PCI Card 54 or your Gigaset USB Adapter. You can do this using the Gigaset WLAN Adapter Monitor.

To configure the ad-hoc mode on your PC:

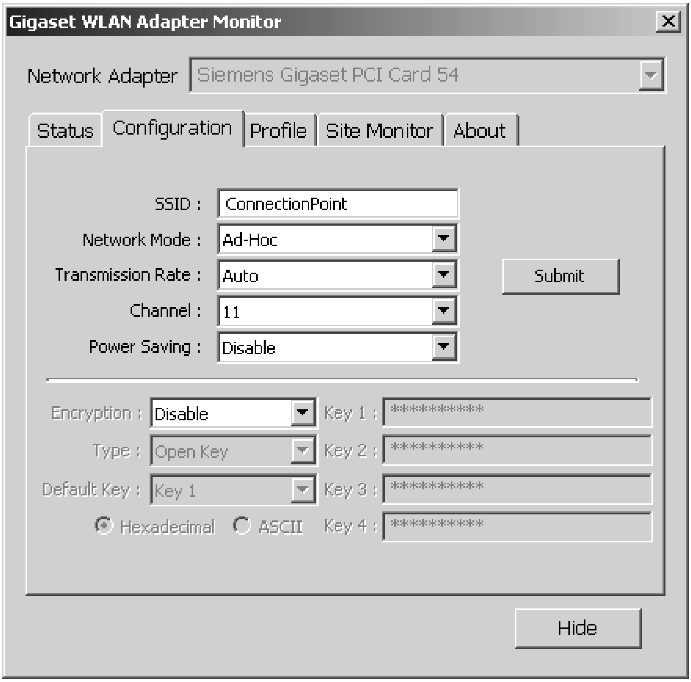
→ Start the Gigaset WLAN Adapter Monitor by double clicking on the icon in the taskbar.



The ***Gigaset WLAN Adapter Monitor*** is displayed.

→ Open the ***Configuration*** tab.

(The user interfaces may vary slightly according to the device used.)



Gigaset WLAN Adapter Monitor

Network Adapter Siemens Gigaset PCI Card 54

SSID : ConnectionPoint

Network Mode : Ad-Hoc

Transmission Rate : Auto

Channel : 11

Power Saving : Disable

Encryption : Disable

Type : Open Key

Default Key : Key 1

● Hexadecimal ○ ASCII

Key 1 : ***********

Key 2 : ***********

Key 3 : ***********

Key 4 : ***********

→ In the ***Network mode*** list, select the entry ***Ad-hoc***.

Please note:
You must use the same values for ***Channel***, ***SSID*** and ***Encryption*** on all PCs involved.

→ Click ***Submit***.

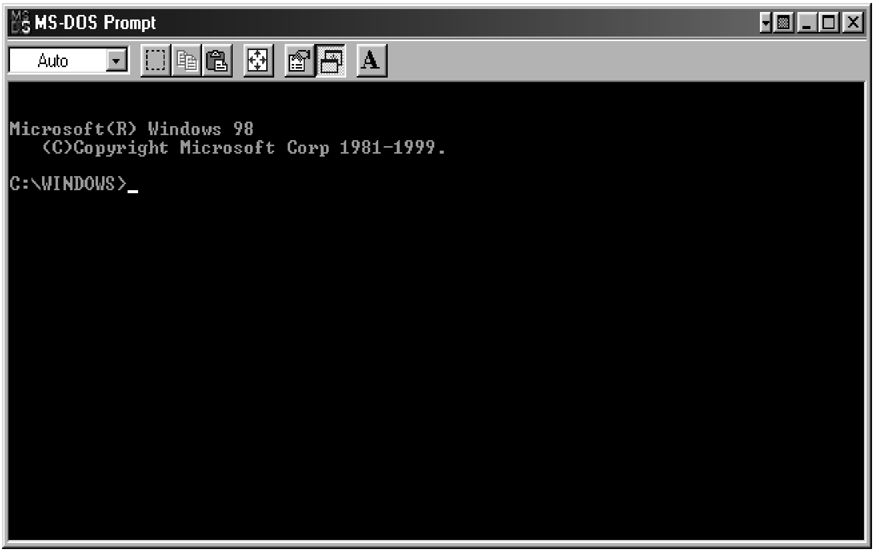
→ Click ***Hide*** to close the window.

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 ***MS-DOS prompt***. This can be done by clicking ***Start*** – ***Programs*** – ***Accessories*** – ***Command Prompt***.



```
Microsoft(R) Windows 98
   (C)Copyright Microsoft Corp 1981-1999.

C:\WINDOWS>_
```

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

Example:

You want to connect three PCs in your ad-hoc network. You have assigned the IP addresses 192.168.2.101 (PC 1), 192.168.2.102 (PC 2) and 192.168.2.103 (PC 3) for the PCs.

Enter in the command prompt on PC 1:

`ping 192.168.2.102` (checks whether data exchange with PC 2 is possible)
`ping 192.168.2.103` (checks whether data exchange with PC 3 is possible)

Apply the same procedure on the other PCs.

Please note:

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.

Extending the network using repeaters

You can use repeaters to extend the range of the Gigaset SE505 dsl/cable in your network. Two options for using the Gigaset WLAN Repeater are described below:

- Extending wireless coverage using a Gigaset WLAN Repeater
- Roaming using several Gigaset WLAN Repeater

Extending the network wireless coverage

The Gigaset WLAN Repeater uses the functionality of the Wireless Distribution System (WDS) to extend the range of an existing wireless network (see also "Extending a wireless network using a repeater" on page 10).

To achieve this, you must configure the Gigaset WLAN Repeater accordingly and activate the Wireless Distribution System (WDS) function on the Gigaset SE505 dsl/cable.

This is done as follows:

1. On the Gigaset SE505 dsl/cable make the settings for operation with a repeater (see below).
2. If necessary, disable encryption (WEP) and MAC control on the Gigaset SE505 dsl/cable (see page 20).
3. Configure the Gigaset WLAN Repeater to work with the Gigaset SE505 dsl/cable (see page 21). Do not set any encryption yet.
4. Now test the connection between the router and the repeater (see page 22).
5. Set WEP encryption on the router and the repeater (see page 23).
6. Make the necessary settings on the PCs to integrate them into the network (see page 24).

Settings on the Gigaset SE505 dsl/cable

To start configuration, proceed as follows:

→ Start your Internet browser.

→ Enter the router IP address in the address bar of your Internet browser. Unless you have configured the router with a different IP address, this will be

`http://192.168.2.1`

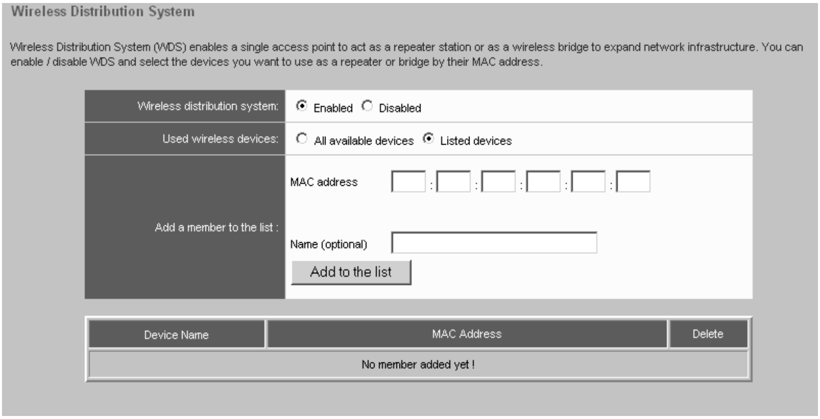
You will then see an Internet site containing a login dialog.

→ If a password has already been assigned, enter it and click ***LOGIN***.

→ After successfully logging in, select ***Advanced Setup***.

Wireless Distribution System (WDS)

→ In the ***Wireless Settings*** menu, select ***Wireless Distribution System.***



Wireless Distribution System

Wireless Distribution System (WDS) enables a single access point to act as a repeater station or as a wireless bridge to expand network infrastructure. You can enable / disable WDS and select the devices you want to use as a repeater or bridge by their MAC address.

Wireless distribution system:	● Enabled ○ Disabled
Used wireless devices:	○ All available devices ● Listed devices
Add a member to the list :	MAC address □ : □ : □ : □ : □ : □ Name (optional) □ Add to the list

Device Name	MAC Address	Delete
No member added yet !		

→ In the ***Wireless Distribution System*** field, select the ***Enabled*** option.

→ In the ***Used wireless devices*** field, select ***Listed devices*** and enter the MAC address of the repeater in the fields underneath. The MAC address of the repeater can be found on the underside of the device or on the Gigaset WLAN Adapter Monitor site monitor.

→ Enter the name of your choice for the repeater. This name helps you to identify the various devices more easily.

→ Click on ***Add to list***.

The repeater is added to the list.

→ Click on ***APPLY***.

Basic settings

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

→ Activate the wireless module on the repeater.

→ Change the default SSID, e.g. ***my_router***, and note the name.

LAN settings

→ Open the ***LAN*** menu.

→ Use the default IP address 192.168.2.1, and 255.255.255.0 as the subnet mask (menu option ***IP of internal router***).

→ Activate the DHCP server for automatic assignment of IP addresses to the connected devices (menu option ***DHCP server***)

Disabling encryption and access control

First of all, disable encryption until you have made the basic settings on the repeater and tested the connection to the repeater.

→ In the ***Wireless Settings*** menu, select ***Encryption***.

- Depending on the set encryption type, change the following selection fields: For ***Network Authentication*** select ***disabled***, for ***Data encryption*** select ***off***.
- In the ***Wireless Settings*** menu, select ***Access control*** and disable it.

Configuring the Gigaset WLAN Repeater

To prepare for configuration, first of all carry out the following steps:

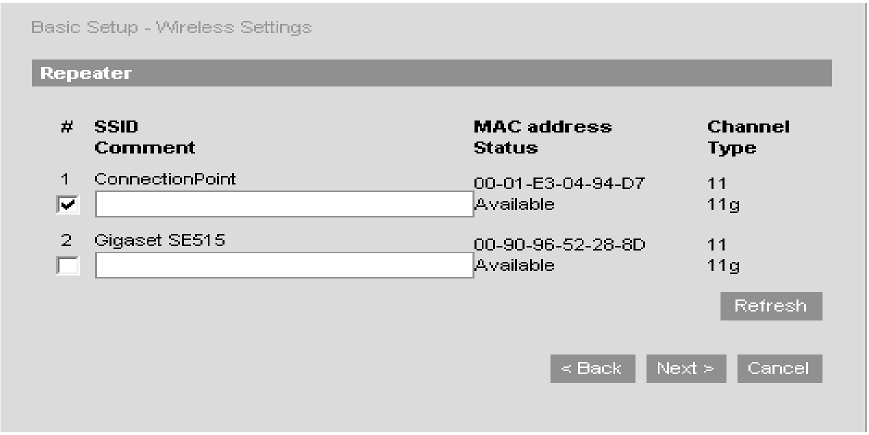
- Using a cable, connect the repeater to the PC you want to use for configuration and turn on the repeater.
- Update your PC's IP address. To do this, open the command prompt (***Start*** – ***All Programs*** – ***Accessories*** – ***Command Prompt***) and enter the commands **`ipconfig /release`** and **`ipconfig /renew`** one after the other. The PC is connected to the repeater and you can now call up its configuration program.

The Gigaset WLAN Repeater is preset as the repeater in the factory. Therefore, you only have to make a few entries for the basic and security settings.

- Start your Internet browser.
- Enter the repeater IP address in the address bar of your Internet browser. Unless you have configured your device with a different IP address, this will be

  192.168.2.254

  You will then see an Internet site containing a login dialog.
- If a password has already been assigned, enter it and click ***OK*** (the default settings is **admin**).
- After successfully logging in, select ***Basic Setup***.
- In the next two windows, click on ***Next***.
- On the ***Repeater*** page, select the Gigaset SE505 dsl/cable, whose range you want to extend.



Basic Setup - Wireless Settings

Repeater

#	SSID Comment	MAC address Status	Channel Type
1 ☑	ConnectionPoint	00-01-E3-04-94-D7 Available	11 11g
2 ☐	Gigaset SE515	00-90-96-52-28-8D Available	11 11g

You will now see a list of all access points that can be reached with their SSID, MAC address, wireless channel and type.

- To refresh the display, click on ***Refresh***.
- Select the check box with the SSID (***my_router***) for the Gigaset SE505 dsl/cable.
- Enter a name for the router in the box below the SSID. This name will help you to identify the various devices more easily.
- Click on ***Next.***

WLAN settings

- Next enter the SSID of the repeater on the ***Wireless Network*** page. The radio channel is automatically transferred from the router.
- Click on ***Next.***

LAN settings

In the next step, you will see the ***LAN*** screen for the basic settings of your local network.

- Under ***IP address type***, activate the ***Obtained automatically*** option.

  The repeater then obtains its IP address from the router.
- Exit the basic settings.

Testing the connection between the router and the repeater

Once you have made the basic settings on the repeater, it should be possible to establish a connection between the repeater and the Gigaset SE505 dsl/cable.

- Open a new browser window and enter the IP address of the Gigaset SE505 dsl/cable (default 192.168.2.1).

The start window for the router configuration program then appears. If not, check the settings made previously on the router and the repeater, as described above.

Setting WEP encryption on the router and the repeater

If you were able to establish a connection between the router and the repeater after completing the basic settings on the two devices, now set the encryption you want to use to protect your wireless data transmission from eavesdropping.

Setting the encryption on the repeater

In the configuration program, select ***Advanced Setup*** – ***Security*** – ***WEP***.

- → Enable WEP encryption on the Gigaset WLAN Repeater.
- → Select the ***WEP encryption length*** corresponding to the settings on the Gigaset SE505 dsl/cable (128 bit).
- → Enter the 128-bit key you are using for the router (e.g. 234567ABC8912345DEF1234567) in the ***Key 1*** field. The box next to ***Passphrase*** must not be checked.
- → In the ***Default key*** list, select the number of the field in which you entered your key, i.e. ***1***.
- → Click on ***OK***.

You can now set up the repeater at the desired location.

Setting the encryption on the router

For operation with a Gigaset WLAN Repeater the only encryption method currently supported is WEP encryption.

- → Connect the router to the PC using a cable and start the configuration program.
- → In the ***Wireless Settings*** menu, select ***Encryption***.
- → Enable WEP encryption. If you have not yet set any encryption, set the same 128-bit key as is set on the repeater, e.g. 234567ABC8912345DEF1234567 (see "64- and 128-bit key" on page 40). Note the key, as you will need it for configuration of the network adapters.

The connection between the router and the repeater should now work again.

Please note:

The wireless connection to wireless connected PCs is interrupted until you have also set up WEP encryption on the PCs' network adapters.

Settings on the PCs in the wireless network

PCs that are to be integrated into a wireless local network using a Gigaset WLAN Repeater must be equipped with a wireless network adapter (Gigaset PC Card 54, Gigaset PCI Card 54 or a Gigaset USB Adapter).

➙ Set the PCs to automatically obtain the IP address (see "Configuring the local network" in the operating instructions on the CD).

➙ Set WEP encryption on the network adapter. Use the same 128-bit key as for the router and the repeater (e.g. 234567ABC8912345DEF1234567). Refer to "Setting WEP encryption on the network adapters" on page 48 for details.

➙ Now edit and activate the list for MAC access control on the router (see page 42).

➙ You should restart all the devices once all the configuration settings have been made.

Roaming using repeaters

The Gigaset WLAN Repeater enables you to use roaming in your network. Roaming provides optimum connection quality and uninterrupted data transmission while you move around within the range of your network. Your PC always automatically establishes a connection to the access point via the repeater with the strongest signal, without interrupting data traffic (see also "Roaming" on page 11).

To operate a network with roaming, note the following:

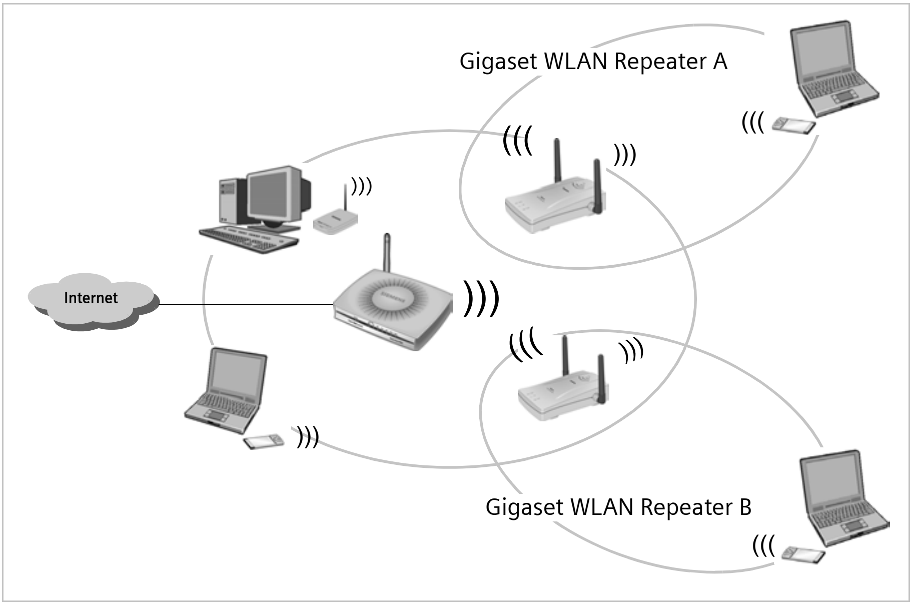
◆ The same SSID must be used on all components in your network, i.e. on the router, the repeater and the PCs' network adapters.

◆ The same radio channel must be used. This setting is normally made automatically.

◆ All components must be located in the same IP subnet. This means:
  - You must use the same subnet mask (e.g. 255.255.255.0).
  - With a subnet mask of 255.255.255.0 only the last section of the IP addresses may be different.

◆ If the DHCP server is activated on the repeaters, address blocks for the IP addresses to be assigned may not overlap.

Example of roaming with two repeaters



In the example below, the two repeaters are configured with the following settings:

Repeater A IP address: 192.168.2.210

Address block for PCs connected to repeater A: 192.186.2.211 - 192.186.2.229

Repeater B IP address: 192.168.2.230

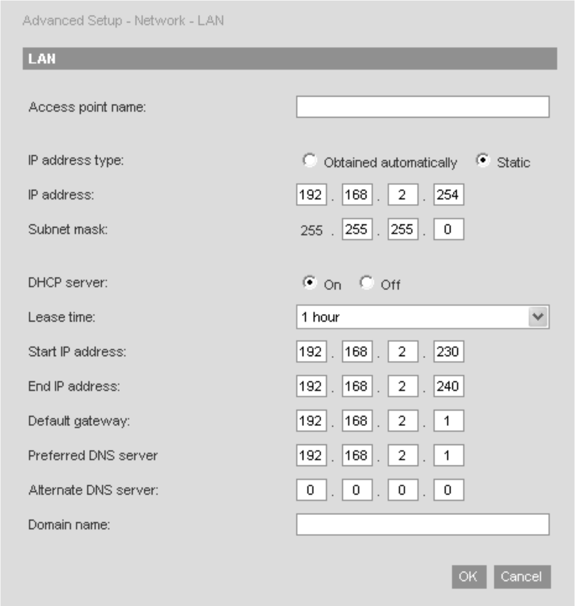
Address block for PCs connected to repeater B: 192.186.2.231 - 192.186.2.249

The Gigaset SE505 dsl/cable that acts as the access point has the IP address 192.168.2.1.

The configuration settings described below must be made separately for each of the two repeaters. To do this, connect each of the repeaters in turn to a PC using a cable.

→ Log into the configuration program as described in section "Configuring the Gigaset WLAN Repeater" on page 21.

→ In the ***Advanced Setup*** – ***Network*** menu in the configuration program, select the ***LAN*** option.



Advanced Setup - Network - LAN

LAN

Access point name:	
IP address type:	○ Obtained automatically ● Static
IP address:	192 . 168 . 2 . 254
Subnet mask:	255 . 255 . 255 . 0
DHCP server:	● On ○ Off
Lease time:	1 hour
Start IP address:	192 . 168 . 2 . 230
End IP address:	192 . 168 . 2 . 240
Default gateway:	192 . 168 . 2 . 1
Preferred DNS server	192 . 168 . 2 . 1
Alternate DNS server:	0 . 0 . 0 . 0
Domain name:	

- In the ***Access point name*** field, enter a name for repeater A.
- Under ***IP address type***, select the ***Static*** option.
- In the fields below, enter 192.168.2.210 as the IP address for repeater A and 192.168.2.230 for repeater B and enter 255.255.255.0 as the subnet mask.
- For ***DHCP server***, select the ***On*** option.
- In ***Lease time***, specify how long the PCs should retain the assigned IP addresses before changing them. You can set the connection time to ***Unlimited***. This means that an IP address is assigned for an unlimited period of time.

The values of ***Start IP / End IP*** define the range of IP addresses that repeater A is to use to automatically assign IP addresses to PCs.

- Select 192.168.2.211 to 192.168.2.229 as the address range for repeater A and 192.168.2.231 to 192.168.2.249 for repeater B.
- In the ***Default gateway*** and ***Preferred DNS server*** fields, enter the IP address of the Gigaset SE505 dsl/cable.
- Click on ***OK*** to apply the settings.

Please note:

- The address block you enter must not overlap with those of DHCP servers in your network or static address of devices connected to your network. Otherwise there might be IP address conflicts if the same IP address is assigned to several devices in your network. This can impair or block the reachability of some or all of the devices in your network.
- The first three fields of the first and last IP address must always be identical to the first three fields of your Gigaset WLAN Repeater's IP address, as the subnet mask is always 255.255.255.x. This means that the first three address segments for all network components must be identical.

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 29)

  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 34)

  This allows you to prevent a particular Internet site with a particular URL address or Internet sites from a particular domain from being displayed.

  Example:

  - Blocking the URL http://www.abcd.com means that no Internet sites from the domain www.abcd.com are displayed.
  - Blocking the URL http://www.abcd.com/produkte means that the specific Internet site http://www.abcd.com/produkte and all subordinate sites are blocked.

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:

- 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.

- 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 note:**
>
> Changing the network adapter renders the PC's authorization ineffective, as a different adapter also has 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 series of Internet addresses (URLs) is 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. Configure access to Internet services (see page 29).

   Create a filter list with

   – an entry for the PC "My_PC" with unrestricted access (see page 31),

   – an entry for Peter's PC with access to "SuperService" (see page 32),

   – an entry for Anna's PC with access to the HTTP service (see page 33).
2. Block access to particular Internet sites by defining URL blocks (see page 34).

Starting filter configuration

To start filter configuration:

➞ Start your Internet browser.

➞ Enter the router IP address in the address bar of your Internet browser. If you have not configured the router with a different IP address, this will be

```
http://192.168.2.1
```

You will then see an Internet site containing a login dialog.

➞ If a password has already been assigned, enter it and click ***LOGIN***.

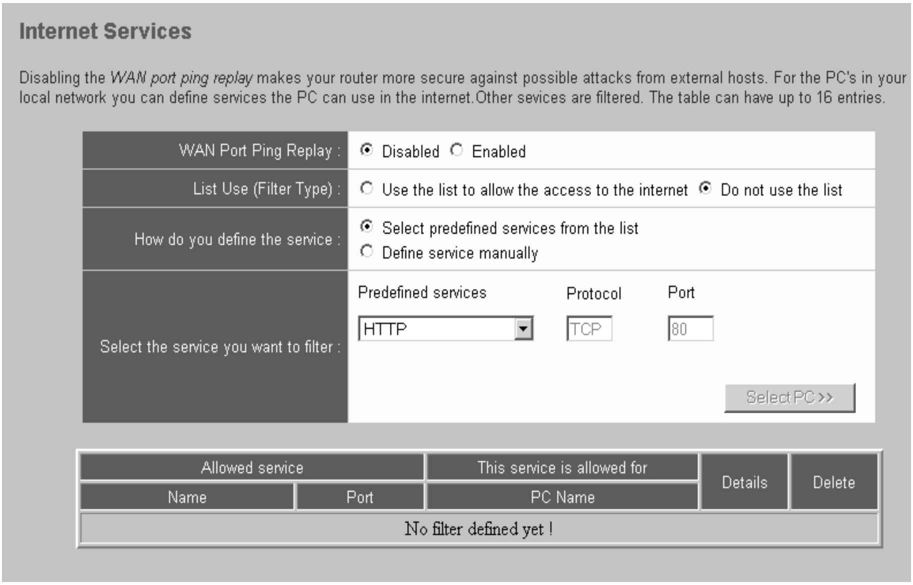
➞ After logging in, select ***Advanced Setup***.

➞ 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 sevices 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: HTTP Protocol: TCP Port: 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.

Please note:

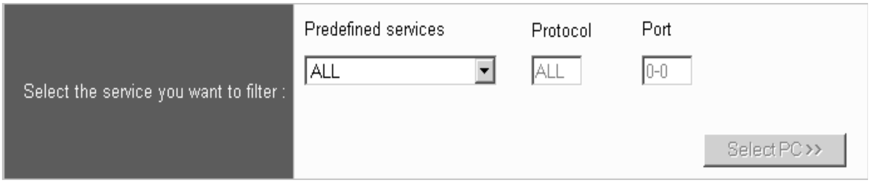
If you block the Internet access for the PC you are using you will no longer have any access to your Gigaset Router user interface because you have to enter an http address to open it and thus use an Internet service. The access block applies once you activate the filter. If you have accidentally blocked access to the user interface, you will have to reset the router. To do this, press the Reset button on the rear of the device for at least seven seconds. Please bear in mind that this will restore **all** configuration settings to the factory settings.

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:

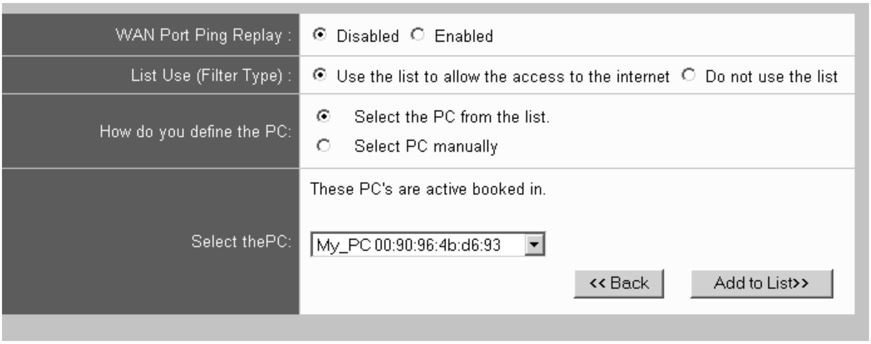
→ Open the ***Predefined services*** selection list and select the entry ***ALL***.



Select the service you want to filter :

Predefined services	Protocol	Port
ALL	ALL	0-0

→ Click ***Select PC>>***

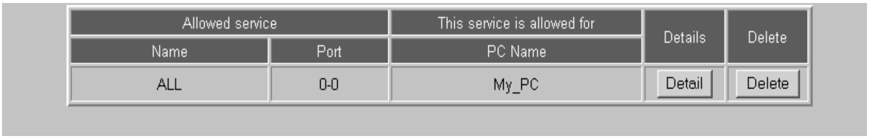


WAN Port Ping Replay :	● Disabled ○ Enabled
List Use (Filter Type) :	● Use the list to allow the access to the internet ○ Do not use the list
How do you define the PC:	● Select the PC from the list. ○ Select PC manually
Select thePC:	These PC's are active booked in. My_PC 00:90:96:4b:d6:93

→ 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

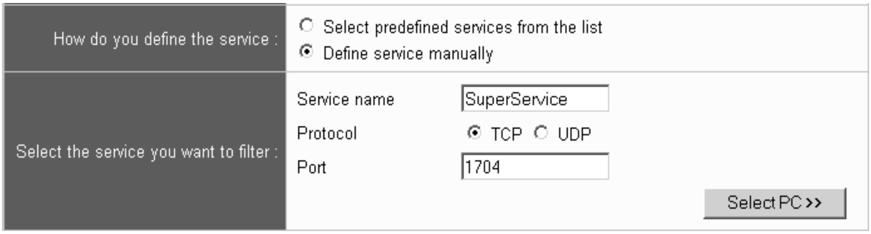
The PC has now been added to the table.

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

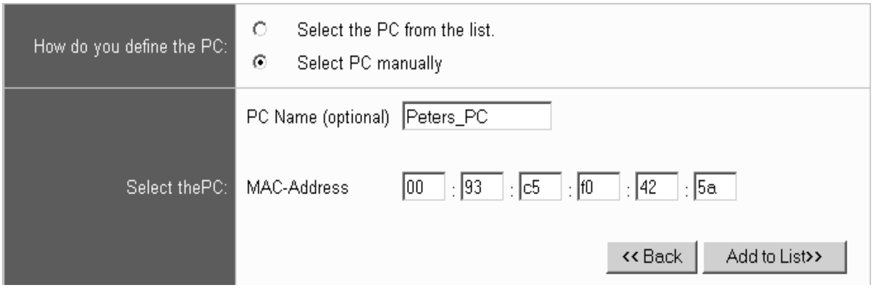
→ Again enter the name of the service.

→ 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***.



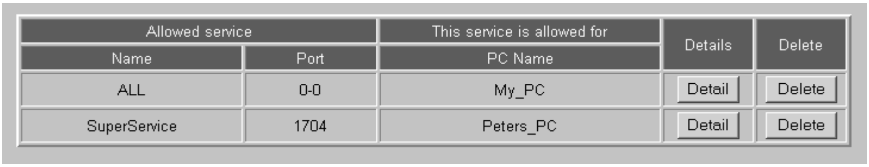
How do you define the PC:	○ Select the PC from the list. ● Select PC manually
Select thePC:	PC Name (optional): Peters_PC MAC-Address: 00 : 93 : c5 : f0 : 42 : 5a

→ 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 28).

→ Click ***Add to list***.

→ Click ***APPLY***.



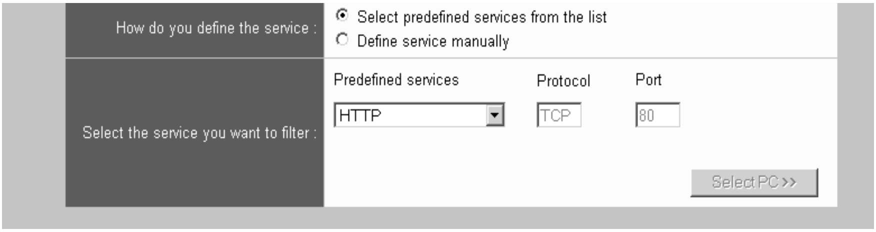
Allowed service		This service is allowed for	Details	Delete
Name	Port	PC Name		
ALL	0-0	My_PC	Detail	Delete
SuperService	1704	Peters_PC	Detail	Delete

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***.

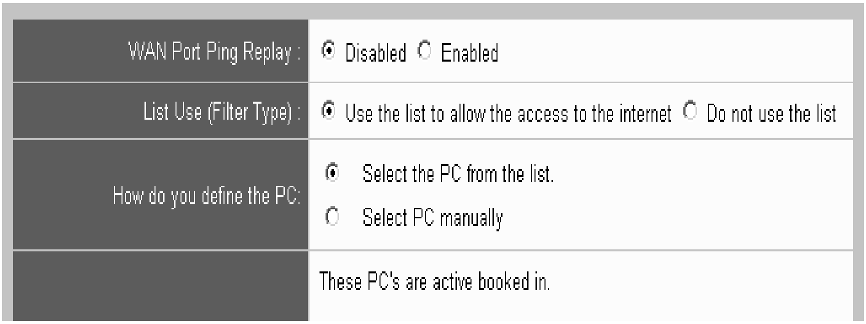


How do you define the service : ● Select predefined services from the list ○ Define service manually

Select the service you want to filter :

Predefined services	Protocol	Port
HTTP	TCP	80

→ 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

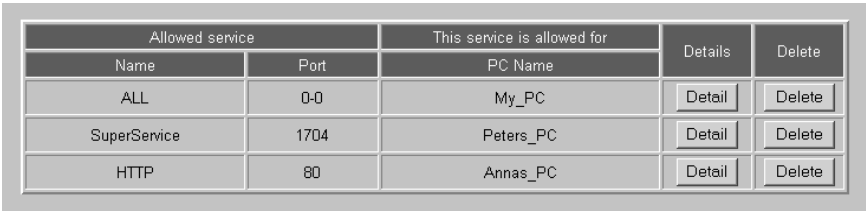
How do you define the PC: ● Select the PC from the list. ○ Select PC manually

These PC's are active booked in.

→ Select the appropriate PC from the list of registered PCs.

→ Click ***Add to list***.

→ Click ***APPLY.***

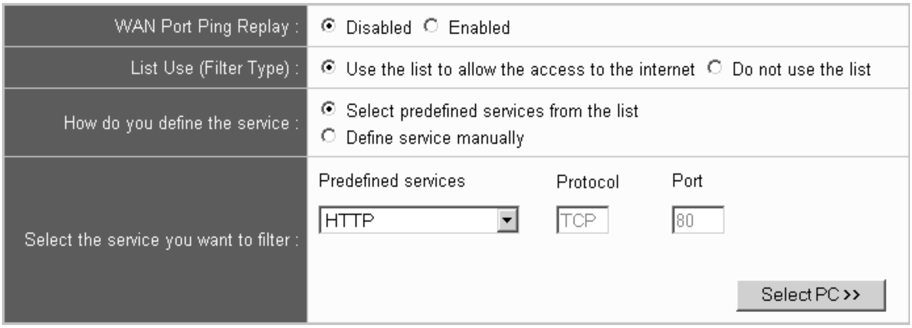


Allowed service		This service is allowed for	Details	Delete
Name	Port	PC Name		
ALL	0-0	My_PC	Detail	Delete
SuperService	1704	Peters_PC	Detail	Delete
HTTP	80	Annas_PC	Detail	Delete

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***.

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

Blocking access to certain Internet pages

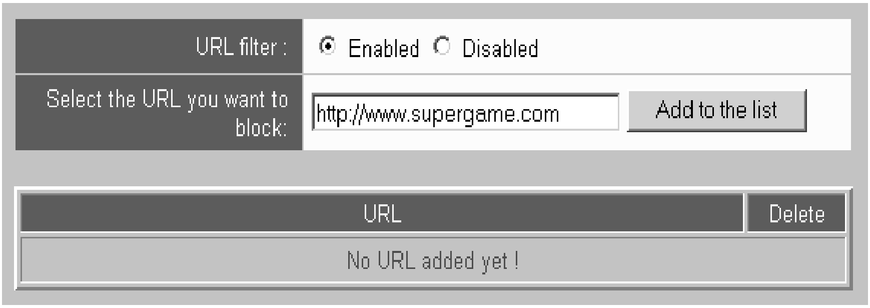
All we have to do now is set up the URL filter for blocking Internet pages.

Please note:
The assigned URL filters must always be valid for **all** PCs.

→ In the left-hand pane, select the option ***Filter*** – ***URL Filter***.

Initially the list is empty.

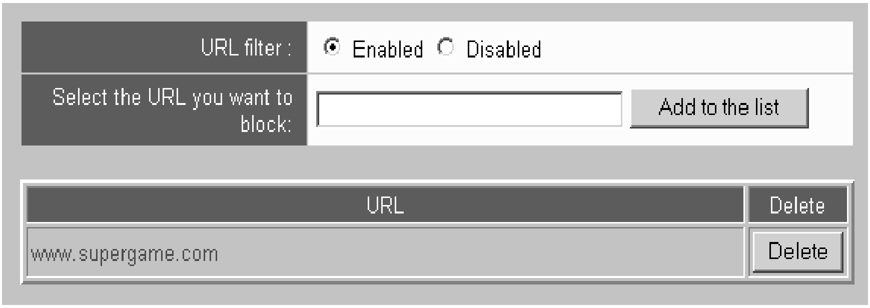
→ Enter the URL you want to block. The specified domain or Internet page and all the subsequent pages will be blocked.



URL filter :	● Enabled ○ Disabled
Select the URL you want to block:	http://www.supergame.com

URL	Delete
No URL added yet !	

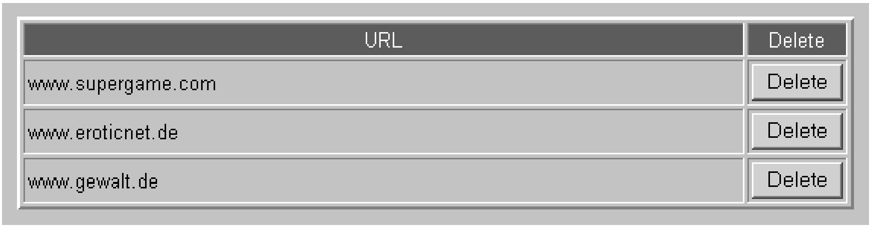
→ Click ***Add to list***.



URL filter :	● Enabled ○ Disabled
Select the URL you want to block:	

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 37).

  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 38).

  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 38).

  Then the router will no longer transmit the new SSID and it can no longer be "read" by eavesdroppers.
- Enable an encryption method (WEP or WPA-PSK) (see page 39).

  The flow of data is encrypted, preventing eavesdropping in the network.
- Create an access table (MAC access table, see page 42)

  This determines which PCs have wireless access to your router. All the others will be excluded.

Please note:

- The SSID, the encryption method and the key used must be the same on all wireless devices.
- 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:

→ Start your Internet browser.

→ Enter the router IP address in the address bar of your Internet browser. Unless you have configured the router with a different IP address, this will be

```
http://192.168.2.1
```

You will then see an Internet site containing a login dialog.

→ If a password has already been assigned, enter it and click ***LOGIN***.

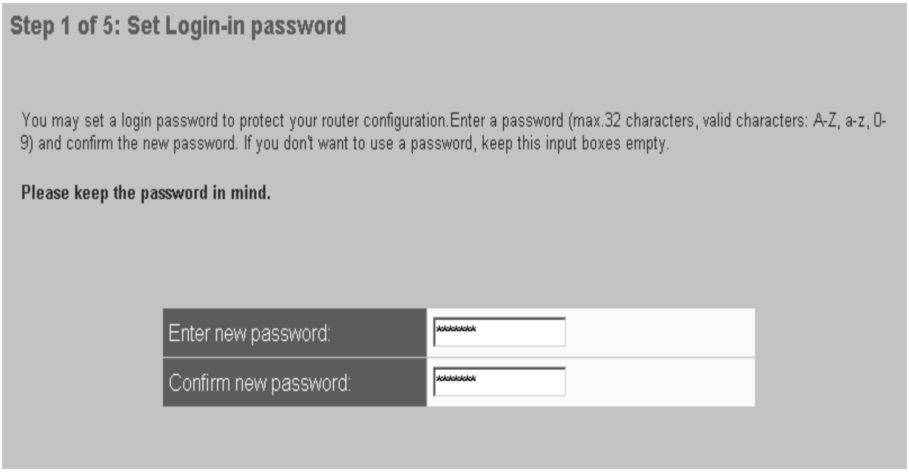
→ After logging in, select ***Security Setup***.

Security Setup takes you through the following steps:

1. Assign configuration password (see page 37)
2. Change the router's SSID (see page 38)
3. Set up encryption (see page 39)
4. Set up access control (see page 42)
5. Back up the configuration (see page 46)

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.

Please note:

Remember the password that you have assigned. If you ever forget the password you will have to reset your router. To do this, press the Reset button on the rear of the device for at least seven seconds. 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***.

Please note:

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

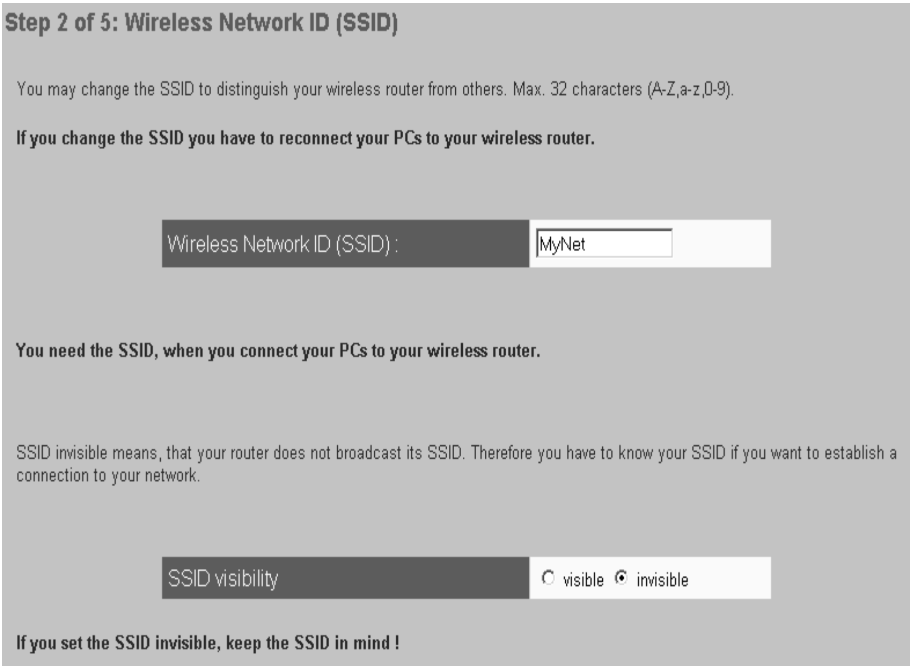
Changing the SSID and disabling Broadcast

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 47).

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) : MyNet

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 alphanumerical characters long. Avoid names and all too obvious words. Mix letters and numbers.

→ In the ***SSID visible*** row, select the option ***invisible***. This disables the broadcast function for the SSID.

→ To apply the settings click ***NEXT***.

> **Please note:**
>
> 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. For details of how to do this on a Siemens Gigaset PC Card 54, Siemens Gigaset PCI Card 54 or a Siemens Gigaset USB Adapter, refer to page 47.

Transferring encrypted data

Wireless networks are even more susceptible to the risk of eavesdropping than wired networks. Given the typical ranges of wireless network adapters all the intruder needs is a laptop or PDA with an appropriately configured network card to listen in on any communications over a nearby wireless LAN. We therefore recommend that you enable one of the following encryption methods on your wireless network components.

- WEP

  The WLAN standard IEEE 802.11 specifies the ***WEP*** (Wired Equivalent Privacy) encryption mechanism for data encryption and authentication of a terminal with a base station (e. g. the Gigaset SE505 dsl/cable). The following section describes the configuration of the router for WEP encryption.
- WPA-PSK

  Encryption and authentication using ***WPA-PSK*** provides a higher level of security. To use ***WPA-PSK***, it is necessary for all components in your wireless network to support WPA-PSK. Details of the Gigaset SE505 dsl/cable settings for ***WPA-PSK*** can be found on page 41.

If you are using a Gigaset WLAN Repeater to extend the range of your network, you must use WEP as your encryption method.

> **Please note:**
>
> WEP or WPA-PSK will protect data that is transferred between wireless stations. However, encryption does not protect transmissions on your wired network or over the Internet.

WEP encryption

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 48).

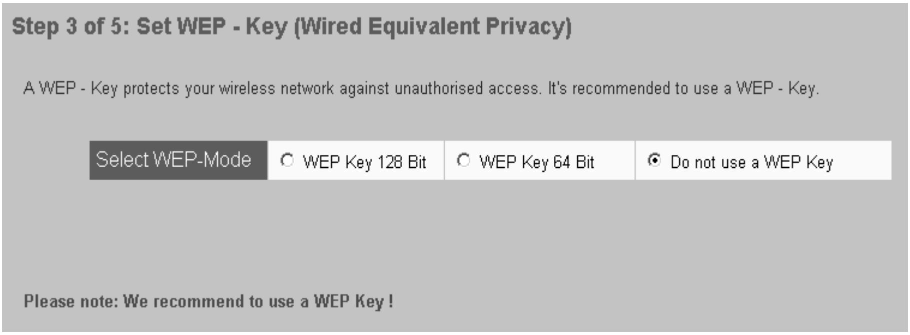
In the following steps we assume that your wireless network has already been set up and is functioning properly.

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.

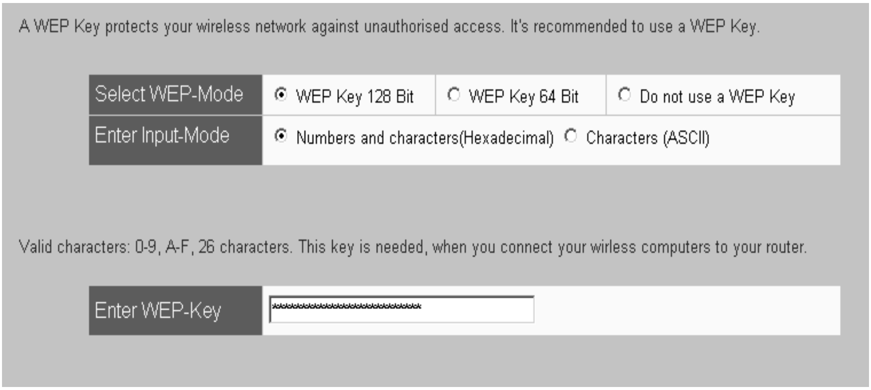
Select WEP-Mode: ○ WEP Key 128 Bit ○ WEP Key 64 Bit ● Do not use a WEP Key

Please note: We recommend to use a WEP Key !

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

The Internet site 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 wirless computers to your router.

Enter WEP-Key: **************************

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.

> **Please note:**
>
> 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***.

> **Please note:**
>
> Use the following function in Advanced Setup if you want to change the WEP key later on: ***Wireless Settings*** – ***Encryption***

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. For details of how to do this on a Siemens Gigaset PC Card 54, Siemens Gigaset PCI Card 54 or a Siemens Gigaset USB Adapter, refer to page 48.

WPA encryption

WPA is a standard method for user identification during network login as well as for data encryption during transmission. WPA is more secure than WEP.

Not all of the network adapters currently available in the Gigaset range support WPA. The necessary settings for the example of the Gigaset USB Adapter are described on page 50. Please check in the operating instructions for your device whether WPA is supported. We recommend that you set this WPA encryption on your wireless network components.

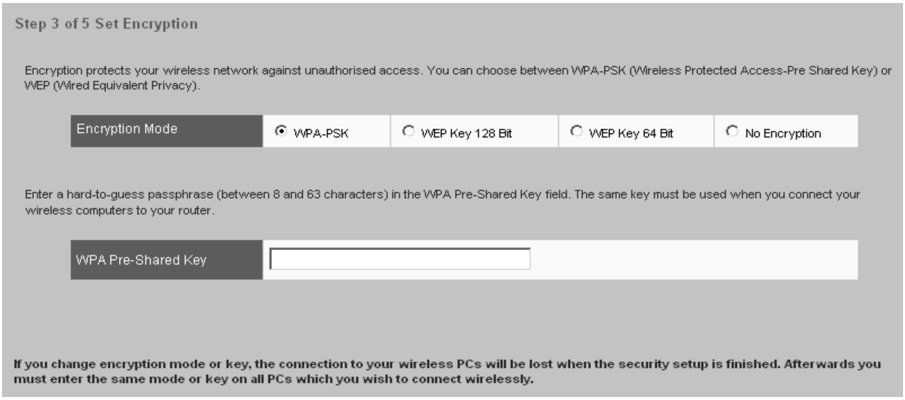
If you also want to use this encryption method with a Gigaset network adapter that does not support WPA, note the following:

◆ Your PCs must run on the Windows XP operating system.

◆ Additional software is needed on the PCs. On the Microsoft website, you will find an update for installing WPA on your PC. Configuration is then carried out using the standard configuration tool for "Wireless Network Connections" in your Windows system. Further information is available on the Microsoft website and under "Configuring WPA encryption under Windows XP" on page 52. No further configuration actions are necessary for the network adapter.

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

→ In the ***Encryption mode*** field, select ***WPA-PSK***.



Step 3 of 5 Set Encryption

Encryption protects your wireless network against unauthorised access. You can choose between WPA-PSK (Wireless Protected Access-Pre Shared Key) or WEP (Wired Equivalent Privacy).

Encryption Mode	● WPA-PSK	○ WEP Key 128 Bit	○ WEP Key 64 Bit	○ No Encryption

Enter a hard-to-guess passphrase (between 8 and 63 characters) in the WPA Pre-Shared Key field. The same key must be used when you connect your wireless computers to your router.

WPA Pre-Shared Key

If you change encryption mode or key, the connection to your wireless PCs will be lost when the security setup is finished. Afterwards you must enter the same mode or key on all PCs which you wish to connect wirelessly.

→ Enter a key in the ***Pre-shared key*** field, e.g. xyz545556cba. Make a note of the key. The key can be made up of between 8 and 63 characters. The same key must be entered when you connect your wireless PCs to the router.

→ To go to the next step in the Security Setup, click on ***NEXT***.

Please note:

To set or modify the WPA key at a later date, use the following function in the advanced setup: ***Wireless Settings*** – ***Encryption***

Once you have connected the Security Setup, you must then set the WPA encryption on the wireless network adapters for the connected PCs, as otherwise they will no longer be able to access the wireless network via the router. For details of how to do this for a SiemensGigaset USB Adapter, refer to page 50. For details of how to set up WPA encrcryption for PCs with network adapters that do not support WPA, refer to page 52.

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.

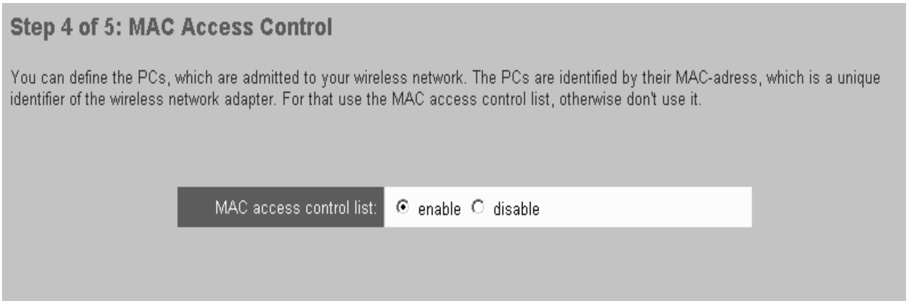
Please note:

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. To do this, press the Reset button on the rear of the device for at least seven seconds. 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

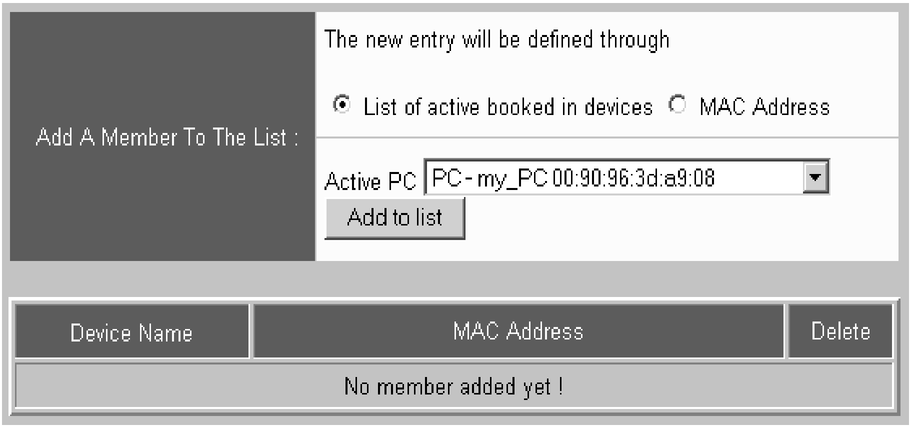
You can define the PCs, which are admitted to your wireless network. The PCs are identified by their MAC-adress, which is a unique identifier of the wireless network adapter. For that use the MAC access control list, otherwise don't use it.

MAC access control list: ● enable ○ disable

To activate access control :

→ Select ***MAC access control list***. 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 PC - my_PC 00:90:96:3d:a9:08 ▾

Add to list

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 logged on PC's*** option.

  – Then select from the list all the PCs that are to have access and then click ***Add to list***.

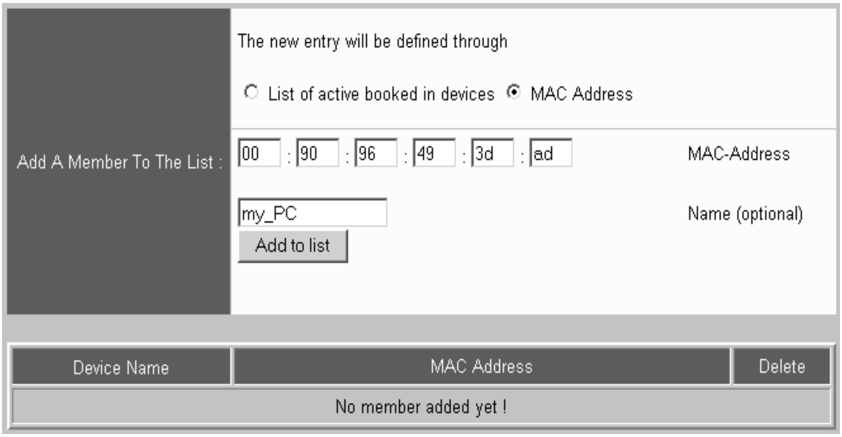
> **Please note:**
>
> If you want to add PCs to the table that are not registered at the moment, first deactivate the MAC access table, register all the PCs you want to include in the table with your router and then reactivate the MAC access table.

- 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.

> **Please note:**
>
> 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.



Add A Member To The List :

The new entry will be defined through

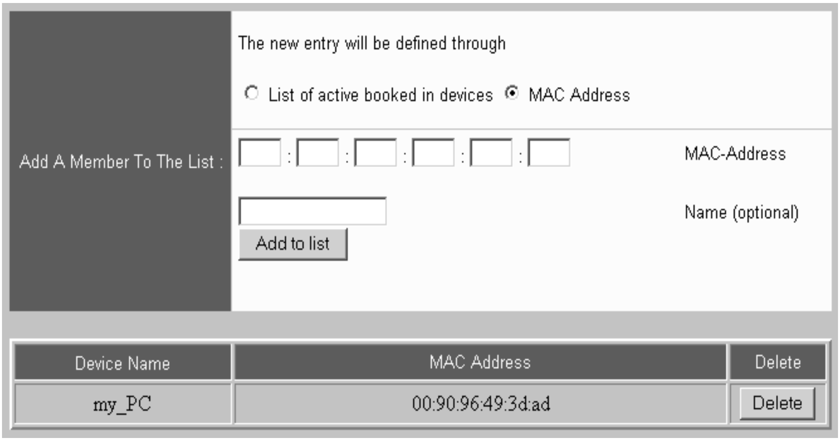
○ List of active booked in devices ● MAC Address

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

Name (optional): my_PC

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***.



Add A Member To The List :

The new entry will be defined through

○ List of active booked in devices ● MAC Address

MAC-Address: □ : □ : □ : □ : □ : □

Name (optional): □

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.

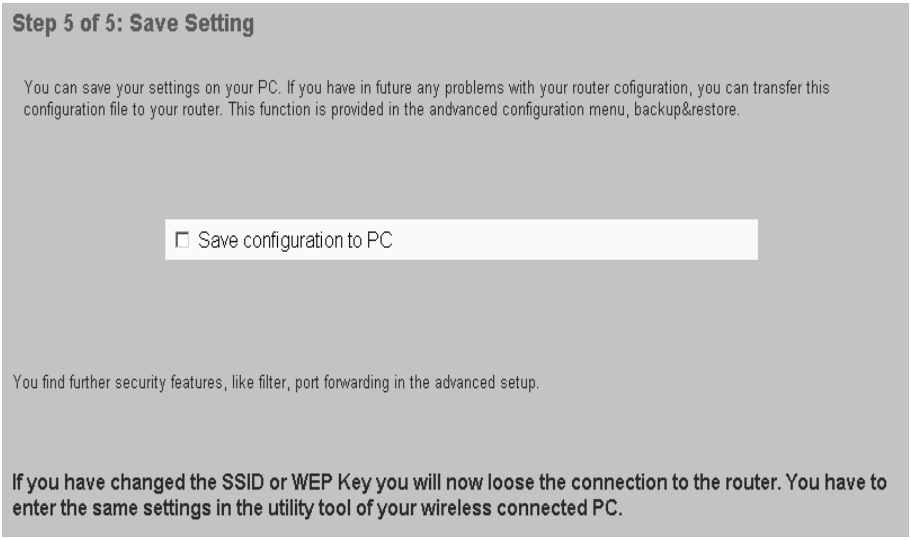
→ To apply the settings click ***NEXT***.

Please note:

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 cofiguration, you can transfer this configuration file to your router. This function is provided in the andvanced 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.

Please note:

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

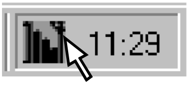
You then have to configure the set SSID and – if set up – the WEP or WPA key for the wireless network adapters on your PCs. Only then can you register with the router again.

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, Gigaset PCI Card 54 or Gigaset USB Adapter)

Carry out the following steps:

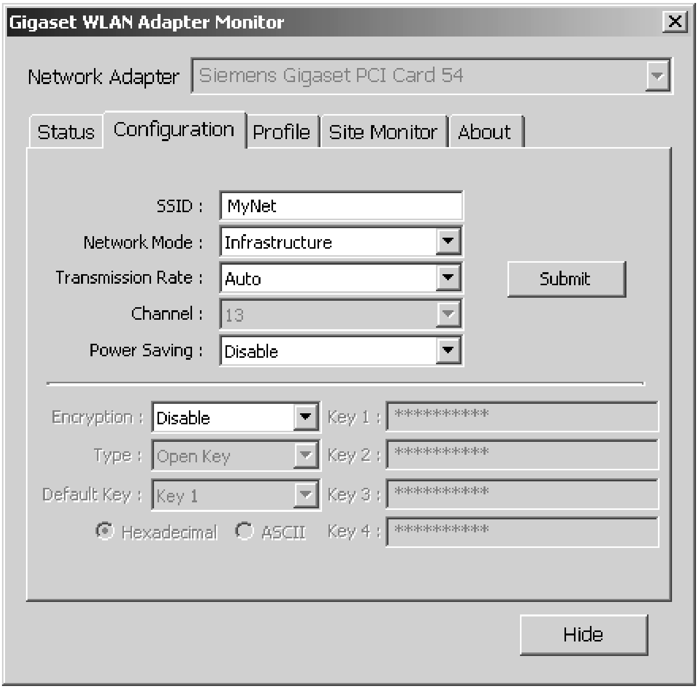
→ Start the Gigaset WLAN Adapter Monitor by double clicking on the icon in the taskbar.



The ***Gigaset WLAN Adapter Monitor*** is displayed.

→ Open the ***Configuration*** tab.

(The user interfaces may vary slightly according to the device used.)


Gigaset WLAN Adapter Monitor

Network Adapter: Siemens Gigaset PCI Card 54

SSID : MyNet

Network Mode : Infrastructure

Transmission Rate : Auto

Channel : 13

Power Saving : Disable

Encryption : Disable

Type : Open Key

Default Key : Key 1

● Hexadecimal ○ ASCII

Key 1 : ***********

Key 2 : ***********

Key 3 : ***********

Key 4 : ***********

→ 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.

If you have set WEP encryption on the router, read the next section. If you are using WPA-PSK as the encryption method on the router, you can find

- instructions for setting the encryption Gigaset USB Adapter on page 50,
- instructions for the configuration of Windows XP on page 52.

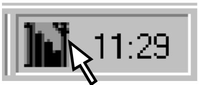
Setting WEP encryption on the network adapters

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, the Gigaset PCI Card 54 or a Gigaset USB Adapter using the ***Gigaset WLAN Adapter Monitor***.

To enter the WEP key:

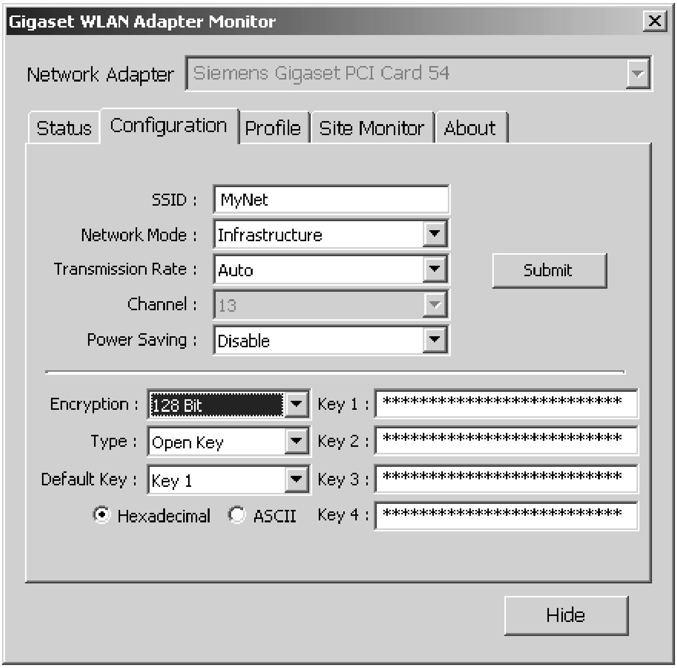
Start the Gigaset WLAN Adapter Monitor by double clicking the icon in the taskbar.



The ***Gigaset WLAN Adapter Monitor*** is displayed.

→ Open the ***Configuration*** tab.

(The user interfaces may vary slightly according to the device used.)



Network Adapter: Siemens Gigaset PCI Card 54

SSID : MyNet

Network Mode : Infrastructure

Transmission Rate : Auto

Channel : 13

Power Saving : Disable

Encryption : 128 Bit

Type : Open Key

Default Key : Key 1

● Hexadecimal ○ ASCII

Key 1 : **************************

Key 2 : **************************

Key 3 : **************************

Key 4 : **************************

➙ In the ***Encryption*** menu, select 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***.

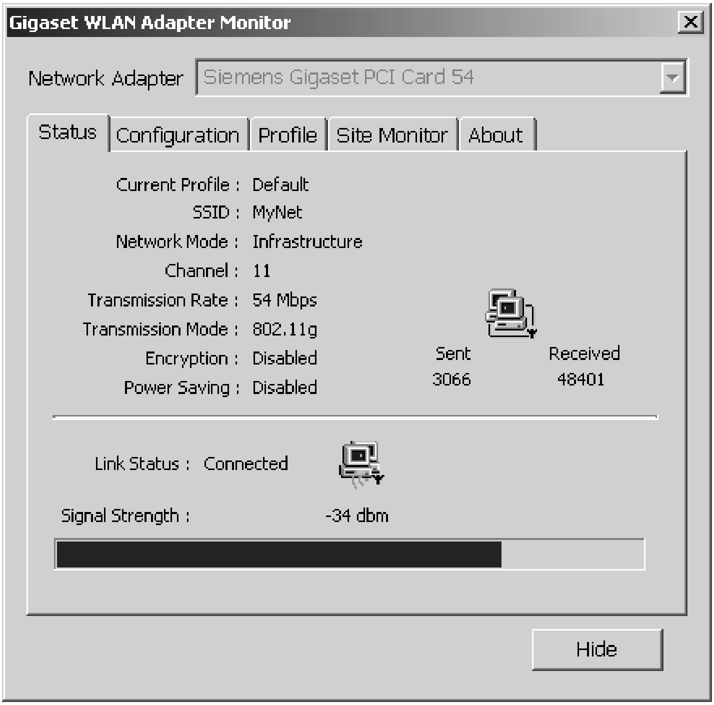
➙ Choose whether you want to assign a hexadecimal or ASCII key. The selection must be the same as on the router.

➙ Enter the key you noted when configuring the router in the field for the ***default key*** you selected.

➙ Click ***Submit***.

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

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



Network Adapter: Siemens Gigaset PCI Card 54

Current Profile : Default
SSID : MyNet
Network Mode : Infrastructure
Channel : 11
Transmission Rate : 54 Mbps
Transmission Mode : 802.11g
Encryption : Disabled
Power Saving : Disabled

Sent	Received
3066	48401

Link Status : Connected

Signal Strength : -34 dbm

➙ Click ***Hide*** to close the window.

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

Please note:

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. To do this, press the Reset button on the rear of the device for at least seven seconds. 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.

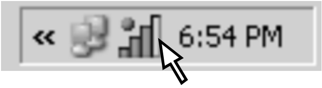
Setting WPA encryption on the Gigaset USB Adapter

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

You can configure the Gigaset USB Adapterusing the ***Gigaset WLAN Adapter Monitor***. For other network adapters, the user interface may differ slightly.

To enter the WPA key, proceed as follows:

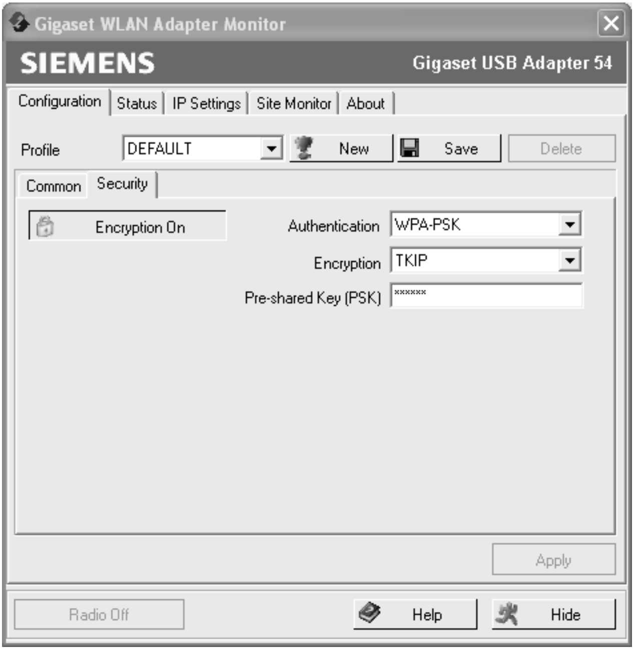
→ Start the Gigaset WLAN Adapter Monitor by double clicking on the icon in the taskbar.



The ***Gigaset WLAN Adapter Monitor*** is displayed.

→ Open the ***Configuration*** tab.
You can find the security settings under ***Security*** on the ***Configuration*** tab. On this tab, the security mode ***Encryption off*** is preset. To log into the encrypted wireless network, you must activate the security options on your Gigaset USB Adapter.

→ Click on the ***Encryption off*** button to activate the entry fields. The button changes to ***Encryption on***.



Profile DEFAULT

Authentication WPA-PSK

Encryption TKIP

Pre-shared Key (PSK) ******

You must now make further settings according to your network environment.

- → In the ***Authentication*** field, select the entry ***WPA-PSK***.
- → In the ***Encryption*** field, select ***TKIP*** as the encryption method.

  When selecting the encryption method, note that two communicating parties must be using the same type of encryption.
- → In the ***Pre-Shared Key (PSK)*** field, enter the key you entered on the router, e.g. xyz545556cba.

  Note that all components in a network must use the same ***Pre-Shared Key (PSK)*** in order to be able to communicate with one another.
- → Click on ***Apply*** to apply the changes.

The security options for your Gigaset USB Adapter are activated. The connection to the Gigaset SE505 dsl/cable is established.

Please note:

If the key you entered in 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, you have the following options:

◆ Reset the router. To do this, turn the router off and press the Reset button on the rear of the device for at least seven seconds. Please bear in mind that this will restore all configurations to the factory settings. Then disable encryption for the network adapters as well and start the whole process again from the beginning.

◆ Re-configure the WPA function for the router via a PC connected to the router by a cable.

Configuring WPA encryption under Windows XP

Before setting up WPA encryption for your PC, note the following points:

◆ If your network adapter does not support WPA, WPA can currently only be used if your PC runs on the Windows XP operating system. You will also need the Windows XP Service Pack 1 (SP1) and an additional patch from Microsoft for SP1. The number of this patch is 815485. It should be included in SP2.

  Information about encryption and the patch, as well as files for download, can be found on the Microsoft server: http://www.microsoft.de.

  Click on Support and then enter the patch number 815485 under Search Knowledge Base. You will then be presented with a document containing a link that you can use to download the software.

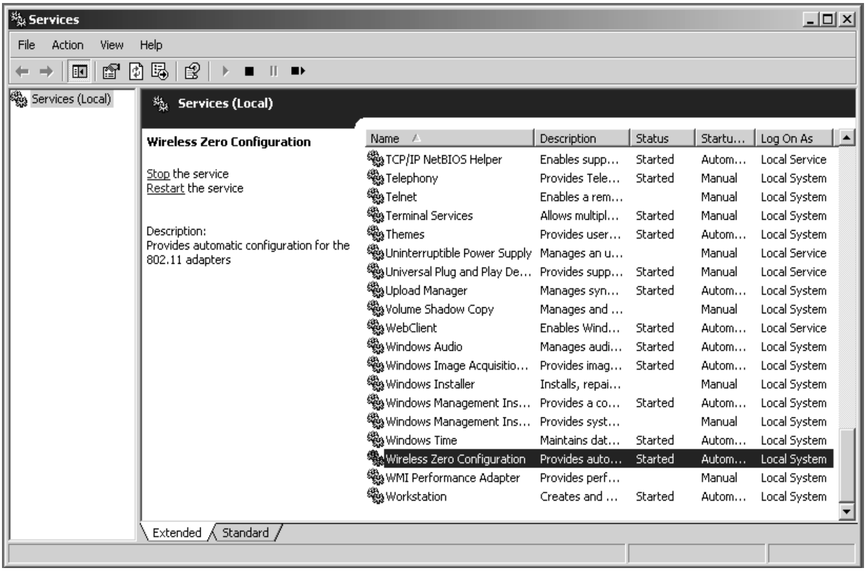
  Install this software on your PC.

◆ The drivers can encrypt and decrypt data packages in accordance with WPA. However, configuration is **not** carried out using the ***Gigaset WLAN Adapter Monitor*** but under Windows XP.

Proceed as follows to configure your PC in such a way that the corresponding Windows XP service is used instead of the ***Gigaset WLAN Adapter Monitor***.

➜ Disable the ***Gigaset WLAN Adapter Monitor*** (e.g. by removing it from Autostart or right clicking on its icon in the taskbar then on ***Exit***).

➜ Then click on ***Start*** – ***Control Panel*** – ***Administrative Tools*** – ***Services***.



Wireless Zero Configuration

Stop the service
Restart the service

Description:
Provides automatic configuration for the 802.11 adapters

Name	Description	Status	Startu...	Log On As
TCP/IP NetBIOS Helper	Enables supp...	Started	Autom...	Local Service
Telephony	Provides Tele...	Started	Manual	Local System
Telnet	Enables a rem...		Manual	Local System
Terminal Services	Allows multipl...	Started	Manual	Local System
Themes	Provides user...	Started	Autom...	Local System
Uninterruptible Power Supply	Manages an u...		Manual	Local Service
Universal Plug and Play De...	Provides supp...	Started	Manual	Local Service
Upload Manager	Manages syn...	Started	Autom...	Local System
Volume Shadow Copy	Manages and ...		Manual	Local System
WebClient	Enables Wind...	Started	Autom...	Local Service
Windows Audio	Manages audi...	Started	Autom...	Local System
Windows Image Acquisitio...	Provides imag...	Started	Autom...	Local System
Windows Installer	Installs, repai...		Manual	Local System
Windows Management Ins...	Provides a co...	Started	Autom...	Local System
Windows Management Ins...	Provides syst...		Manual	Local System
Windows Time	Maintains dat...	Started	Autom...	Local System
Wireless Zero Configuration	Provides auto...	Started	Autom...	Local System
WMI Performance Adapter	Provides perf...		Manual	Local System
Workstation	Creates and ...	Started	Autom...	Local System

➙ Check whether

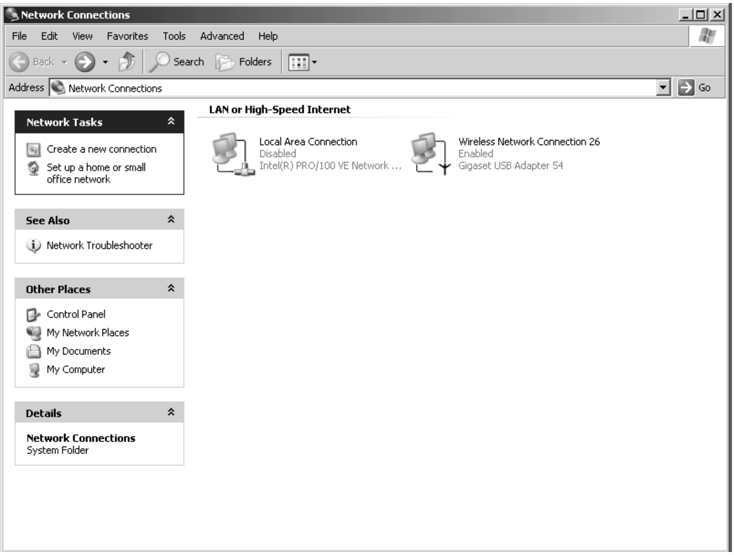
– the service ***Wireless Zero Configuration*** is marked as Started

– the selected startup type is ***Automatic***.

If not, make the appropriate settings.

You now need to set the correct WPA parameters.

➙ To do this, click on ***Start*** – ***Control Panel*** – ***Network Connections***.



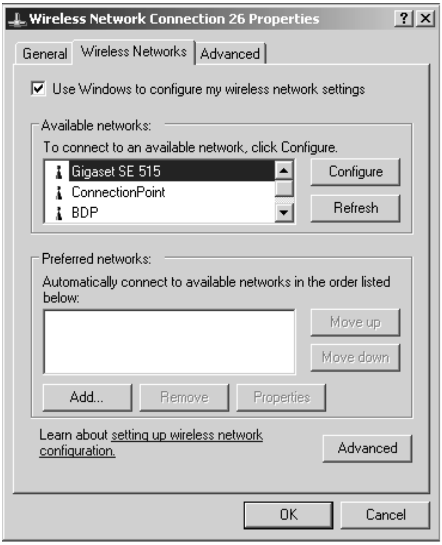
Network Connections
System Folder

LAN or High-Speed Internet

Local Area Connection
Disabled
Intel(R) PRO/100 VE Network ...

Wireless Network Connection 26
Enabled
Gigaset USB Adapter 54

→ Right click on ***Wireless Network Connection***, then on ***Show available wireless networks*** and, in the subsequent window, click on ***Advanced***. The ***Wireless Networks*** tab appears.



☑ Use Windows to configure my wireless network settings

Available networks:
To connect to an available network, click Configure.

Gigaset SE 515
ConnectionPoint
BDP

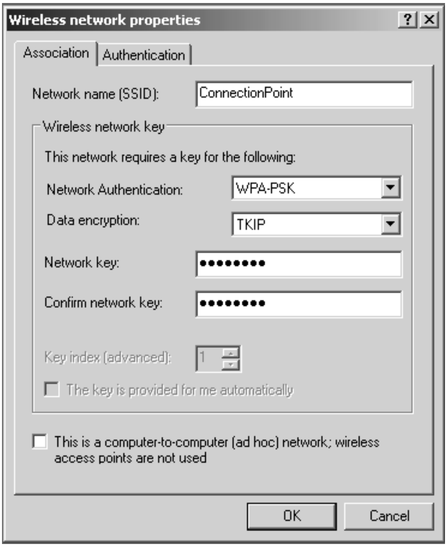
Preferred networks:
Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

→ Select the ***Use Windows to configure my wireless network settings*** check box.

→ Select the network you want to connect to – it can be identified by the SSID.

→ Then click on ***Configure***. The window for entering the configuration parameters appears.



Wireless network properties

Association | Authentication

Network name (SSID): ConnectionPoint

Wireless network key

This network requires a key for the following:

Network Authentication: WPA-PSK

Data encryption: TKIP

Network key: ••••••••

Confirm network key: ••••••••

Key index (advanced): 1

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

When configuring WPA on your PC, make sure that you enter values that match those of the communication partner (Gigaset SE505 dsl/cable).

The SSID is already defined.

→ Select ***WPA-PSK*** (WPA-Pre-Shared Key) as the value for network authentication and the value ***TKIP*** for data encryption.

The network key on your PC must match the ***Pre-shared key*** for the communication partner.

→ Close the open window by clicking on ***OK***

WPA encryption is now configured. The network connection is established.

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:

→ Start your Internet browser.

→ Enter the router IP address in the address bar of your Internet browser. If you have not configured the router with a different IP address, this will be

`http://192.168.2.1`

You will then see an Internet site containing a login dialog.

→ If a password has already been assigned, enter it and click ***LOGIN***.

→ After logging in, select ***Advanced Setup***.

→ Open the ***Virtual server*** menu.

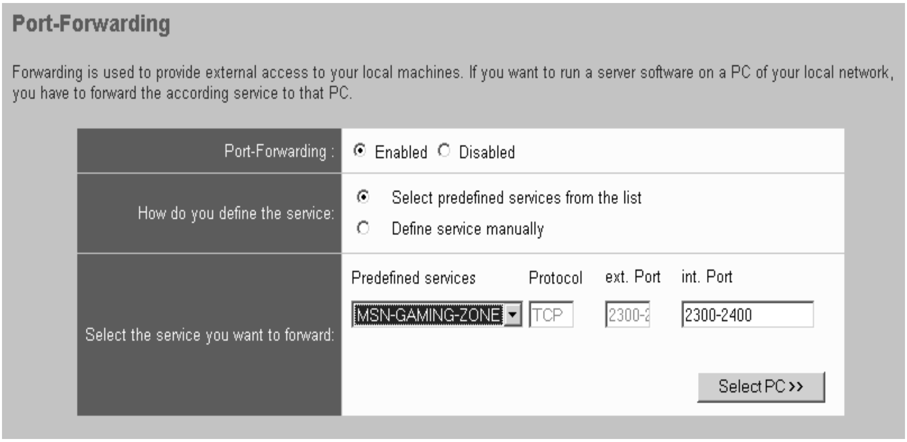
→ Select ***Virtual server*** – ***Port Forwarding***.

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

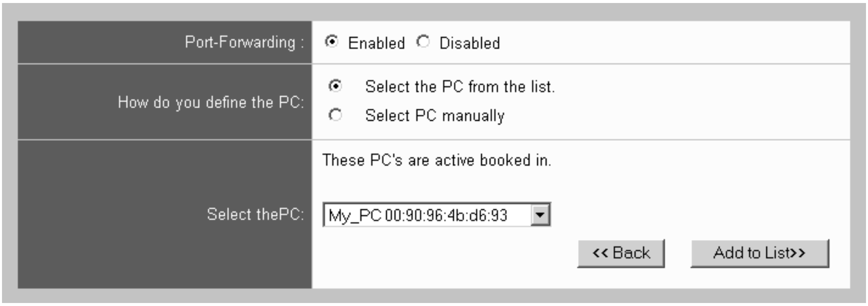
Select the service you want to forward:

Predefined services	Protocol	ext. Port	int. Port
MSN-GAMING-ZONE	TCP	2300-2	2300-2400

→ 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

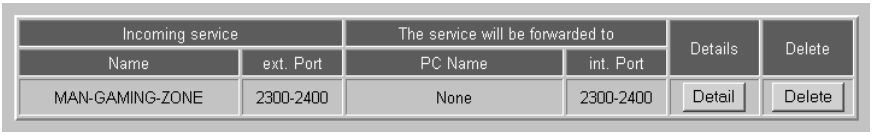
Select thePC: These PC's are active booked in. My_PC 00:90:96:4b:d6:93

→ 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 game and the PC will be displayed in the list.



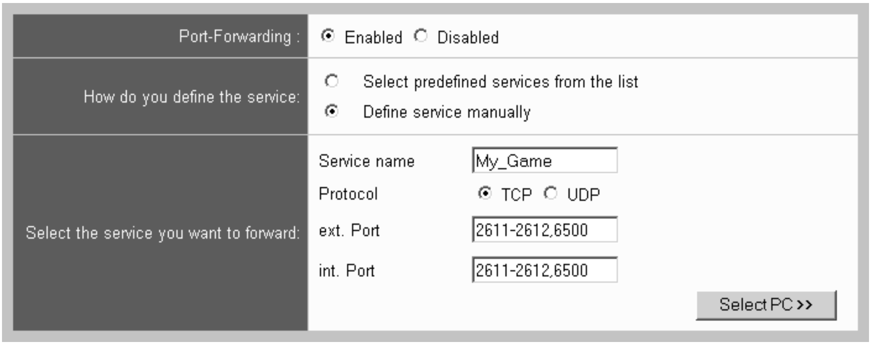
Incoming service		The service will be forwarded to		Details	Delete
Name	ext. Port	PC Name	int. Port		
MAN-GAMING-ZONE	2300-2400	None	2300-2400	Detail	Delete

Setting up Port Forwarding for non predefined games

Please note:

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***.



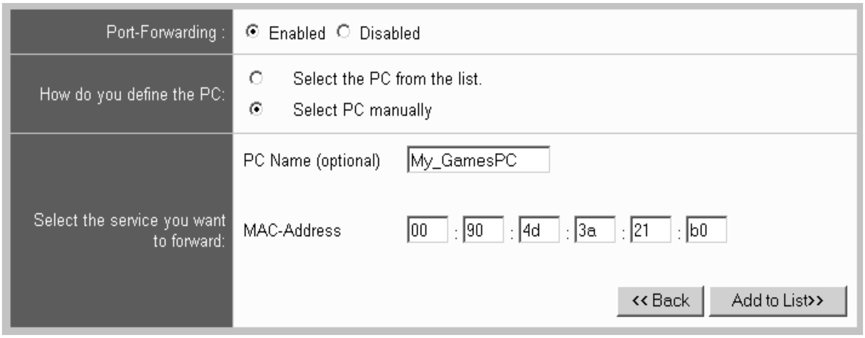
Port-Forwarding :	● Enabled ○ Disabled
How do you define the service:	○ Select predefined services from the list ● Define service manually
Select the service you want to forward:	Service name: My_Game Protocol: ● TCP ○ UDP ext. Port: 2611-2612,6500 int. Port: 2611-2612,6500 Select PC >>

→ 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

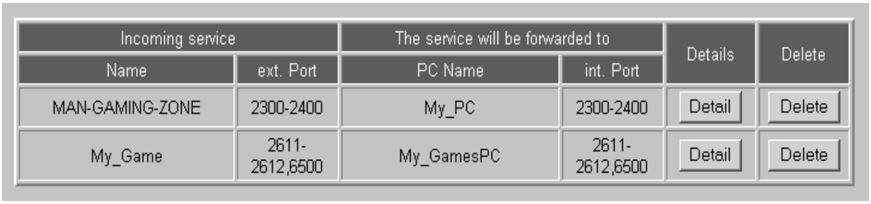
→ Select ***Select PC manually***.

→ Enter the PC's name and MAC address.

> **Please note:**
> 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:

➞ Start your Internet browser.

➞ Enter the router IP address in the address bar of your Internet browser. If you have not configured the router with a different IP address, this will be

`http://192.168.2.1`

You will then see an Internet site containing a login dialog.

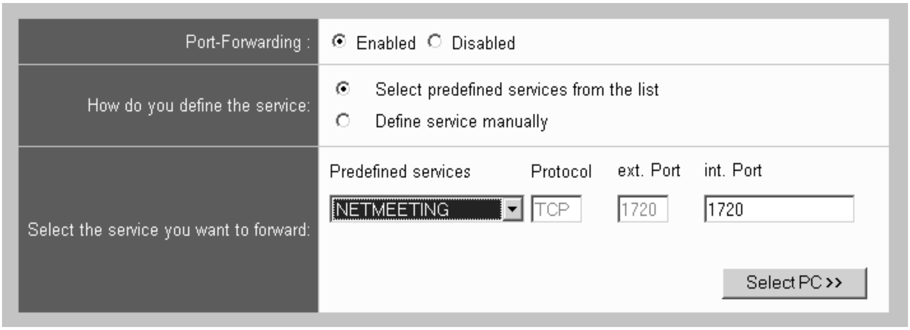
➞ If a password has already been assigned, enter it and click ***LOGIN***.

➞ After logging in, select ***Advanced Setup***.

➞ Open the ***Virtual servermenu***.

➞ Select ***Virtual server*** – ***Port Forwarding***.

Setting up Port Forwarding for MS Netmeeting



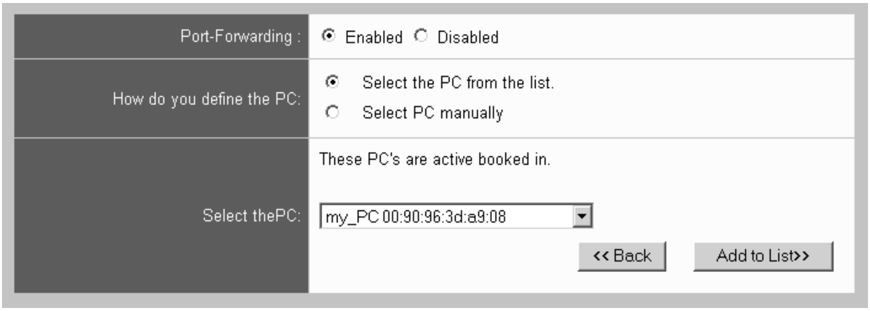
Port-Forwarding : ● Enabled ○ Disabled

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	int. Port
NETMEETING	TCP	1720	1720

- → 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 thePC: These PC's are active booked in.

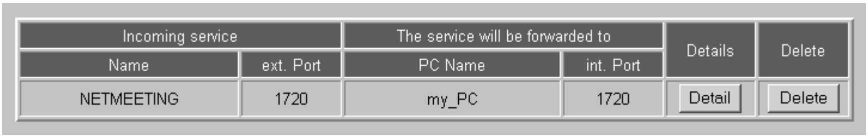
my_PC 00:90:96:3d:a9:08

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

> **Please note:**
> The PC only appears in the list of registered PC if it is registered on the router. If it is not registered, select ***Select PC manually*** and enter the PC's name and MAC address (see page 59).

- → Click ***Add to list***.

➙ 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 64).
- 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 67).

Starting configuration

To start configuration:

→ Start your Internet browser.

→ Enter the router IP address in the address bar of your Internet browser. If you have not configured the router with a different IP address, this will be

```
http://192.168.2.1
```

You will then see an Internet site containing a login dialog.

→ 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

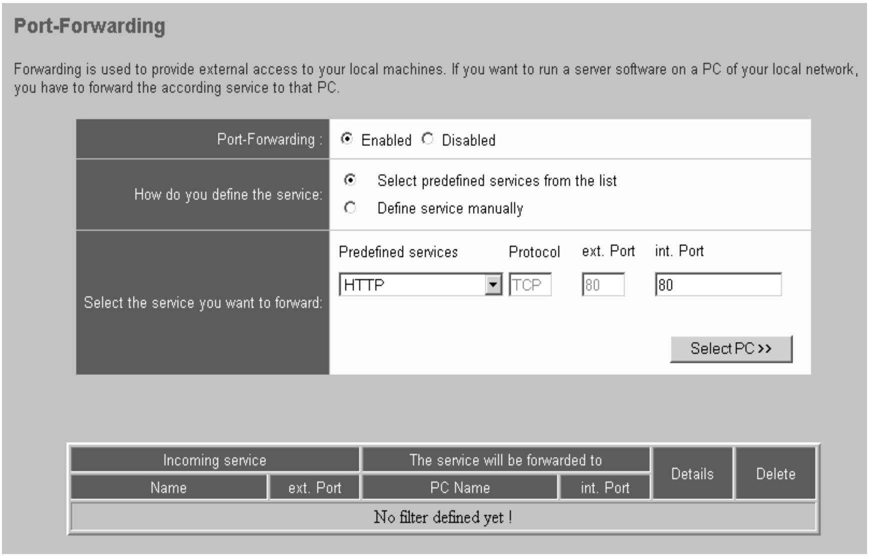
Port Forwarding (directing requests to particular ports) is needed if you want to run server services for the Internet on a PC on your local network. For example, you could use one of your PCs to operate a Web server that provides HTML pages. The router, which in this case functions as a virtual server, 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 :	● 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: HTTP; Protocol: TCP; ext. Port: 80; int. Port: 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***.

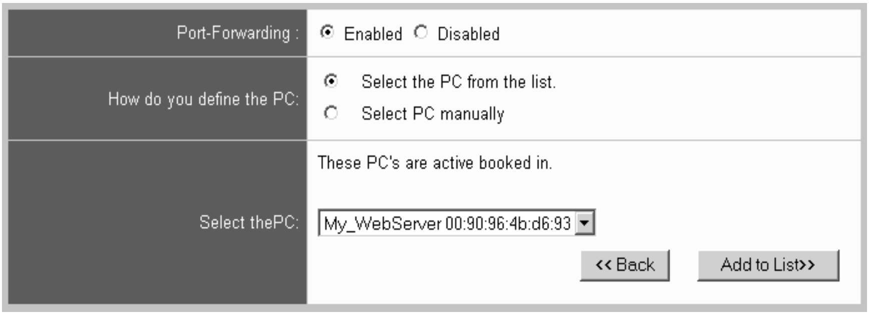
→ Select the predefined service ***HTTP*** from the selection list. The protocol and external port are entered automatically.

→ 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

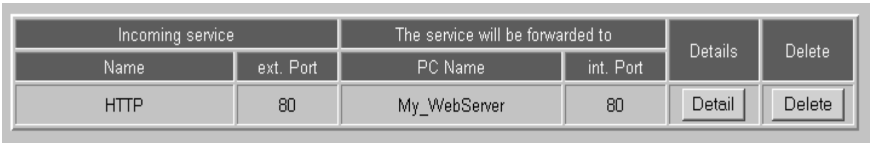
Select thePC: These PC's are active booked in. My_WebServer 00:90:96:4b:d6:93

→ Select ***Select the PC from the list***.

→ Select the PC from the list of registered PCs.

→ Click ***Add to list***.

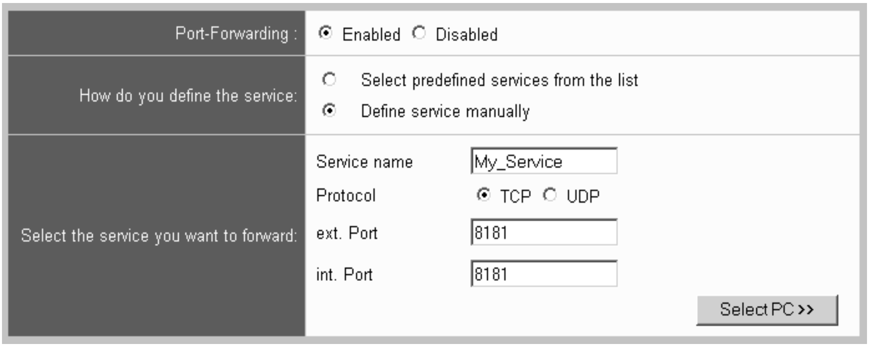
→ Click ***APPLY***. A new entry for the service and the PC will be displayed in the list.



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

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

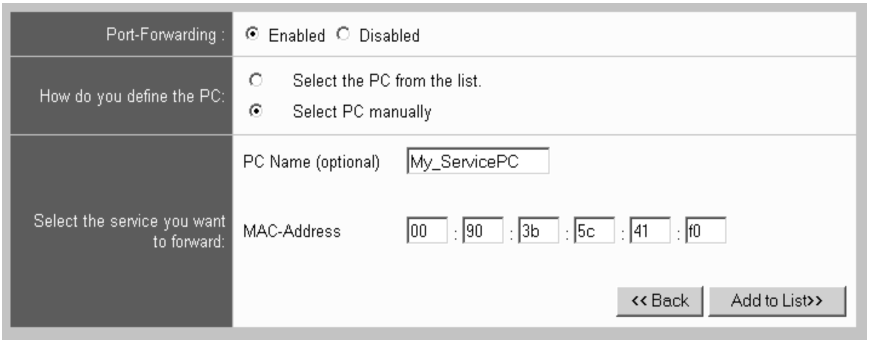
ext. Port: 8181

int. Port: 8181

→ 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.

> **Please note:**
>
> 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

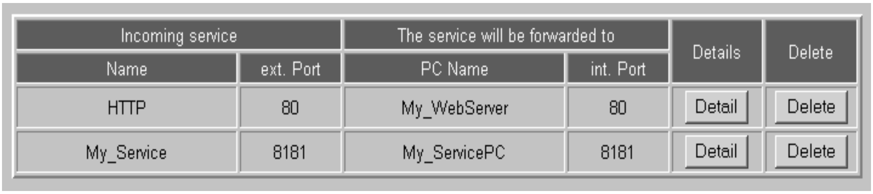
→ Select ***Select PC manually***.

→ Enter the PC's name and MAC address.

> **Please note:**
>
> 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.

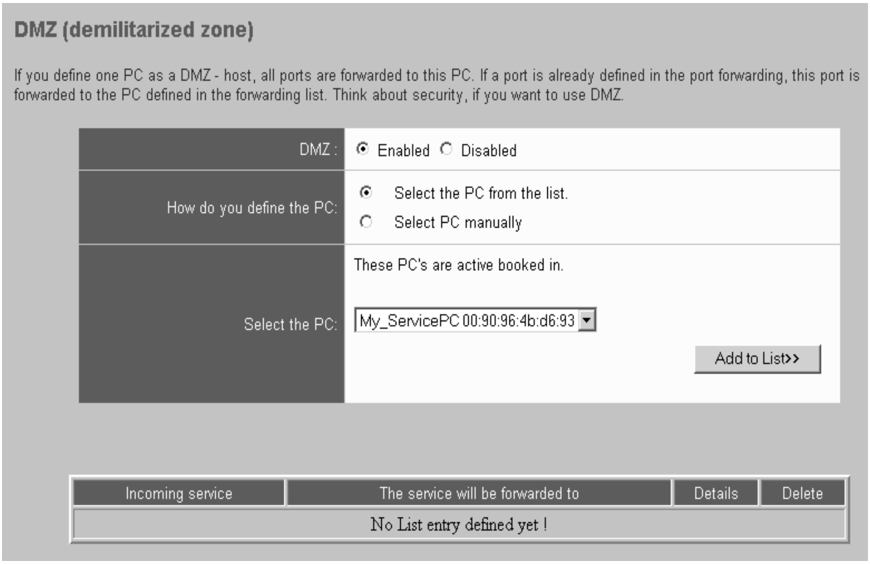
If you define a DMZ, all the requests from the Internet for a service will be redirected to that PC if the service in question has not already been redirected to another PC via Port Forwarding (see page 64).

Please note:

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***

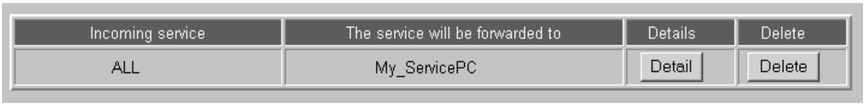
→ ***Select PC manually***

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

Please note:

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.

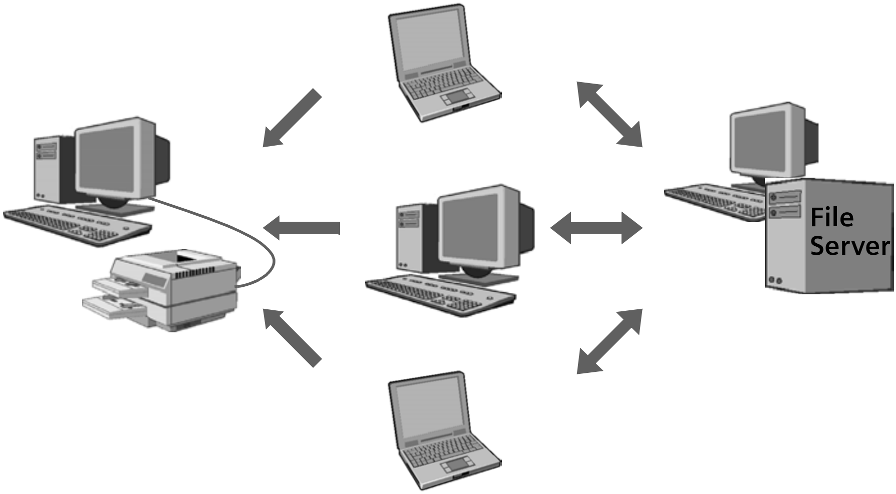


Incoming service	The service will be forwarded to	Details	Delete
ALL	My_ServicePC	Detail	Delete

→ 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.

Please note:

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

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

	Windows 98	Windows XP	Windows 2000
Set up a network	page 70	page 89	page 106
Release your own files	page 79	page 95	page 115
Release your own printers	page 80	page 97	page 119
Set up user IDs	page 81	page 98	page 112
Use files on other PCs	page 83	page 101	page 120
Use printers on other PCs	page 86	page 104	page 124

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:

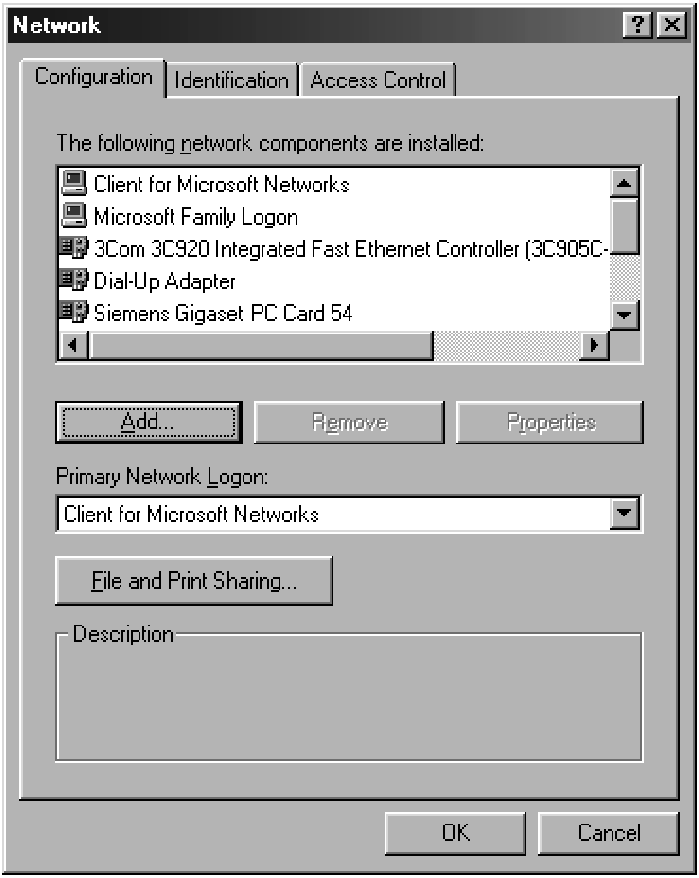
1. Set up PC as Client for Microsoft Networks (see page 70).
2. Select computer names and workgroup (see page 73).
3. Select type of access control (see page 73).
4. Set TCP/IP protocol (see page 74).
5. Install utilities for file and printer release (see page 77).
6. Release files and printer (see page 79).

Setting up a PC as Client for Microsoft Networks

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

→ Open the ***Control Panel*** and then open ***Network***.

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



Network

Configuration | Identification | Access Control

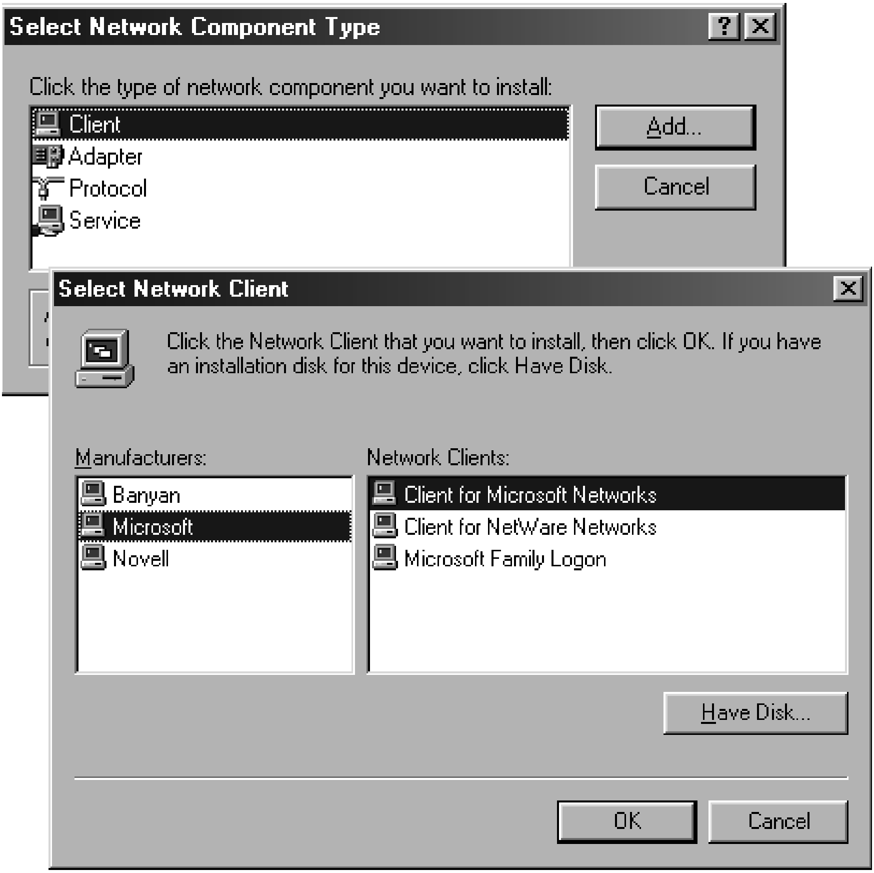
The following network components are installed:

- Client for Microsoft Networks
- Microsoft Family Logon
- 3Com 3C920 Integrated Fast Ethernet Controller (3C905C-
- Dial-Up Adapter
- Siemens Gigaset PC Card 54

Primary Network Logon: Client for Microsoft Networks

If the entry exists, please continue from page 73.

→ If the entry does not exist, click ***Add***


Select Network Component Type

Click the type of network component you want to install:

- Client
- Adapter
- Protocol
- Service

Select Network Client

Click the Network Client that you want to install, then click OK. If you have an installation disk for this device, click Have Disk.

Manufacturers:

- Banyan
- Microsoft
- Novell

Network Clients:

- Client for Microsoft Networks
- Client for NetWare Networks
- Microsoft Family Logon

→ 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

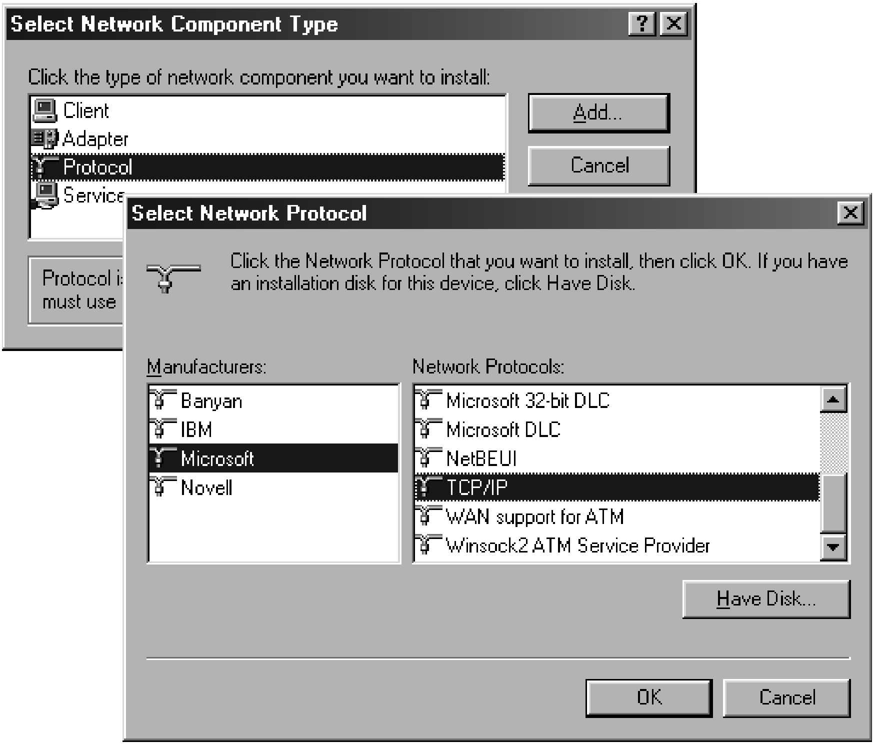
The TCP/IP protocol ensures that the PCs on the network can communicate with each other. This protocol requires certain settings which you will now make so that it can function smoothly.

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 74.

→ If the entry does not exist, click ***Add***.



Select Network Component Type

Click the type of network component you want to install:

Protocol

Select Network Protocol

Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this device, click Have Disk.

Manufacturers: Microsoft

Network Protocols: TCP/IP

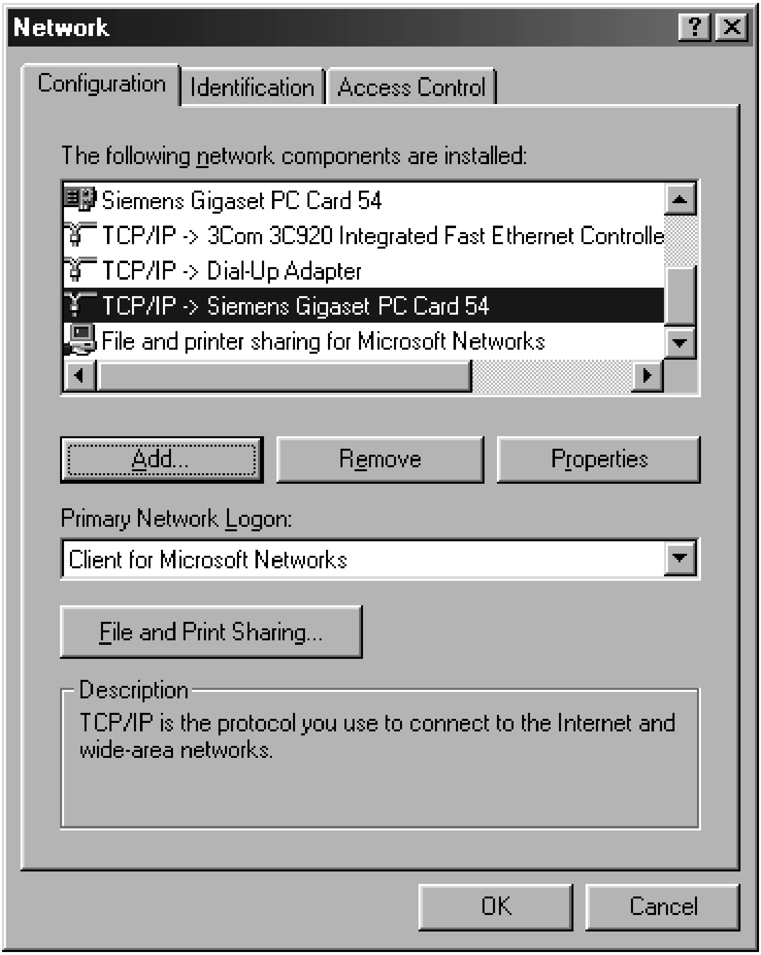
→ Select as network component type ***Protocol*** and click ***Add***.

→ Select in ***Manufacturers*** the entry ***Microsoft*** and in ***Network protocol*** the entry ***TCP/IP*** before confirming with ***OK***.

→ Set TCP/IP protocol.

→ To do this, in the ***Network*** window, switch to the ***Configuration*** tab.

→ Select the ***TCP/IP >*** entry for your network card and click ***Properties***.



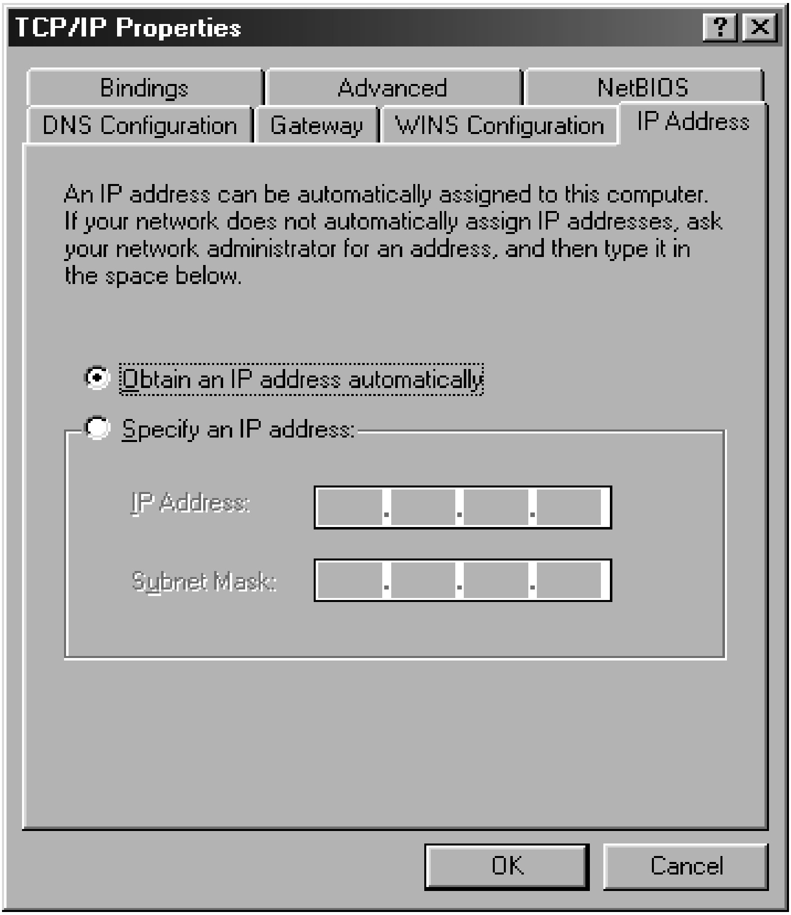
The following network components are installed:

Siemens Gigaset PC Card 54
TCP/IP -> 3Com 3C920 Integrated Fast Ethernet Controlle
TCP/IP -> Dial-Up Adapter
TCP/IP -> Siemens Gigaset PC Card 54
File and printer sharing for Microsoft Networks

Primary Network Logon:
Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

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



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

Please note:

You can of course define IP addresses manually. This is necessary for example in ad-hoc networks. How to assign static IP addresses is described in the Appendix from page 126.

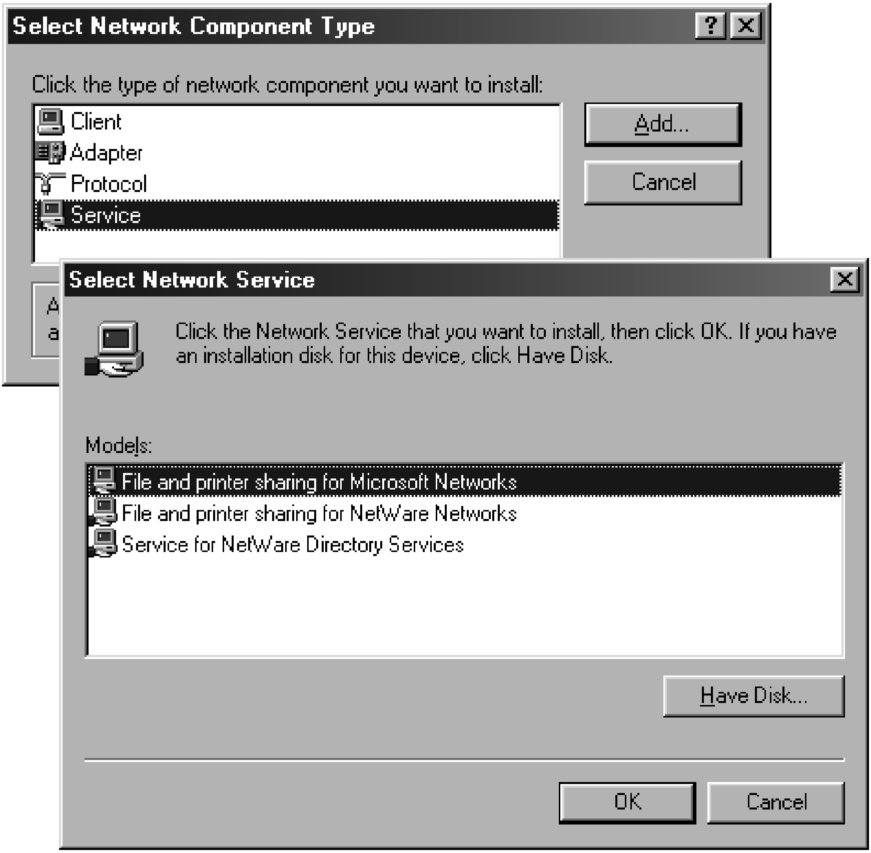
Installing utilities for file and printer release

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 78.

→ If the entry does not exist, click ***Add***.


Select Network Component Type

Click the type of network component you want to install:

Select Network Service

Click the Network Service that you want to install, then click OK. If you have an installation disk for this device, click Have Disk.

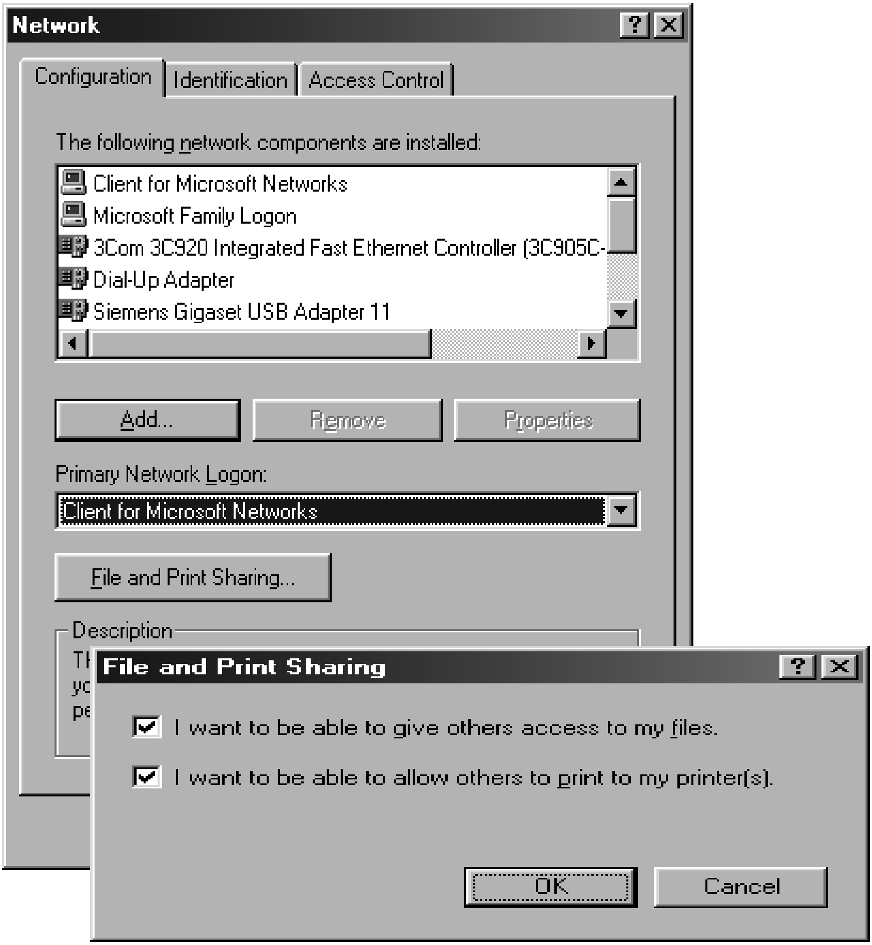
Models:

Client
Adapter
Protocol
Service
Add...
Cancel
File and printer sharing for Microsoft Networks
File and printer sharing for NetWare Networks
Service for NetWare Directory Services
Have Disk...
OK
Cancel

→ 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***.



The following network components are installed:

- Client for Microsoft Networks
- Microsoft Family Logon
- 3Com 3C920 Integrated Fast Ethernet Controller (3C905C-
- Dial-Up Adapter
- Siemens Gigaset USB Adapter 11

Primary Network Logon: Client for Microsoft Networks

☑ I want to be able to give others access to my files.

☑ I want to be able to allow others to print to my printer(s).

→ 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

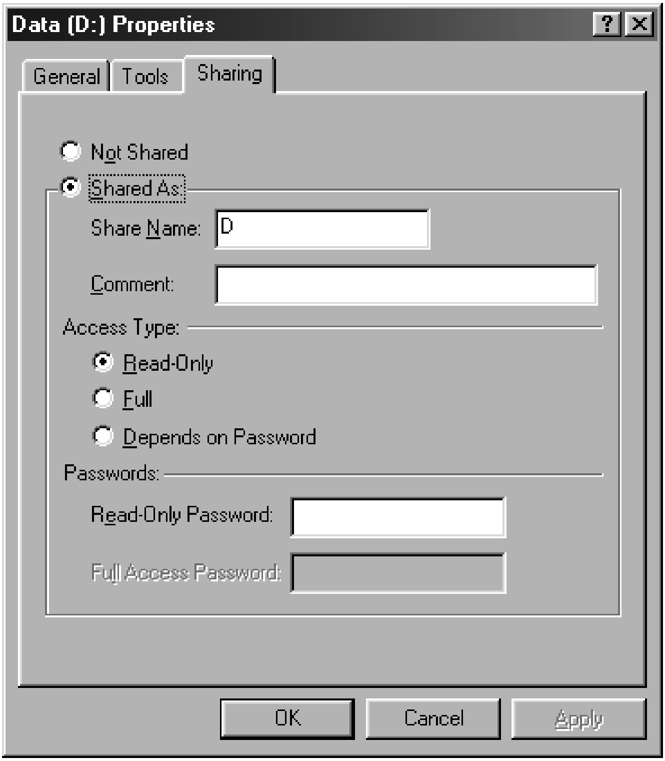
You can now release drives, folders or printers on your PC for other users on the network.

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.



○ Not Shared

● Shared As:

Share Name: D

Comment:

Access Type:

● Read-Only

○ Full

○ Depends on Password

Passwords:

Read-Only Password:

Full Access Password:

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

➔ Select one of the following access types:

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

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

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

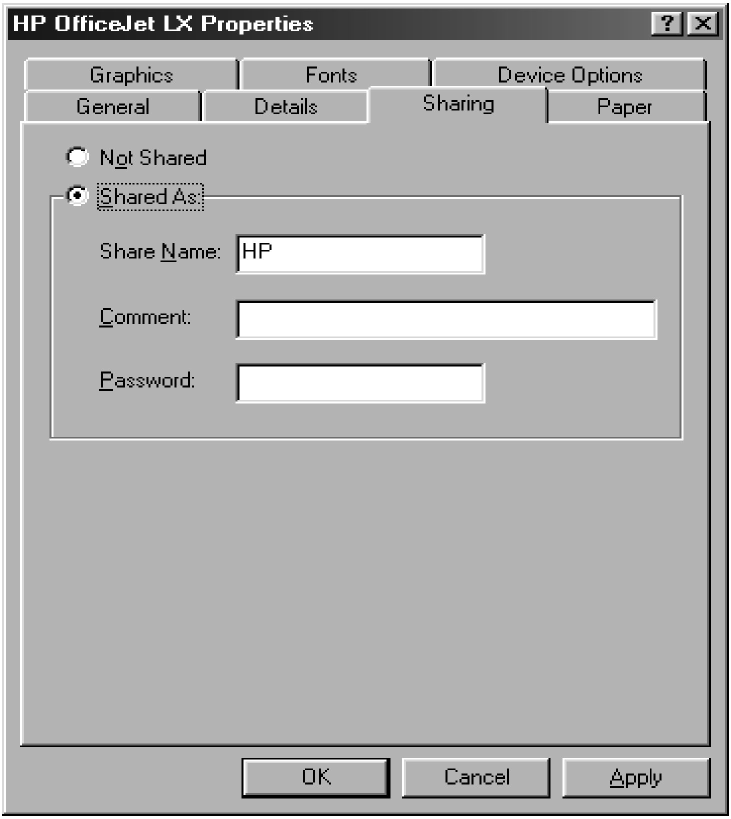
➔ Click ***Apply*** to save your settings and finish with ***OK***.

Releasing printers

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

➔ Left-click the printer you want to release.

➔ Now select ***Share*** with the right-hand mouse button from the pop-up menu. The following window will appear.



○ Not Shared

● Shared As:

Share Name: HP

Comment:

Password:

➔ 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.

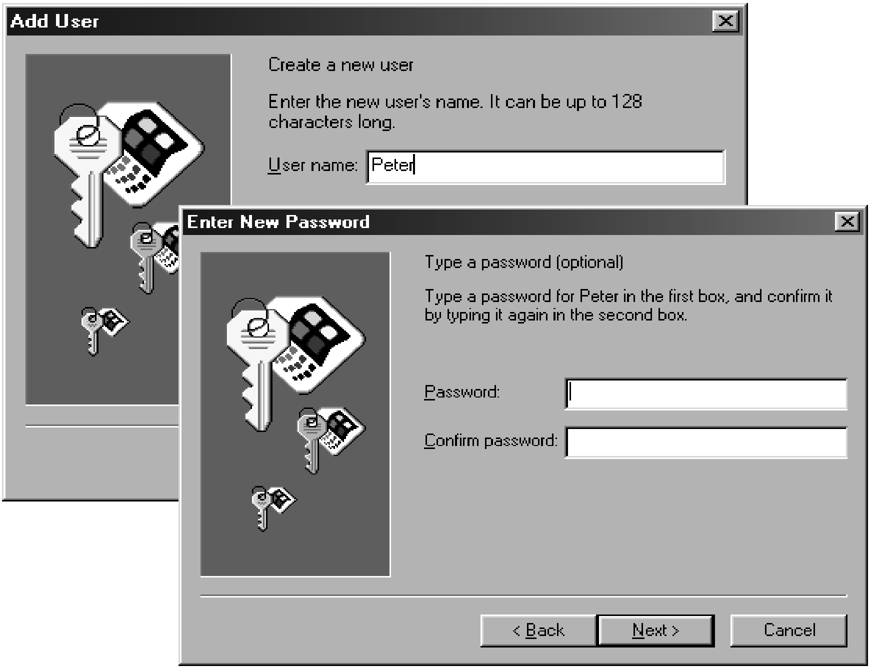
Please note:

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

Setting up user names

To set up a user ID:

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



Add User

Create a new user

Enter the new user's name. It can be up to 128 characters long.

User name: Peter

Enter New Password

Type a password (optional)

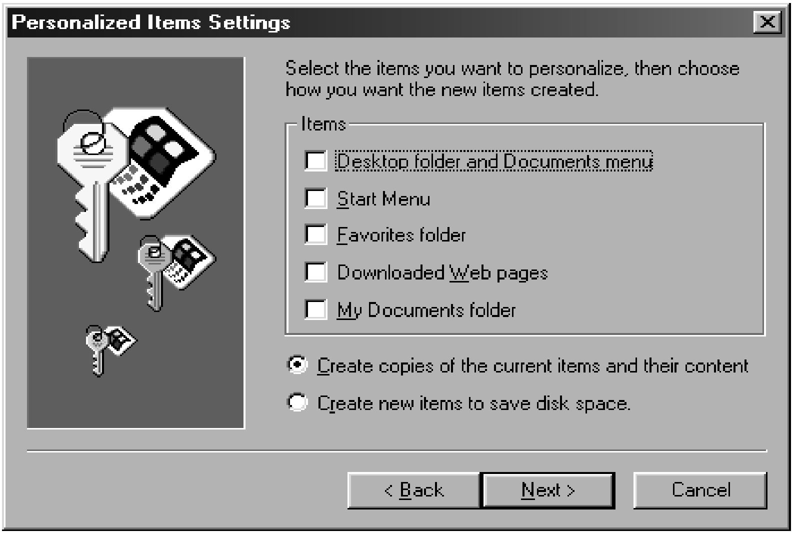
Type a password for Peter in the first box, and confirm it by typing it again in the second box.

Password:

Confirm password:

- → Enter a user name and click ***Next***.
- → Enter a password, repeat it and click ***Next***.

→ Define the settings for the user's interface. If you want to apply the current settings for the user, click ***Next***.



Personalized Items Settings

Select the items you want to personalize, then choose how you want the new items created.

Items

□ Desktop folder and Documents menu

□ Start Menu

□ Favorites folder

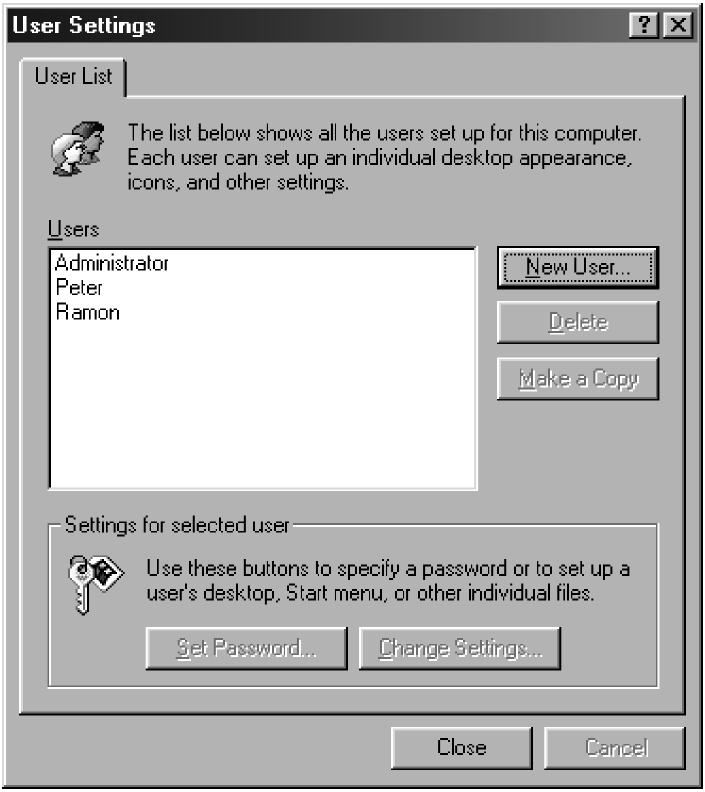
□ Downloaded Web pages

□ My Documents folder

● Create copies of the current items and their content

○ Create new items to save disk space.

The user has now been registered.



The list below shows all the users set up for this computer. Each user can set up an individual desktop appearance, icons, and other settings.

Users

Administrator
Peter
Ramon

Settings for selected user

Use these buttons to specify a password or to set up a user's desktop, Start menu, or other individual files.

→ 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 84).
  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 85).
  You should choose this alternative if you want to work directly with the files or folders of the other PC. In this case, hook on an entire released drive or folder in your PC's file system and work with the files as if they were files on your PC.

Please note:

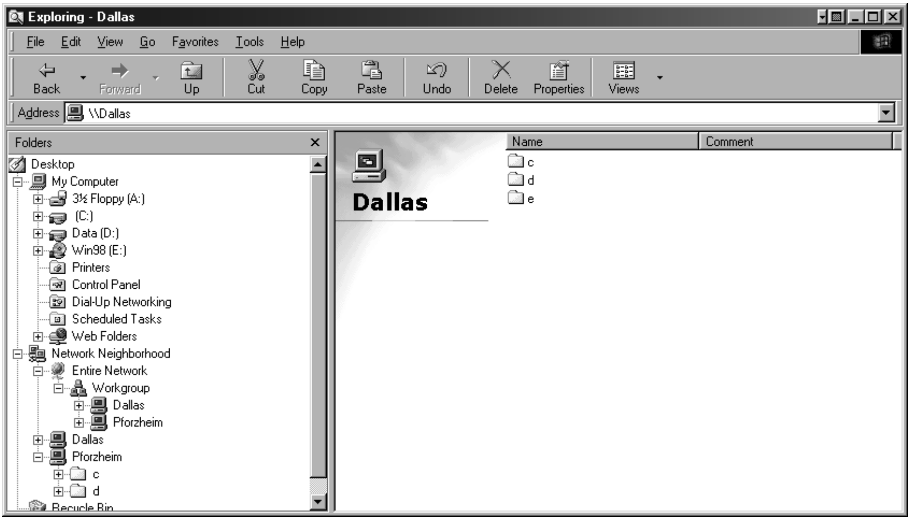
Drives or folders can be simultaneously hooked onto several PCs. It is therefore possible for other users to access the data. Most applications (e. g. word processing software) lock files once they have been opened. This prevents inconsistent data pools. If you cannot open a file because it is locked,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

Accessing external files via the My NetworkPlaces

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

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

Workgroups are marked with the 🖧 symbol:



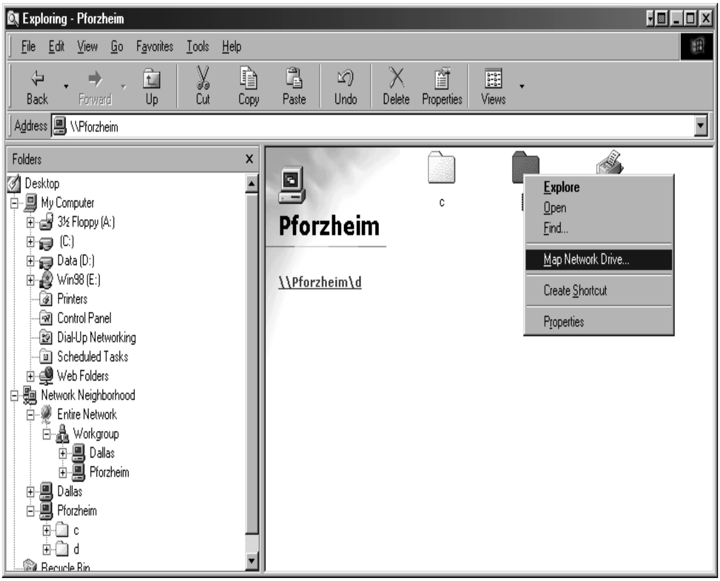
Clicking a PC name shows the released drives and folders on this PC under the name assigned when they were released. You can navigate through the file system in the usual Windows Explorer way by clicking a drive or folder and then opening other branches of the file tree.

Hooking external files on to your own file system

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

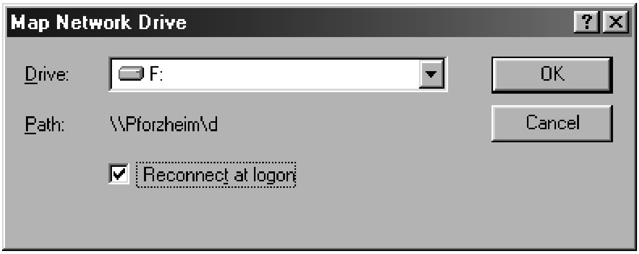
→ Open the ***My NetworkPlaces.***

→ 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***.



Drive: F:

Path: \\Pforzheim\d

☑ Reconnect at logon

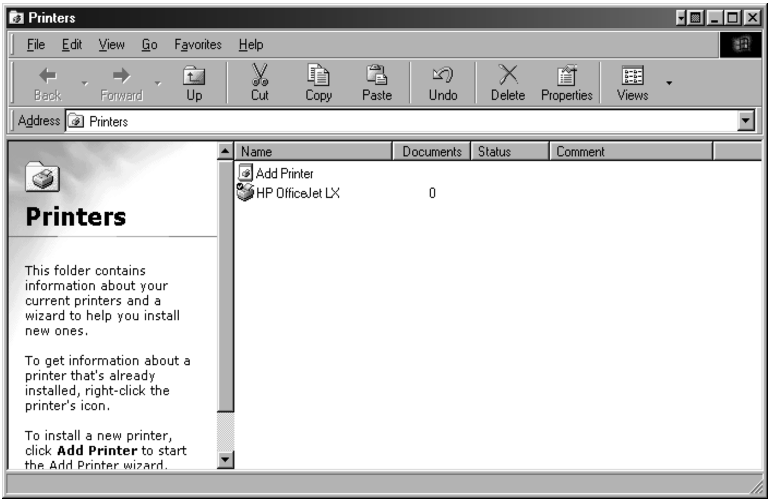
→ Select the drive name under which the remote drive is to be hooked on to your PC. The next free drive will be prompted. If you select the option ***Reconnect at logon***, Windows will hook the drive on every time you start your PC, provided the remote PC is running.

→ Now open the desktop. The remote drive is now available as the network drive. You can access the files as if they were on your own PC.

Accessing released printers from your PC

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

→ Open the printer manager with ***Start*** – ***Settings*** – ***Printers***



Printers

This folder contains information about your current printers and a wizard to help you install new ones.

To get information about a printer that's already installed, right-click the printer's icon.

To install a new printer, click **Add Printer** to start the Add Printer wizard.

Name	Documents	Status	Comment
Add Printer			
HP OfficeJet LX	0		

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

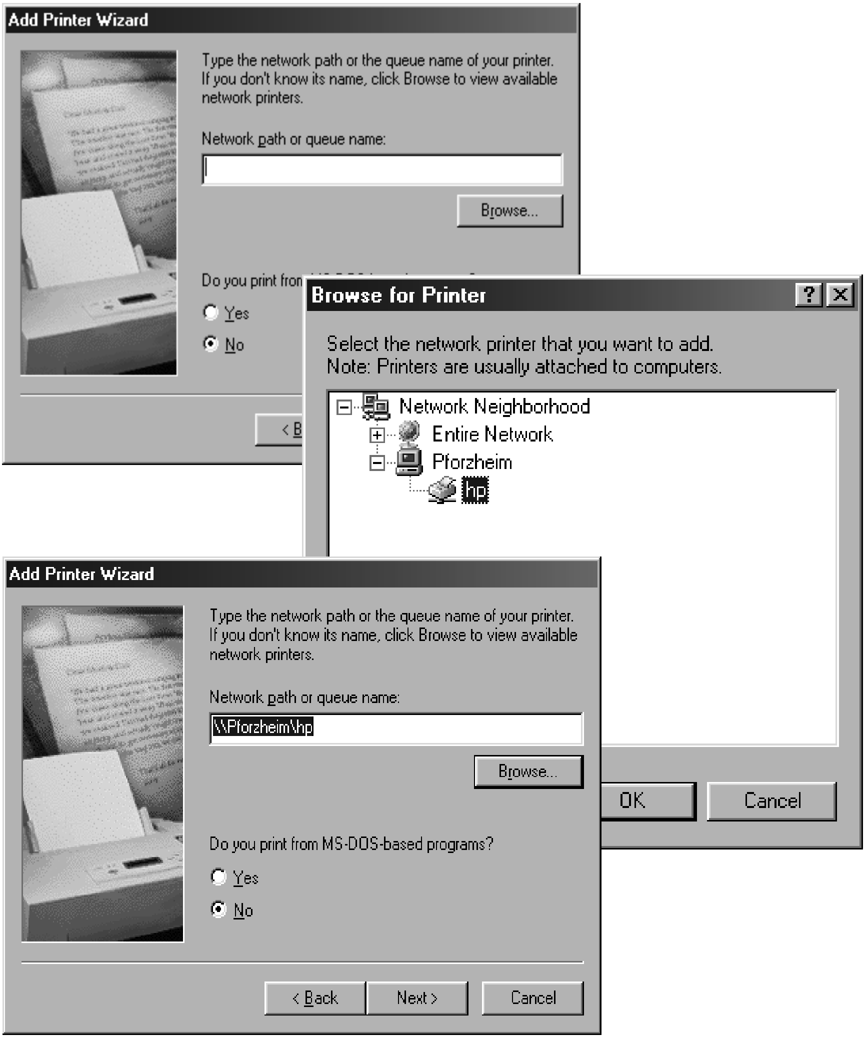
→ Click ***Next***.

→ 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***.



Type the network path or the queue name of your printer. If you don't know its name, click Browse to view available network printers.

Network path or queue name:

Select the network printer that you want to add.
Note: Printers are usually attached to computers.

Type the network path or the queue name of your printer. If you don't know its name, click Browse to view available network printers.

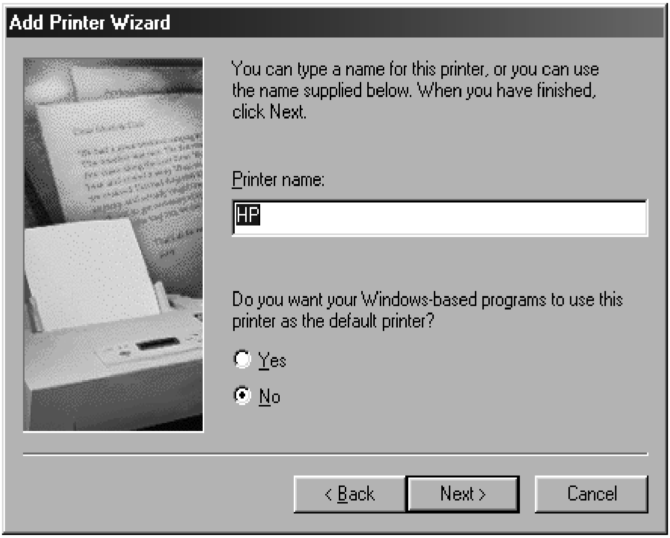
Network path or queue name: \\Pforzheim\hp

Do you print from MS-DOS-based programs?

○ Yes
● No

➞ The printer will now be displayed. Click ***Next***.

→ Now enter a name for the printer on your PC.



You can type a name for this printer, or you can use the name supplied below. When you have finished, click Next.

Printer name: HP

Do you want your Windows-based programs to use this printer as the default printer?

○ Yes

● No

→ Click ***Next***.

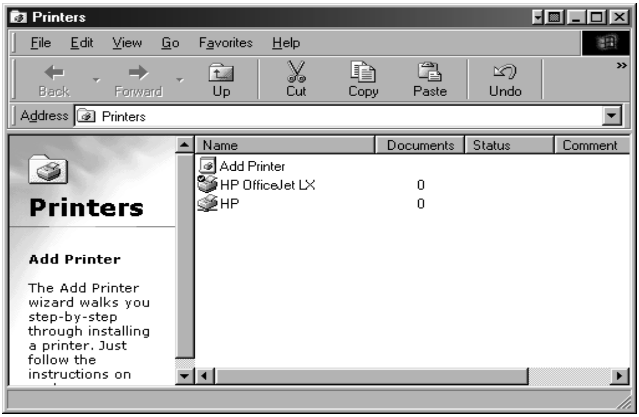
→ You can now print a test page if you want. This will show you whether the printer is functioning properly on the network.

→ 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.



Name	Documents	Status	Comment
Add Printer			
HP OfficeJet LX	0		
HP	0		

Add Printer

The Add Printer wizard walks you step-by-step through installing a printer. Just follow the instructions on

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 92).
3. Accept network settings (see page 93).
4. Close installation procedures (see page 94).
5. Release files and printer (see page 95).

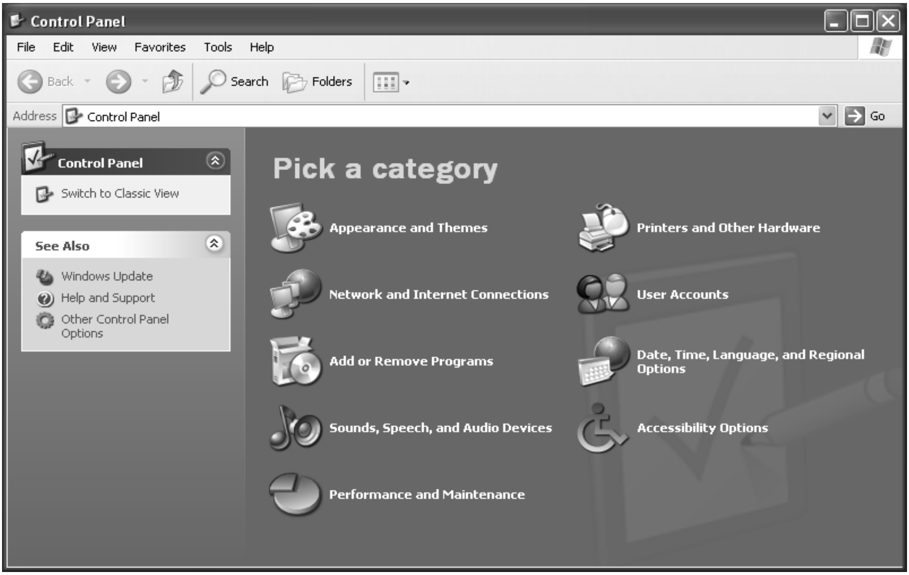
Configuring the network

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

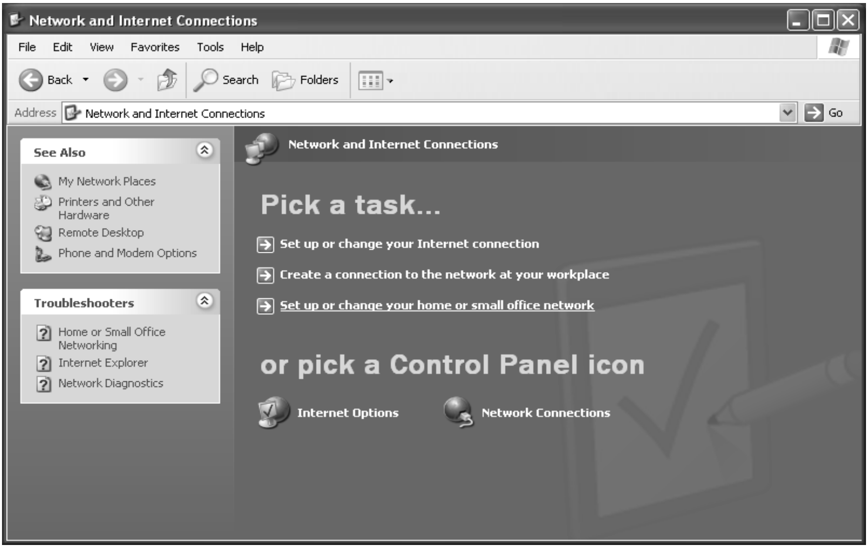
Launching the network wizard

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***.


Network and Internet Connections
File Edit View Favorites Tools Help
Back
Search
Folders
Address
Network and Internet Connections
Go
See Also
My Network Places
Printers and Other Hardware
Remote Desktop
Phone and Modem Options
Troubleshooters
Home or Small Office Networking
Internet Explorer
Network Diagnostics
Network and Internet Connections
Pick a task...
Set up or change your Internet connection
Create a connection to the network at your workplace
Set up or change your home or small office network
or pick a Control Panel icon
Internet Options
Network Connections

This launches the network wizard.

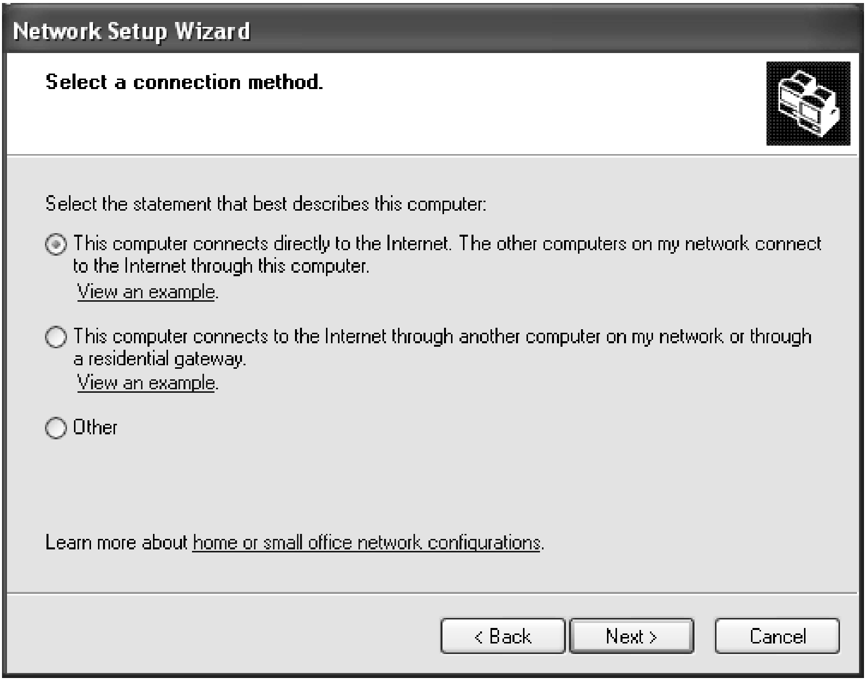
→ Skip the welcome screen and the checklist by clicking ***Next*** each time.

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.



Network Setup Wizard

Select a connection method.

Select the statement that best describes this computer:

● This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer.
View an example.

○ This computer connects to the Internet through another computer on my network or through a residential gateway.
View an example.

○ Other

Learn more about home or small office network configurations.

➞ Select ***This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer.*** and click ***Next***.

➞ In the next window select your network adapter and click ***Next.***

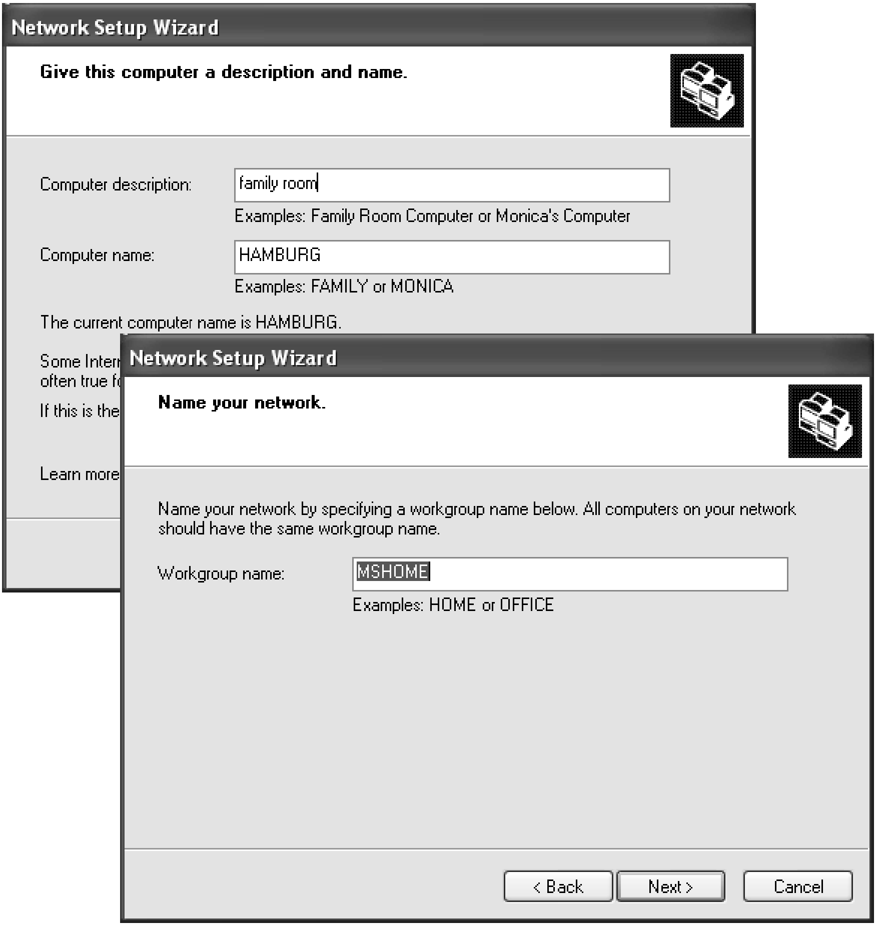
➞ Skip the message ***This network configuration is not advisable*** with ***Next***.

Selecting computer names and workgroup

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

→ Enter the name the PC is to appear under on the network. This name must be unique within the network. You can complete the ***Computer description*** box or leave it empty. Then click ***Next***.

→ Enter a name for the workgroup the PC is to belong to. This name must be identical for all the PC's in the network. Confirm this with ***Next***.



Network Setup Wizard

Give this computer a description and name.

Computer description: family room

Examples: Family Room Computer or Monica's Computer

Computer name: HAMBURG

Examples: FAMILY or MONICA

The current computer name is HAMBURG.

Some Inter
often true f

If this is the

Learn more

Network Setup Wizard

Name your network.

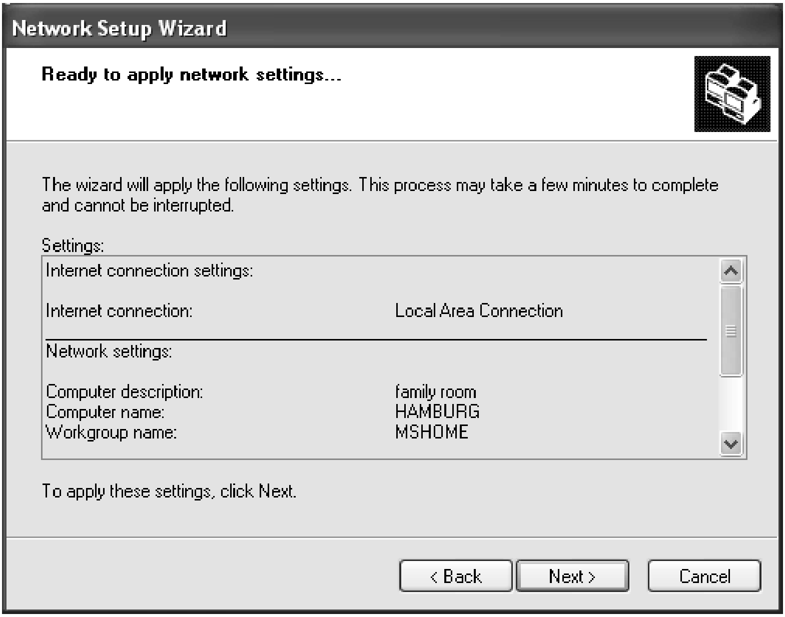
Name your network by specifying a workgroup name below. All computers on your network should have the same workgroup name.

Workgroup name: MSHOME

Examples: HOME or OFFICE

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.



Network Setup Wizard

Ready to apply network settings...

The wizard will apply the following settings. This process may take a few minutes to complete and cannot be interrupted.

Settings:

Internet connection settings:

Internet connection:	Local Area Connection

Network settings:

Computer description:	family room
Computer name:	HAMBURG
Workgroup name:	MSHOME

To apply these settings, click Next.

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

Completing the installation procedure

If you do not want to install any more PCs:

- ➙ Select ***Only finish the wizard, as it is not run on other computers*** and confirm twice with ***Next***.
- ➙ Answer the prompt ***Do you want to restart your computer now?*** with ***Yes***.
- ➙ If you want to set up a network on other PCs with Windows XP, you can now create a network installation disk.
- ➙ Select ***Create a network installation disk*** and click ***Next***.
- ➙ Follow the screen instructions and insert a disk. The necessary data will now be copied. Now label the disk as ***Network installation.***
- ➙ Confirm the next two screens with ***Next*** and complete the installation procedure by rebooting the PC.

After restarting the PC, your local network is installed.

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

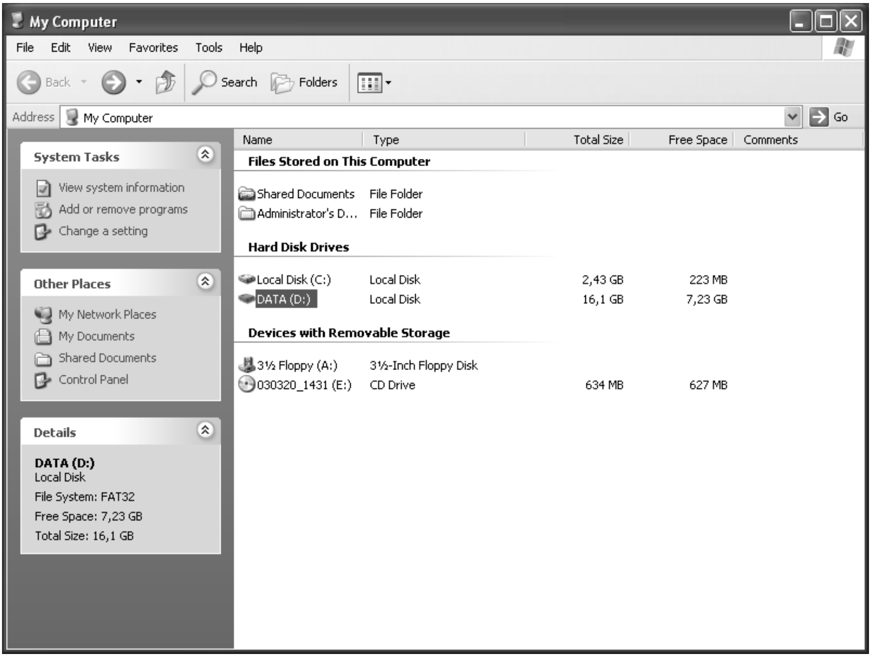
Releasing files and printers

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

Releasing files

→ Open the ***Desktop*** and left-click the folder or drive you want to release.

→ Now select the entry ***Release and security*** with the right-hand mouse button from the pop-up menu.



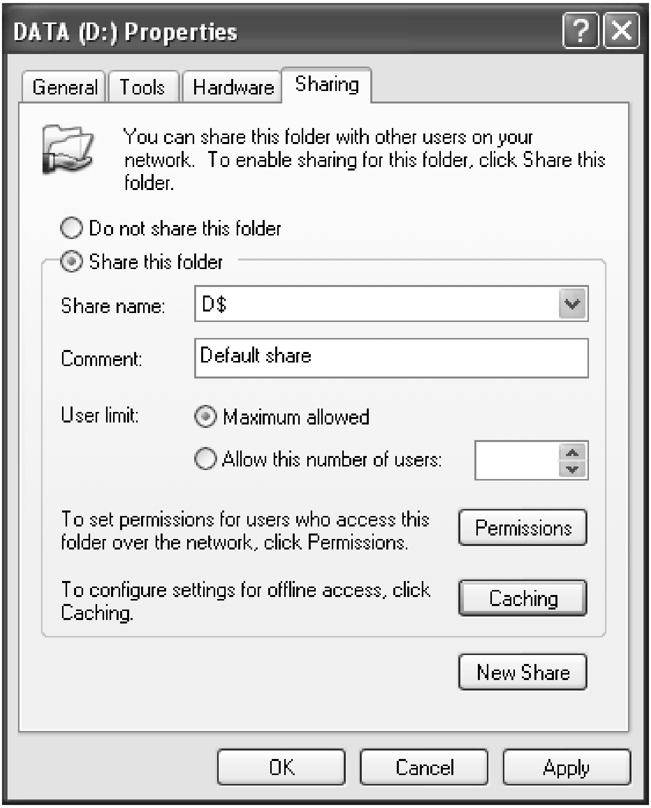
Name	Type	Total Size	Free Space	Comments
Files Stored on This Computer				
Shared Documents	File Folder			
Administrator's D...	File Folder			
Hard Disk Drives				
Local Disk (C:)	Local Disk	2,43 GB	223 MB	
DATA (D:)	Local Disk	16,1 GB	7,23 GB	
Devices with Removable Storage				
3½ Floppy (A:)	3½-Inch Floppy Disk			
030320_1431 (E:)	CD Drive	634 MB	627 MB	

DATA (D:)
Local Disk
File System: FAT32
Free Space: 7,23 GB
Total Size: 16,1 GB

→ 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***.



DATA (D:) Properties

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: D$

Comment: Default share

User limit: ● Maximum allowed

○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

To configure settings for offline access, click Caching.

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

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

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

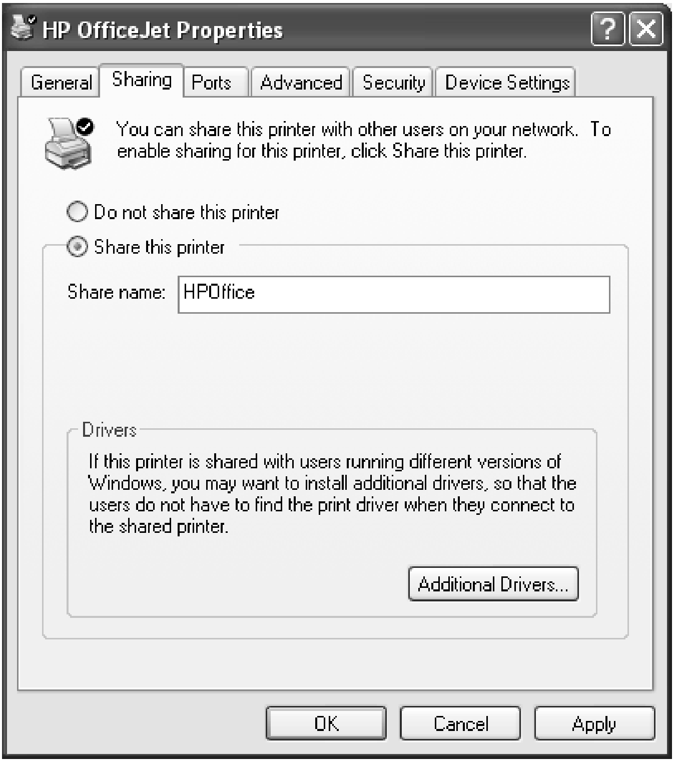
Releasing printers

→ To release printers select ***Printers and Faxes*** in the start menu.

→ Left-click the printer you want to release.

→ Now select the entry ***Sharing*** with the right-hand mouse button.

→ The window for defining the printer properties will appear, and the ***Sharing*** tab is open.



You can share this printer with other users on your network. To enable sharing for this printer, click Share this printer.

○ Do not share this printer

● Share this printer

Share name: HPOffice

Drivers

If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

→ 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)

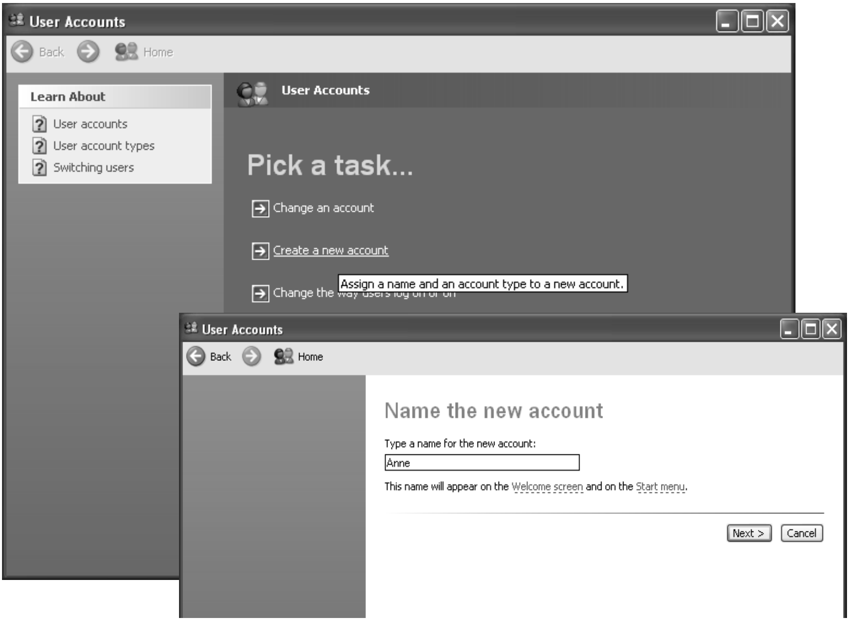
You can use resources on your PC such as files and printers that have been made available by other PCs.

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***.

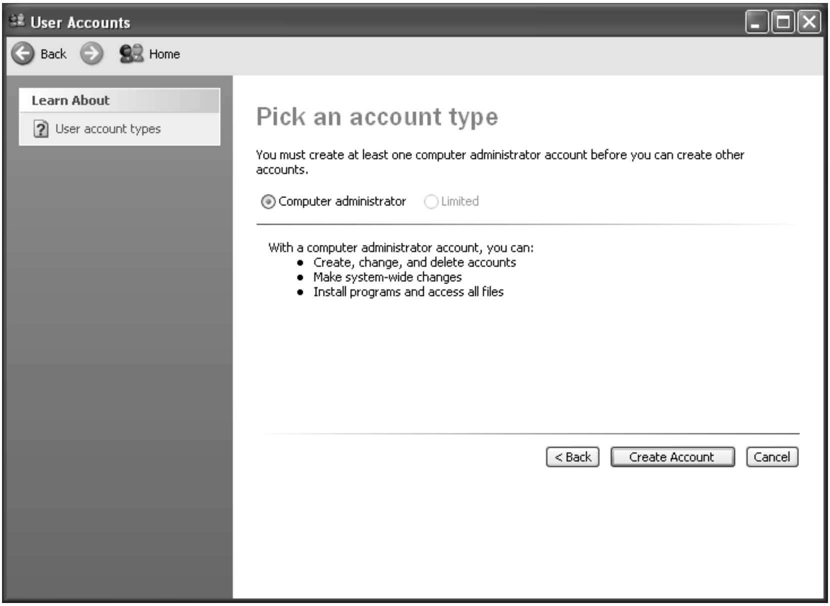


→ Select ***Create new account***.

→ Enter a name for the user.

→ Click ***Next.***

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



User Accounts

Back Home

Learn About

User account types

Pick an account type

You must create at least one computer administrator account before you can create other accounts.

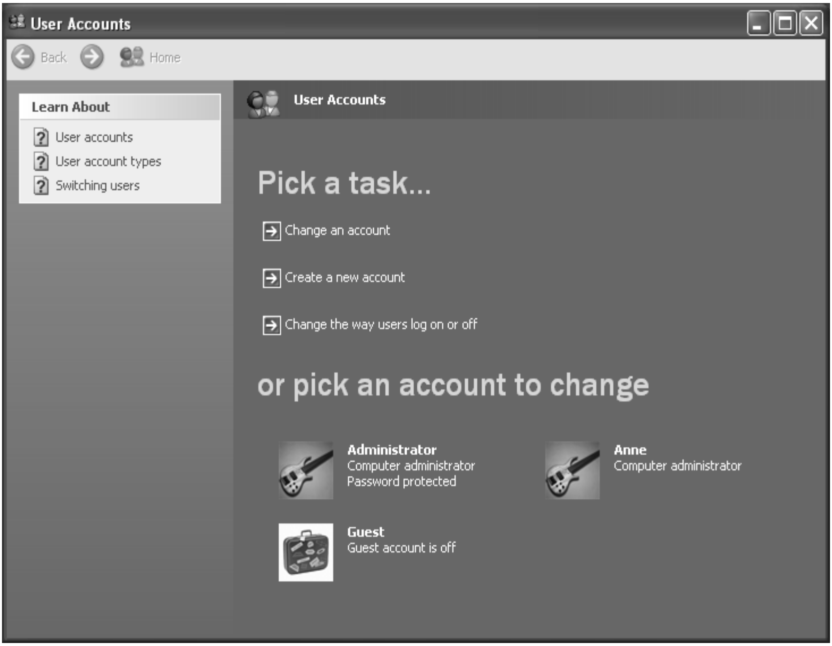
● Computer administrator ○ Limited

With a computer administrator account, you can:

- Create, change, and delete accounts
- Make system-wide changes
- Install programs and access all files

< Back | Create Account | Cancel

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



User Accounts

Back Home

Learn About

User accounts

User account types

Switching users

User Accounts

Pick a task...

Change an account

Create a new account

Change the way users log on or off

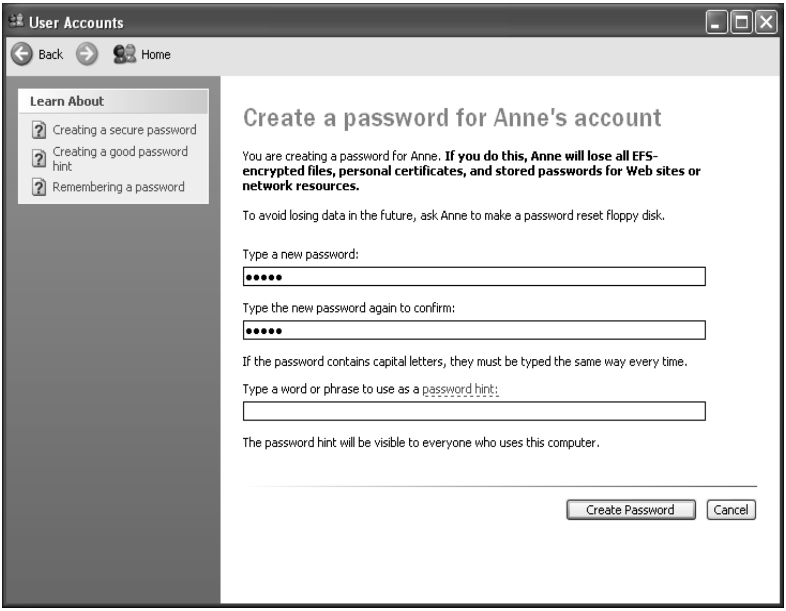
or pick an account to change

Administrator
Computer administrator
Password protected

Anne
Computer administrator

Guest
Guest account is off

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



Create a password for Anne's account

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.**

To avoid losing data in the future, ask Anne to make a password reset floppy disk.

Type a new password:

●●●●●

Type the new password again to confirm:

●●●●●

If the password contains capital letters, they must be typed the same way every time.

Type a word or phrase to use as a password hint:

The password hint will be visible to everyone who uses this computer.

- 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 84).

  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 102).

  You should choose this alternative if you want to work directly with the files or folders of the other PC. In this case, hook on an entire released drive or folder in your PC's file system and work with the files as if they were files on your PC.

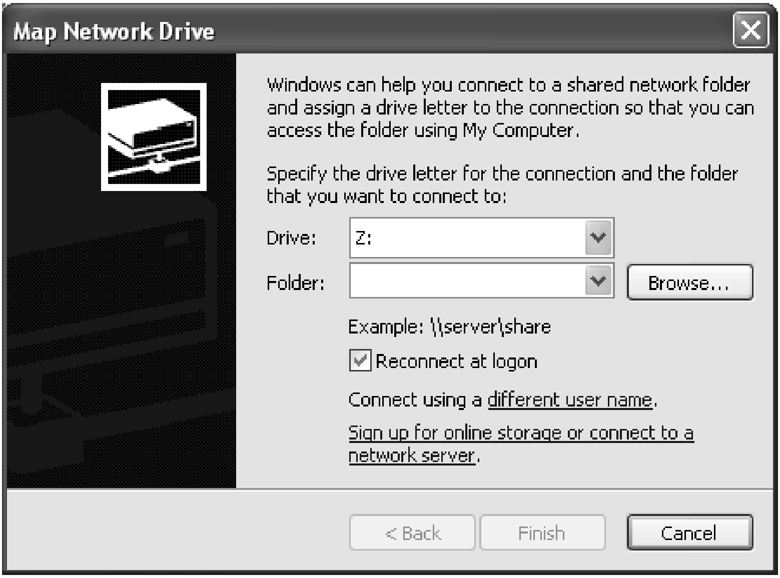
Please note:

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

To hook up network drives:

→ Open the ***Desktop***.

→ In the ***Extras*** menu, select ***Map network drive***.



Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder:

Example: \\server\share

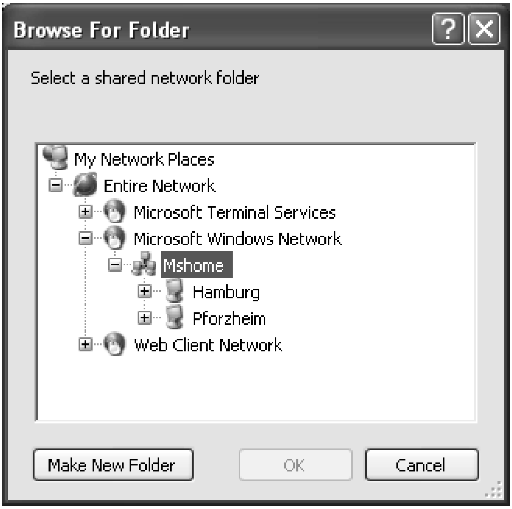
☑ Reconnect at logon

Connect using a different user name.

Sign up for online storage or connect to a network server.

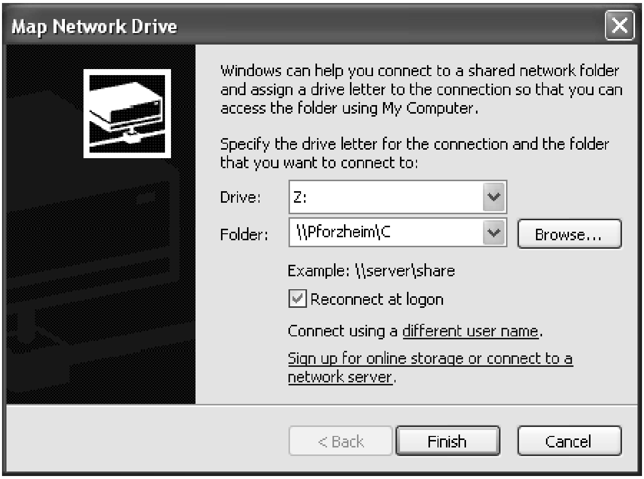
→ Select the drive name under which the remote drive is to be hooked on to your PC.

→ 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.



Select a shared network folder

→ Select the resource you want and click ***OK***.



Map Network Drive

Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder: \\Pforzheim\C

Example: \\server\share

☑ Reconnect at logon

Connect using a different user name.

Sign up for online storage or connect to a network server.

→ If you select the option ***Reconnect at logon***, Windows will hook the drive on every time you start your PC, provided the remote PC is running.

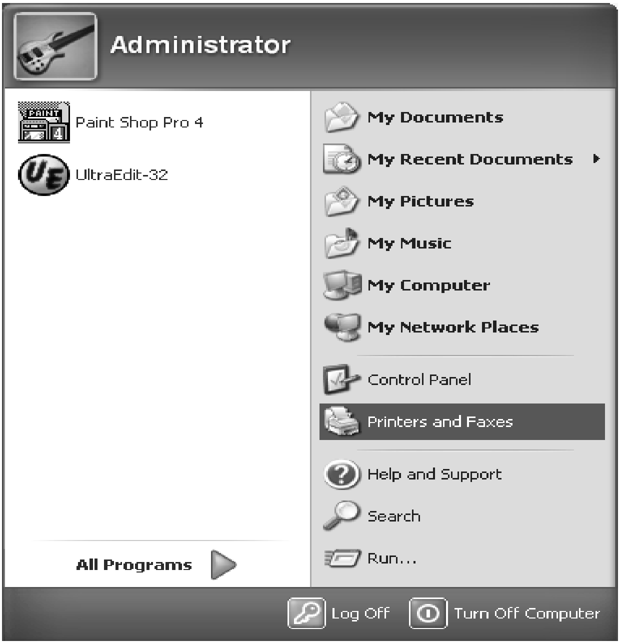
→ Click ***Finish***.

→ Now open the desktop. The remote drive is now available as the network drive. You can access the files as if they were on your own PC.

Accessing released printers from your PC

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

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



→ Select ***Add printer***. This opens the printer installation wizard.

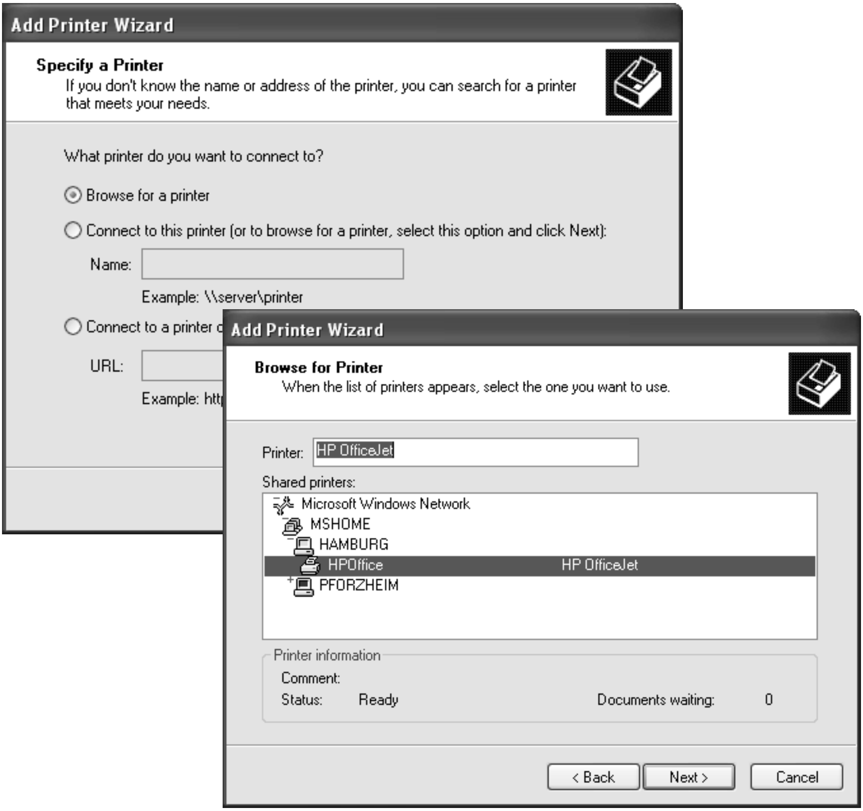
→ Click ***Next***.

→ In the next window select ***Network printer or printer connected to another computer***.

→ Click ***Next*** again.

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

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



Add Printer Wizard

Specify a Printer

If you don't know the name or address of the printer, you can search for a printer that meets your needs.

What printer do you want to connect to?

● Browse for a printer

○ Connect to this printer (or to browse for a printer, select this option and click Next):

Name:

Example: \\server\printer

○ Connect to a printer o

URL:

Example: htt

Add Printer Wizard

Browse for Printer

When the list of printers appears, select the one you want to use.

Printer: HP OfficeJet

Shared printers:

Microsoft Windows Network
MSHOME
HAMBURG
HPOffice HP OfficeJet
PFORZHEIM

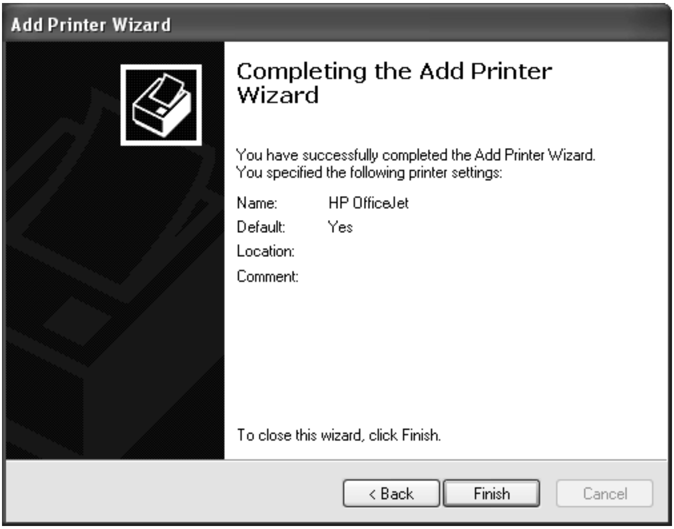
Printer information

Comment:

Status: Ready Documents waiting: 0

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

→ Complete printer installation with ***Finish***.



Completing the Add Printer Wizard

You have successfully completed the Add Printer Wizard.
You specified the following printer settings:

Name:	HP OfficeJet
Default:	Yes
Location:	
Comment:	

To close this wizard, click 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)

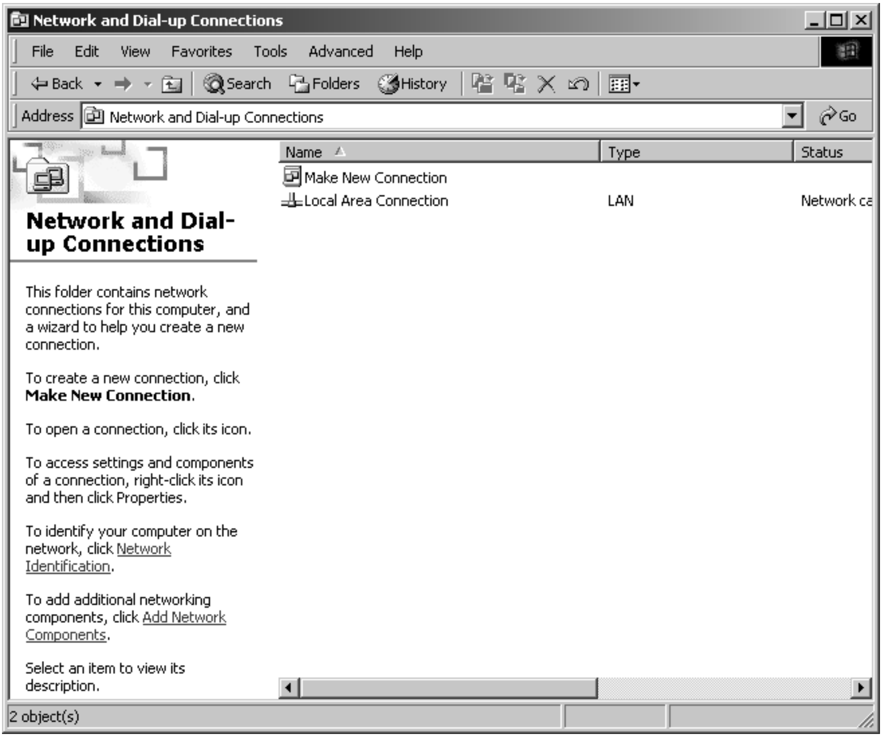
To release files or printers on a PC with Windows 2000 for other users on the network:

1. Install the network services (see below).
2. Select computer names and workgroup (see page 109).
3. Set TCP/IP protocol (see page 110).
4. Set up users (see page 112).
5. Release files and printer (see page 115).

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***.



Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go

Network and Dial-up Connections

This folder contains network connections for this computer, and a wizard to help you create a new connection.

To create a new connection, click **Make New Connection**.

To open a connection, click its icon.

To access settings and components of a connection, right-click its icon and then click Properties.

To identify your computer on the network, click Network Identification.

To add additional networking components, click Add Network Components.

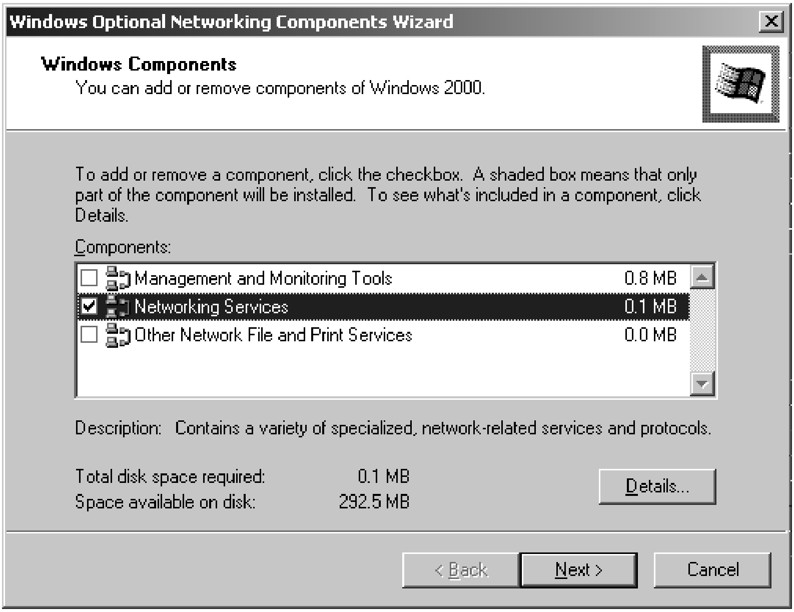
Select an item to view its description.

Name	Type	Status
Make New Connection		
Local Area Connection	LAN	Network ca

2 object(s)

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

→ Select ***Networking services*** and click ***Next***.



Windows Optional Networking Components Wizard

Windows Components
You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

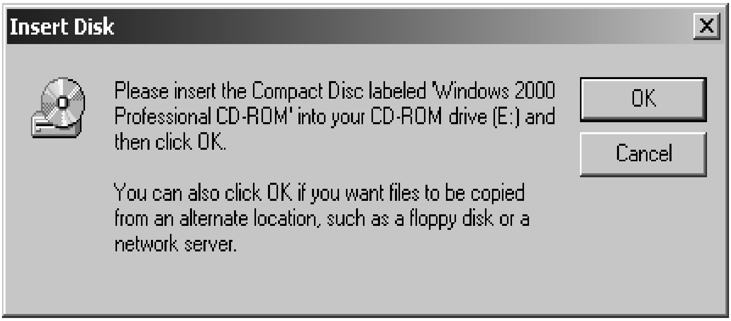
Components:

☐	Management and Monitoring Tools	0.8 MB
☑	Networking Services	0.1 MB
☐	Other Network File and Print Services	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.1 MB
Space available on disk: 292.5 MB

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



Insert Disk

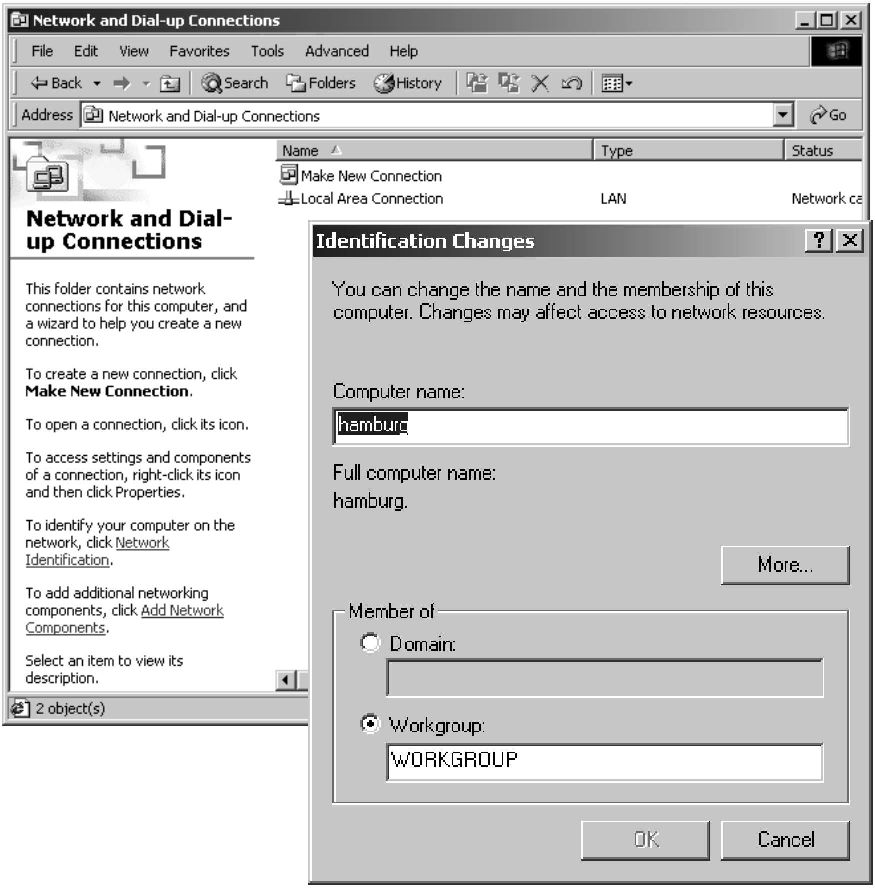
Please insert the Compact Disc labeled 'Windows 2000 Professional CD-ROM' into your CD-ROM drive (E:) and then click OK.

You can also click OK if you want files to be copied from an alternate location, such as a floppy disk or a network server.

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***.



Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Go
Name Type Status
Make New Connection
Local Area Connection LAN Network ca
2 object(s)
Identification Changes
More...
OK Cancel

Address: Network and Dial-up Connections

Network and Dial-up Connections

This folder contains network connections for this computer, and a wizard to help you create a new connection.

To create a new connection, click **Make New Connection**.

To open a connection, click its icon.

To access settings and components of a connection, right-click its icon and then click Properties.

To identify your computer on the network, click Network Identification.

To add additional networking components, click Add Network Components.

Select an item to view its description.

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name: hamburg

Full computer name: hamburg.

Member of

○ Domain:

● Workgroup: WORKGROUP

→ 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.

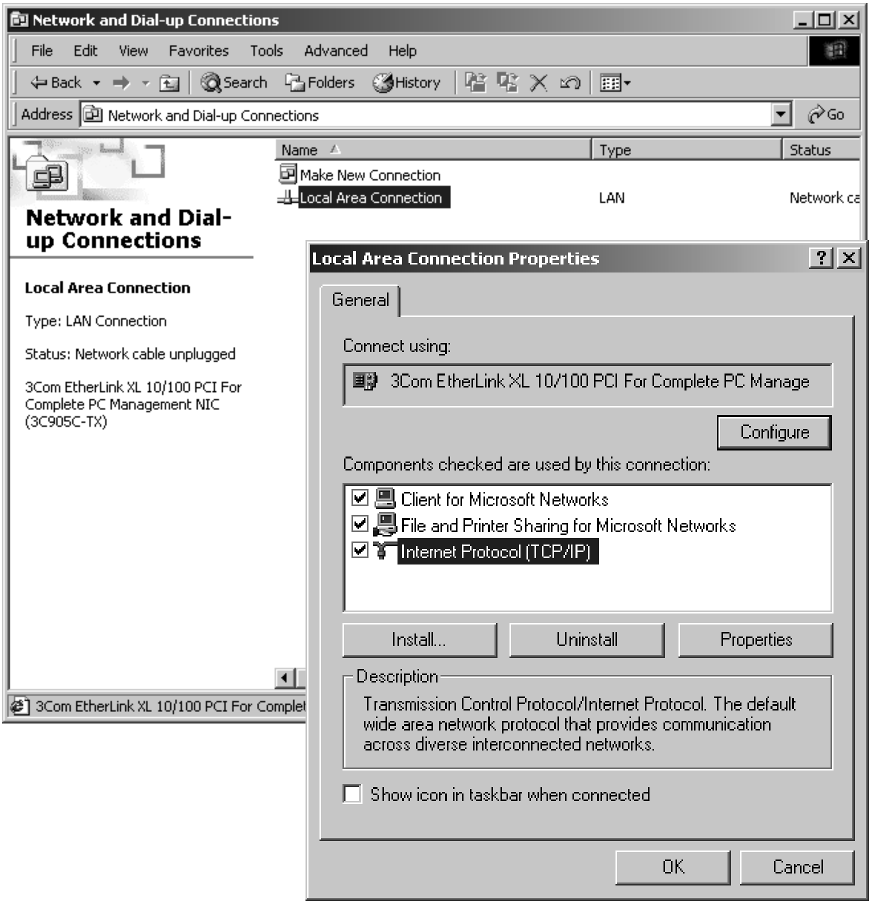
→ In the ***Workgroup*** box, enter a name for the workgroup. This name must be the same for all the PCs on the network.

→ 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***.



Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections Go
Name Type Status
Make New Connection
Local Area Connection LAN Network ca
Network and Dial-up Connections

Local Area Connection

Type: LAN Connection

Status: Network cable unplugged

3Com EtherLink XL 10/100 PCI For Complete PC Management NIC (3C905C-TX)

3Com EtherLink XL 10/100 PCI For Complet

Local Area Connection Properties

General

Connect using:

3Com EtherLink XL 10/100 PCI For Complete PC Manage

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

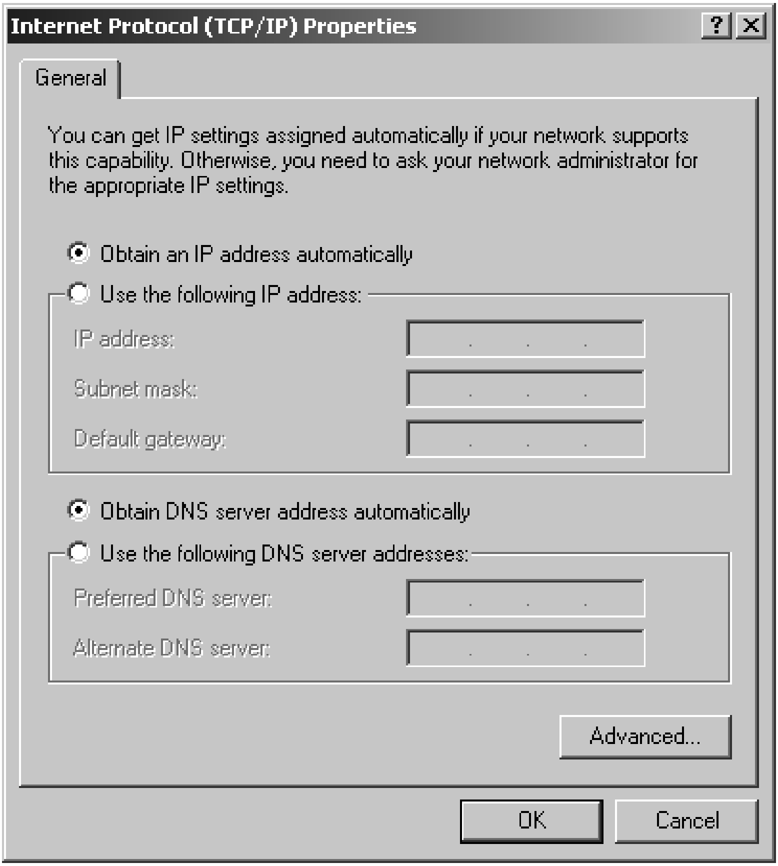
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

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

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

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



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: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

→ Close this and the next window with ***OK***.

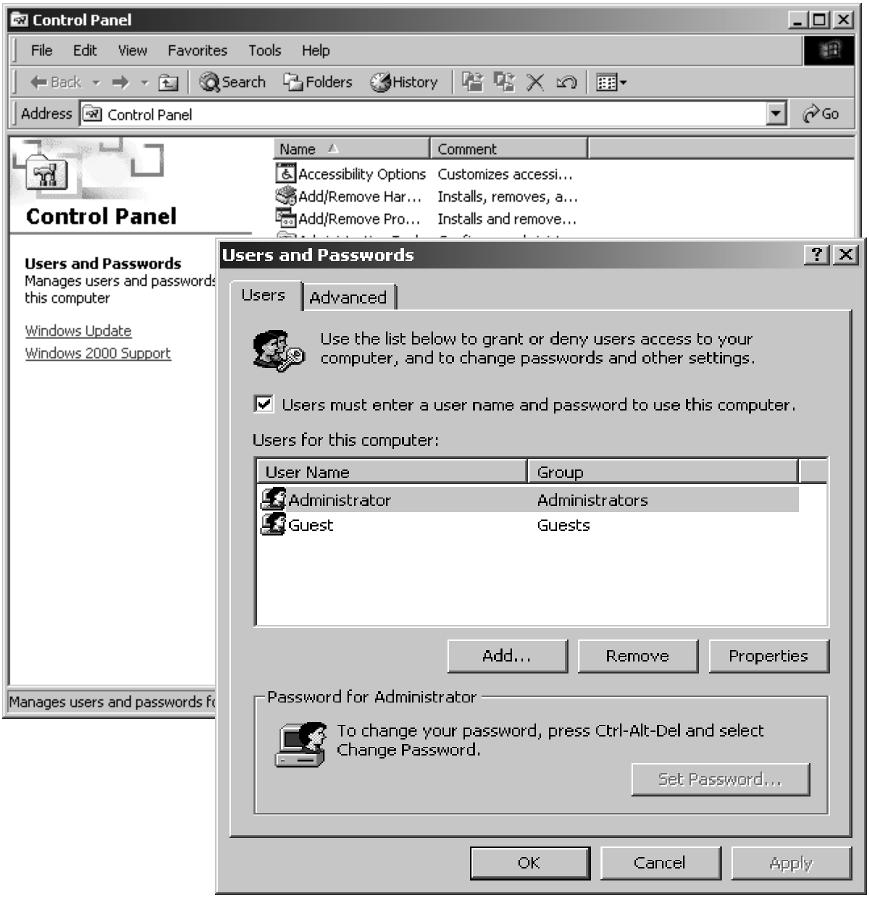
Please note:

You can of course define IP addresses manually. This is necessary for example in ad-hoc networks. How to assign static IP addresses is described in the Appendix on page 126.

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***.



Users and Passwords
Manages users and passwords this computer

Manages users and passwords f

Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

☑ Users must enter a user name and password to use this computer.

Users for this computer:

User Name	Group
Administrator	Administrators
Guest	Guests

Password for Administrator

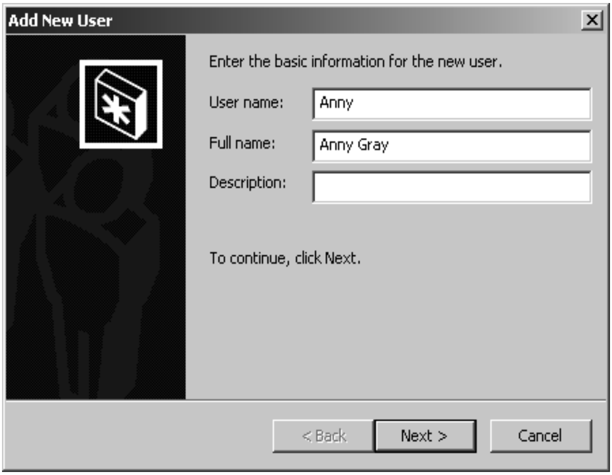
To change your password, press Ctrl-Alt-Del and select Change Password.

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

→ Click ***Add***.

→ 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***.



Add New User

Enter the basic information for the new user.

User name: Anny

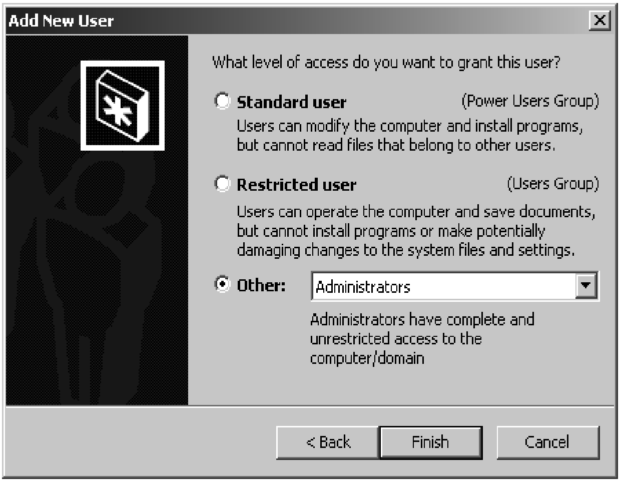
Full name: Anny Gray

Description:

To continue, click Next.

→ 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***.



Add New User

What level of access do you want to grant this user?

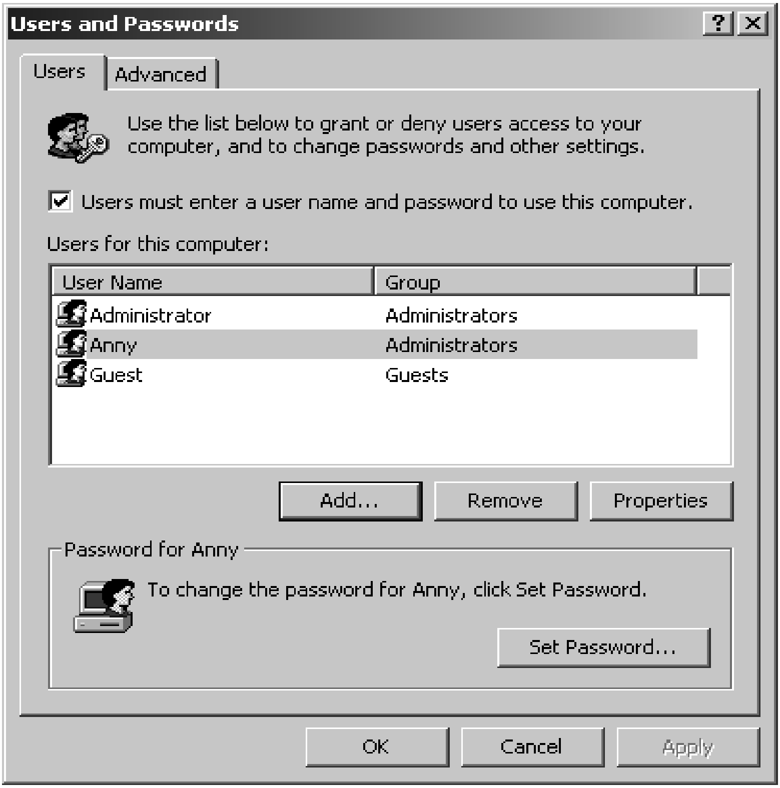
○ **Standard user** (Power Users Group)
Users can modify the computer and install programs, but cannot read files that belong to other users.

○ **Restricted user** (Users Group)
Users can operate the computer and save documents, but cannot install programs or make potentially damaging changes to the system files and settings.

● **Other:** Administrators
Administrators have complete and unrestricted access to the computer/domain

→ 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***.



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

☑ Users must enter a user name and password to use this computer.

Users for this computer:

User Name	Group
Administrator	Administrators
Anny	Administrators
Guest	Guests

Password for Anny

To change the password for Anny, click Set Password.

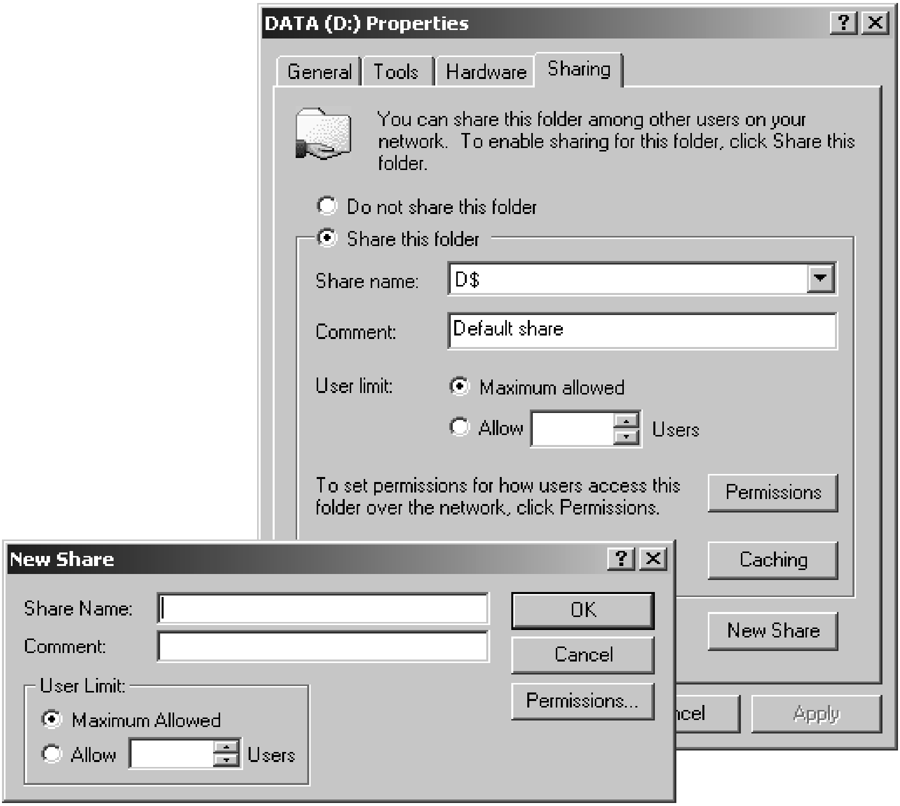
Releasing files and printers

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.



DATA (D:) Properties

You can share this folder among other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: D$

Comment: Default share

User limit: ● Maximum allowed ○ Allow Users

To set permissions for how users access this folder over the network, click Permissions.

New Share

Share Name:

Comment:

User Limit: ● Maximum Allowed ○ Allow Users

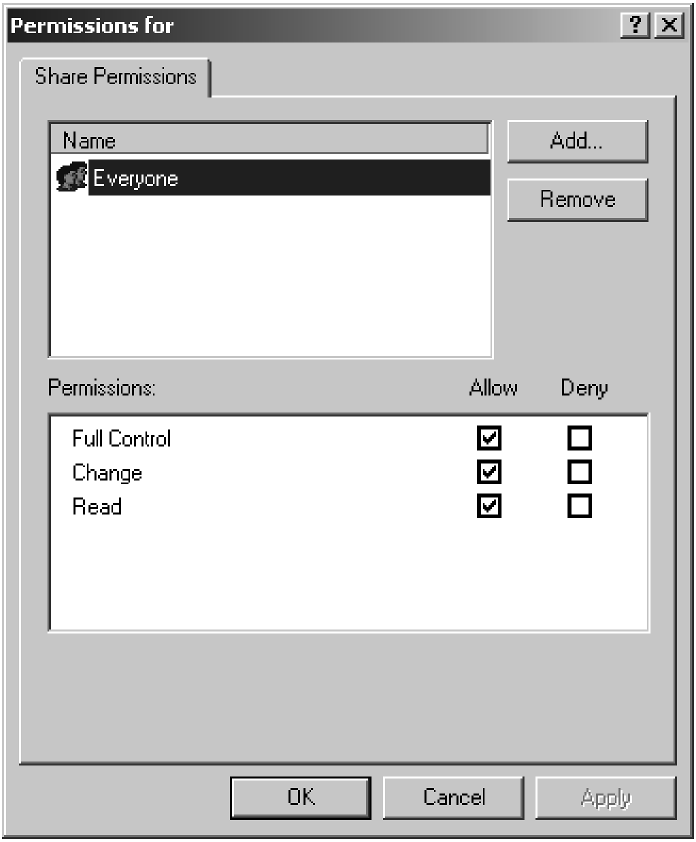
→ Select ***Share this folder*** and click ***New share***.

→ 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***.



Permissions for

Share Permissions

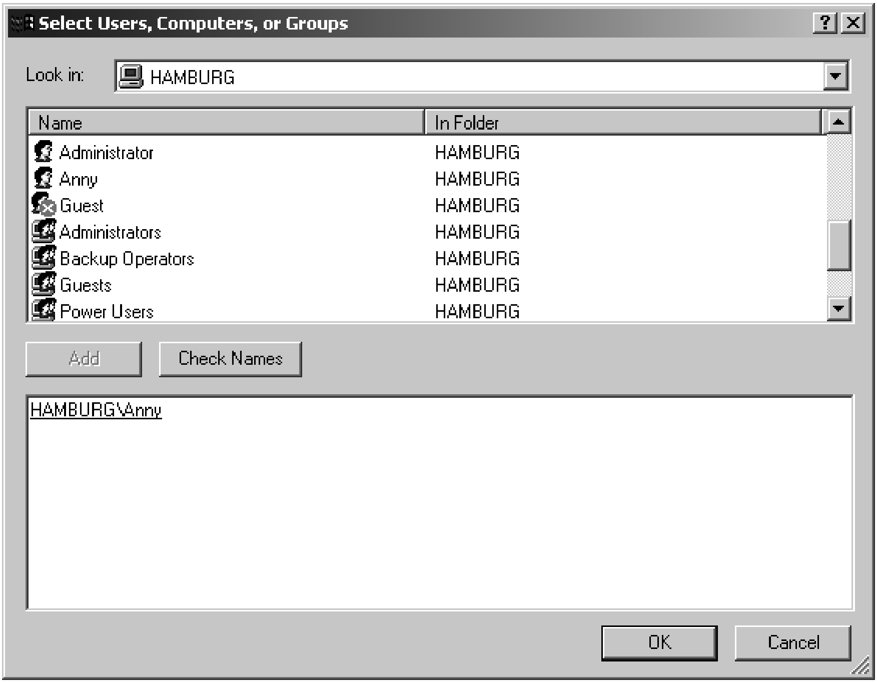
Name

Everyone

Permissions:

Permissions:	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

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

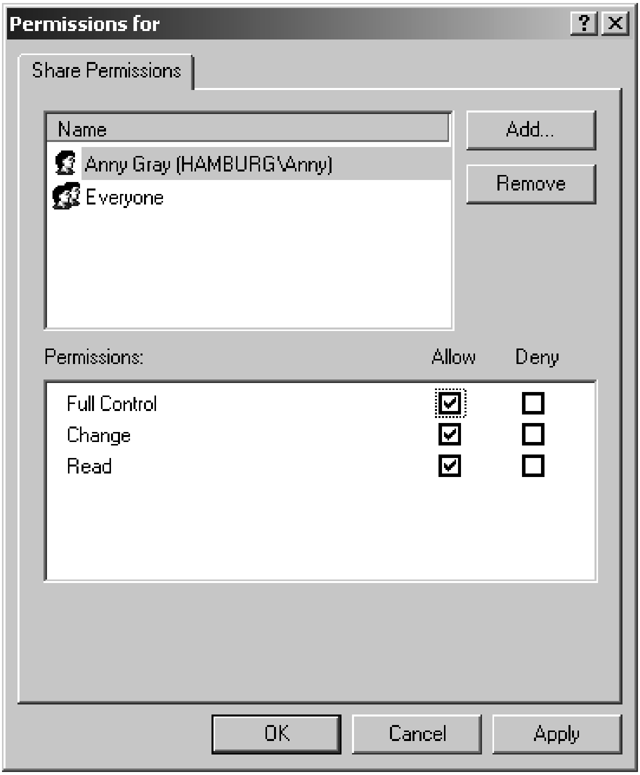


Name	In Folder
Administrator	HAMBURG
Anny	HAMBURG
Guest	HAMBURG
Administrators	HAMBURG
Backup Operators	HAMBURG
Guests	HAMBURG
Power Users	HAMBURG

HAMBURG\Anny

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.



Name

Anny Gray (HAMBURG\Anny)

Everyone

Permissions:	Allow	Deny
Full Control	☑	☐
Change	☑	☐
Read	☑	☐

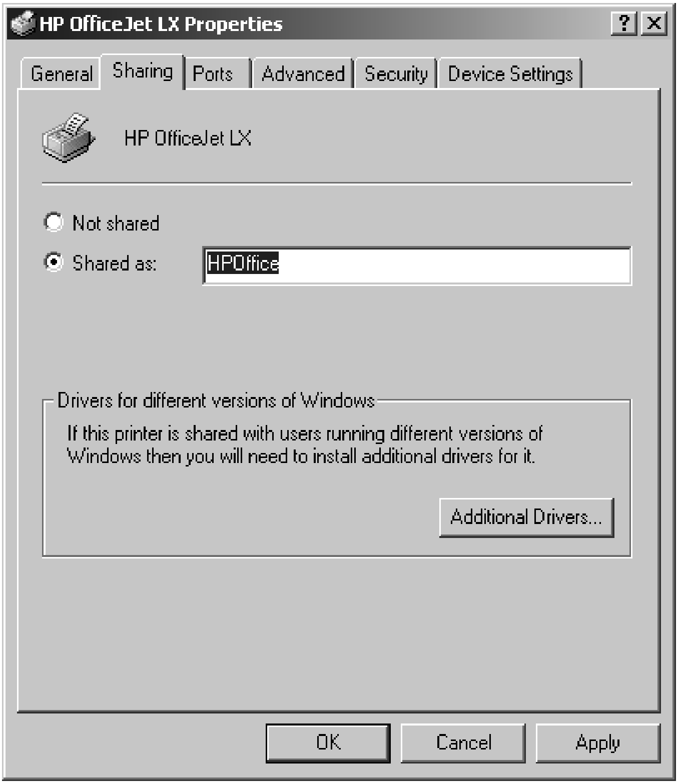
→ To save the settings you have made, click ***Apply*** and ***OK***. Close the next window as well with ***OK***. Close the properties window with ***OK***.

Releasing 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.***



HP OfficeJet LX

○ Not shared

● Shared as: HPOffice

If this printer is shared with users running different versions of Windows then you will need to install additional drivers for it.

→ 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 84).

  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 121).

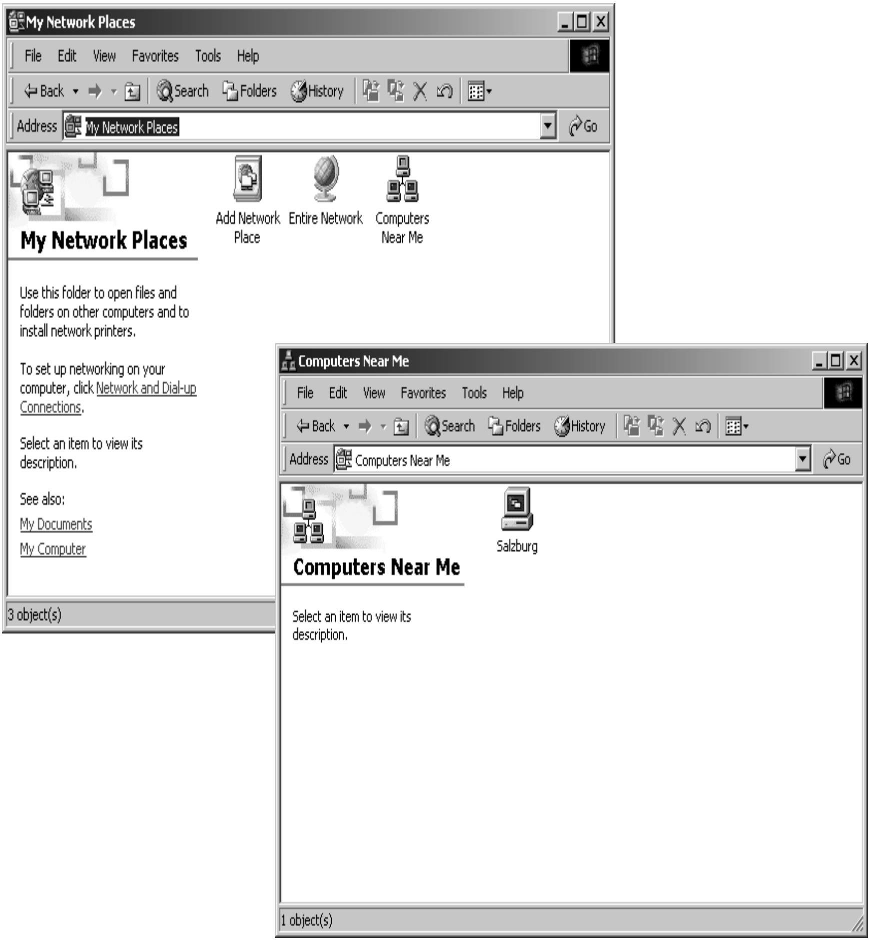
  You should choose this alternative if you want to work directly with the files or folders of the other PC. In this case, hook on an entire released drive or folder in your PC's file system and work with the files as if they were files on your PC.

Please note:

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

To hook up network drives:

→ Open the ***My NetworkPlaces*** and then ***Computers near me***.



Use this folder to open files and folders on other computers and to install network printers.

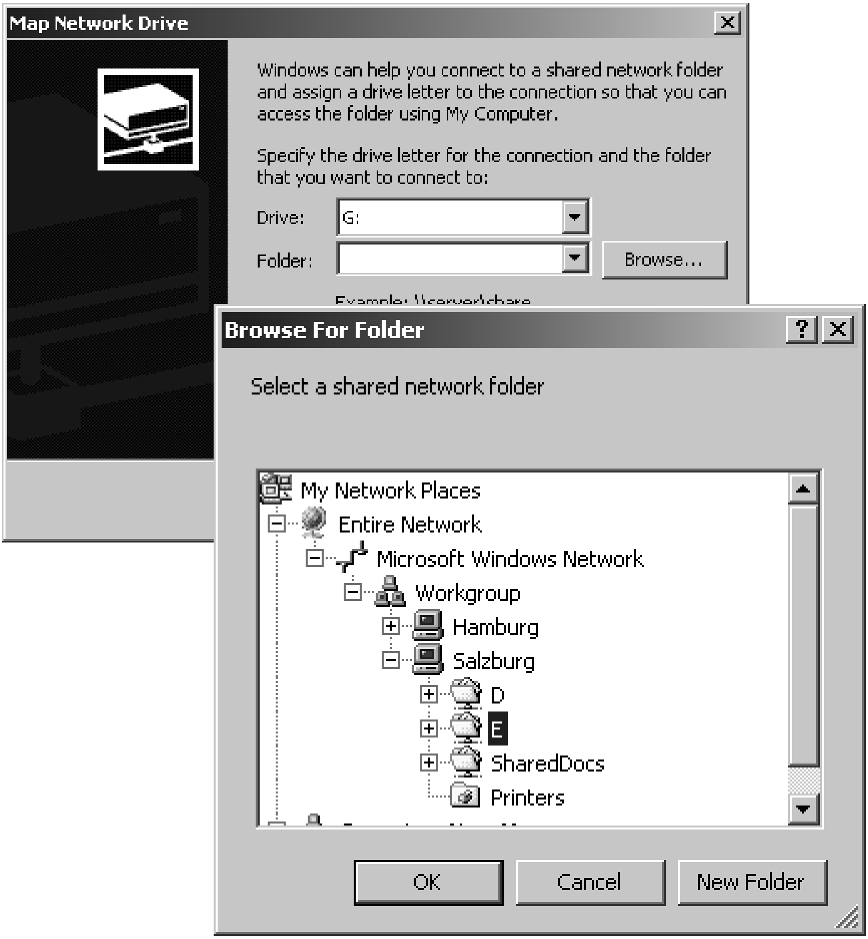
To set up networking on your computer, click Network and Dial-up Connections.

Select an item to view its description.

Select an item to view its description.

→ 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***.



Map Network Drive

Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: G:

Folder:

Example: \\server\share

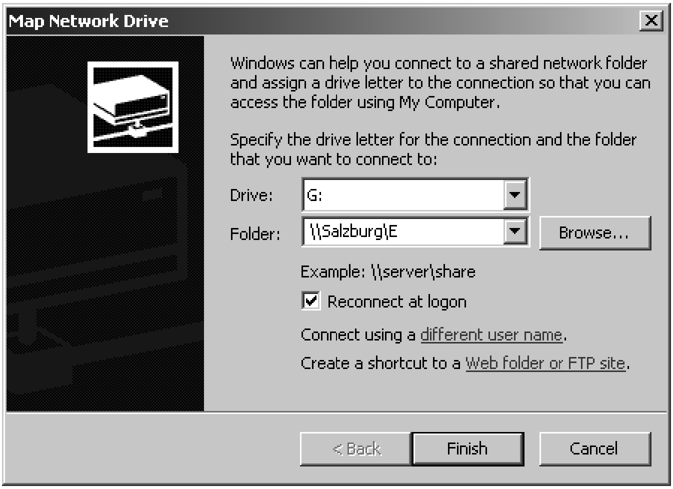
Browse For Folder

Select a shared network folder

→ 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***.



Map Network Drive

Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: G:

Folder: \\Salzburg\E

Example: \\server\share

☑ Reconnect at logon

Connect using a different user name.

Create a shortcut to a Web folder or FTP site.

→ 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.

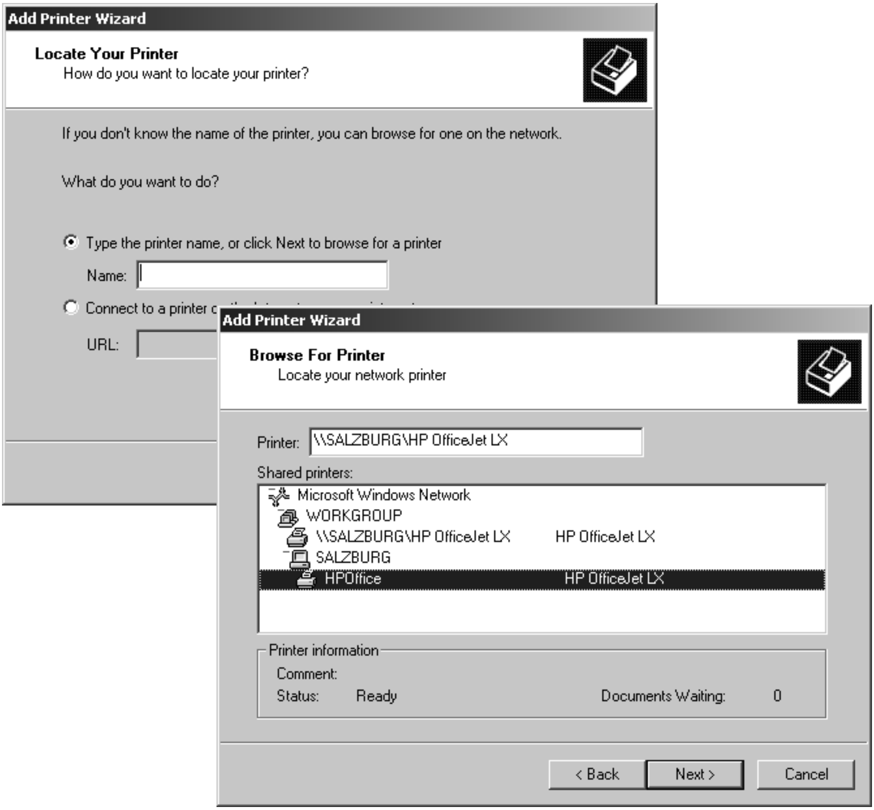
→ Click ***Next***.

→ 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***.



Add Printer Wizard

Locate Your Printer
How do you want to locate your printer?

If you don't know the name of the printer, you can browse for one on the network.

What do you want to do?

● Type the printer name, or click Next to browse for a printer

Name:

○ Connect to a printer c

URL:

Add Printer Wizard

Browse For Printer
Locate your network printer

Printer: \\SALZBURG\HP OfficeJet LX

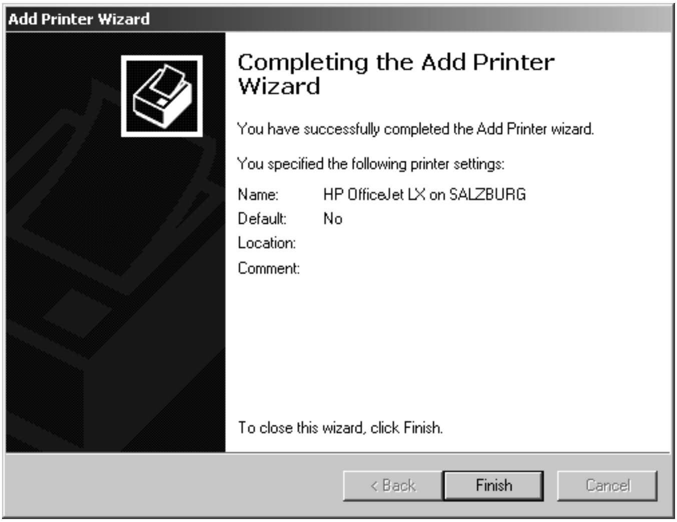
Shared printers:

Microsoft Windows Network
WORKGROUP
\\SALZBURG\HP OfficeJet LX	HP OfficeJet LX
SALZBURG
HPOffice	HP OfficeJet LX

Printer information
Comment:
Status: Ready	Documents Waiting: 0

→ 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***.



Completing the Add Printer Wizard

You have successfully completed the Add Printer wizard.

You specified the following printer settings:

Name:	HP OfficeJet LX on SALZBURG
Default:	No
Location:	
Comment:	

To close this wizard, click 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 127, for Windows XP from page 131 and for Windows 2000 from page 134.

Private IP addresses

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

192.168.0.0 – 192.168.255.254

Example:

PC 1: 192.168.15.1

PC 2: 192.168.15.2 etc.

Please note:

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

- Correct is e. g.:

  Router address: 192.168.2.1

  PC 1: 192.168.2.12

  PC 2: 192.168.2.60 ...

- Incorrect would be e. g.:

  Router address: 192.168.2.1

  PC 1: 192.168.3.2

  PC 2: 192.168.4.3

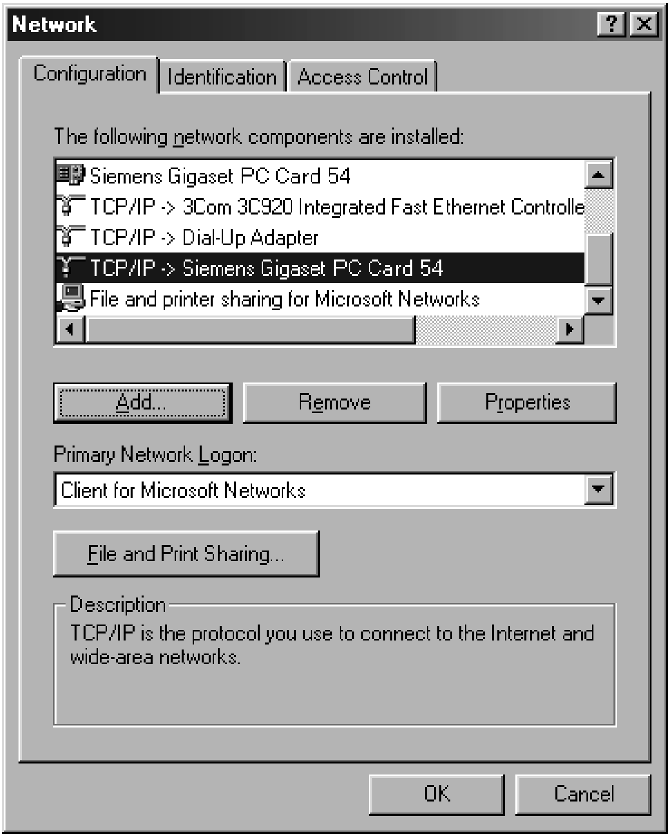
Windows 98

To set an IP address for your PC:

→ Select ***Start*** – ***Settings*** – ***Control Panel***.

→ Double-click the ***Network*** icon.

→ In the ***Network*** window, select the ***TCP/IP*** entry for your network card or network adapter in the ***Configuration*** tab. Make sure you select the right TCP/IP entry if there are several in the selection list.



Network

Configuration | Identification | Access Control

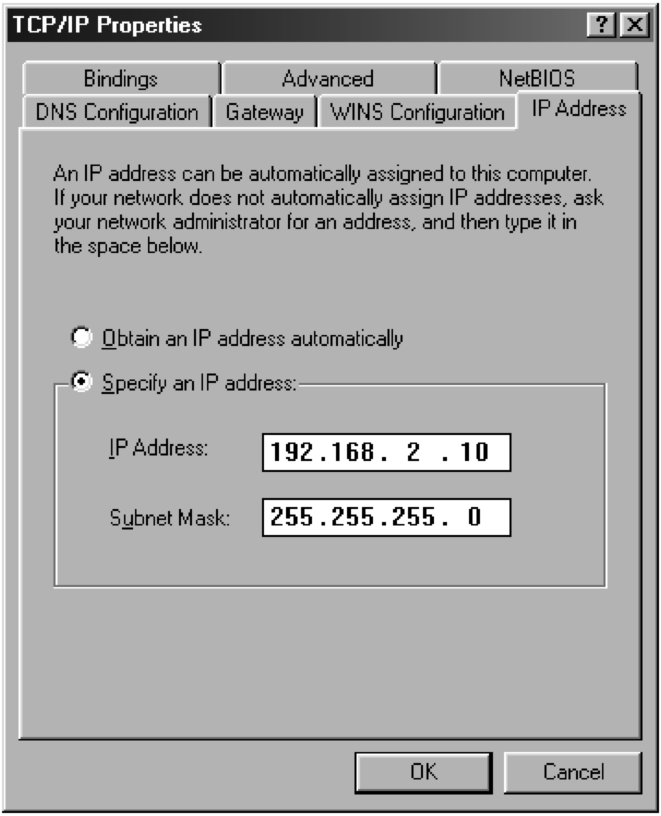
The following network components are installed:

- Siemens Gigaset PC Card 54
- TCP/IP -> 3Com 3C920 Integrated Fast Ethernet Controlle
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> Siemens Gigaset PC Card 54
- File and printer sharing for Microsoft Networks

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

→ Click ***Properties***.



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically

● Specify an IP address:

IP Address: 192.168. 2 .10

Subnet Mask: 255.255.255. 0

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

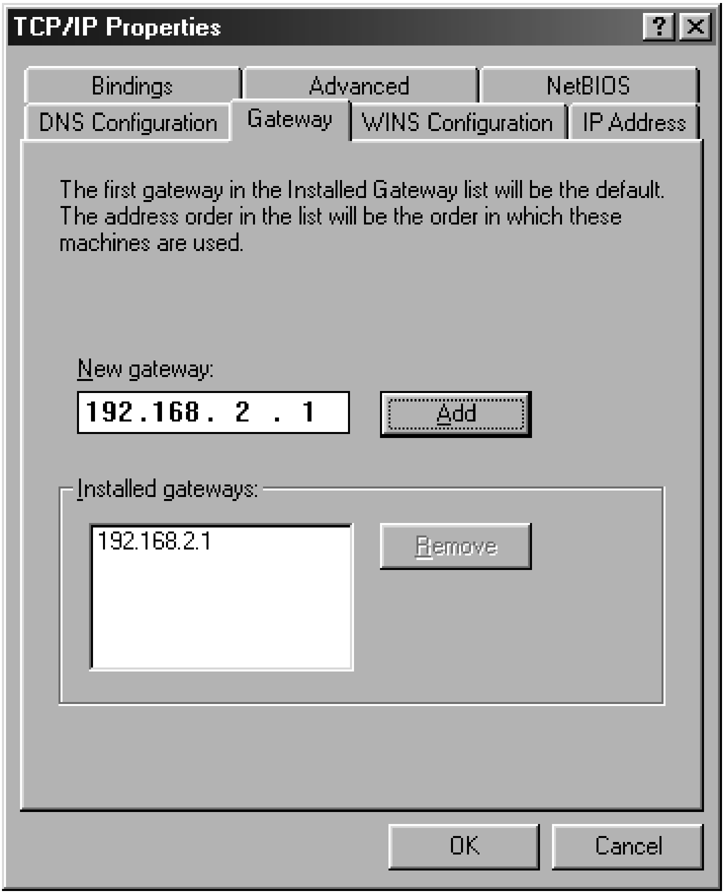
→ Enter the IP address for the PC in the ***IP address*** box. Please bear in mind the information on page 126.

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

Please note:

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

→ Open the ***Gateway*** tab.



TCP/IP Properties

The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway: 192.168.2.1

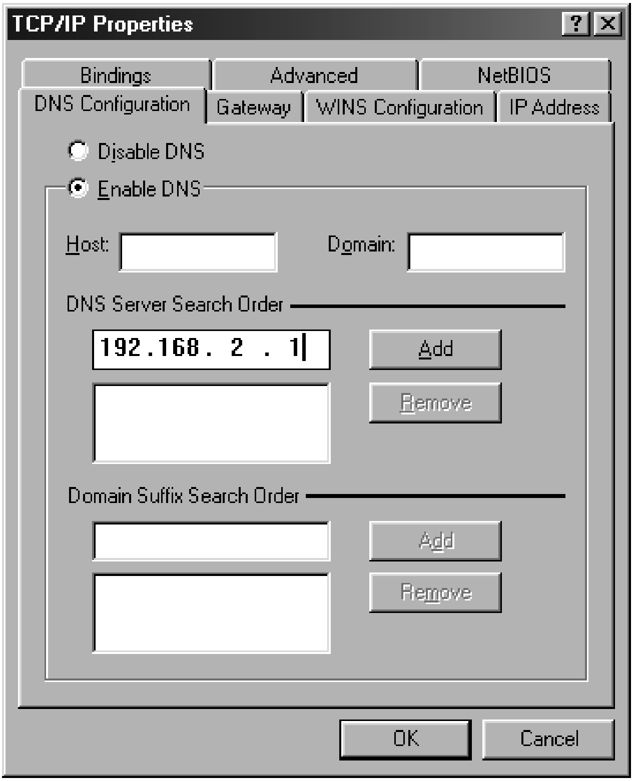
Installed gateways: 192.168.2.1

Please note:

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

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

→ Open the ***DNS configuration*** tab.



TCP/IP Properties

○ Disable DNS

● Enable DNS

Host:

Domain:

DNS Server Search Order

192.168. 2 . 1

Domain Suffix Search Order

→ Select ***Enable DNS***.

> **Please note:**
>
> DNS (Domain Name System) allows IP addresses to be assigned to a PC or domain names.

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

→ Click ***Add***.

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

→ Restart your network.

Windows XP

Please note:

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

This can be done as follows:

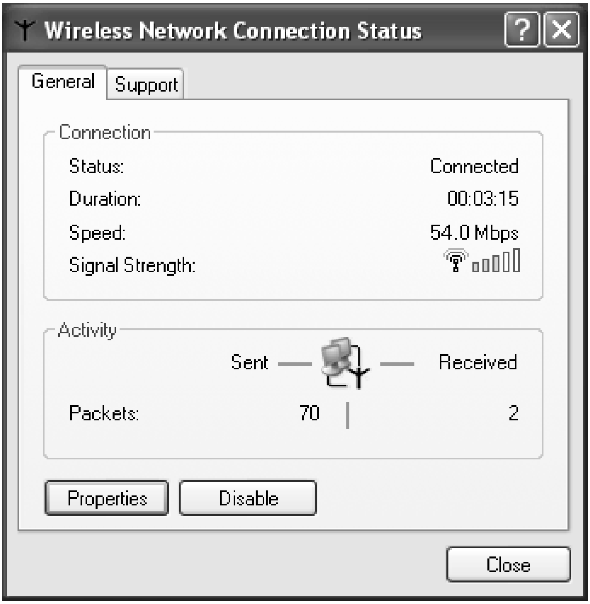
1. Click ***Start*** – ***Settings*** – ***Control Panel*** – ***Network Connections*** – ***LAN or High-Speed Internet*** – ***Wireless Network Connection*** – ***Properties***.
2. In ***Wireless Network Connection Properties*** click ***Wireless Networks***.
3. Deactivate ***Use Windows to configure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

To set a static IP address for your PC:

→ Click ***Start*** – ***Control Panel***.

→ Select ***Network and Internet Connections*** and then click the ***Network Connections*** icon.

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



Wireless Network Connection Status

Connection

Status: Connected

Duration: 00:03:15

Speed: 54.0 Mbps

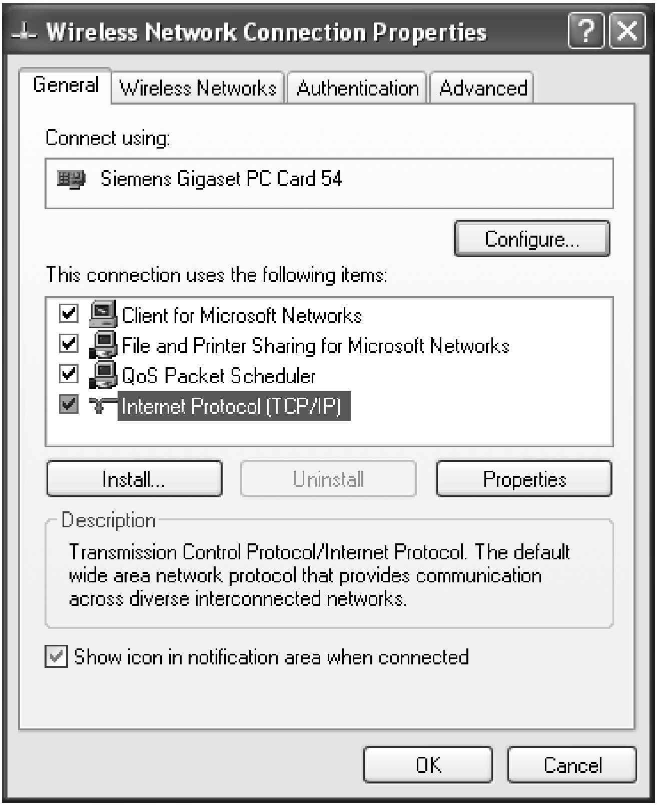
Signal Strength:

Activity

Sent — Received

Packets: 70 | 2

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



Wireless Network Connection Properties

General | Wireless Networks | Authentication | Advanced

Connect using:

Siemens Gigaset PC Card 54

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

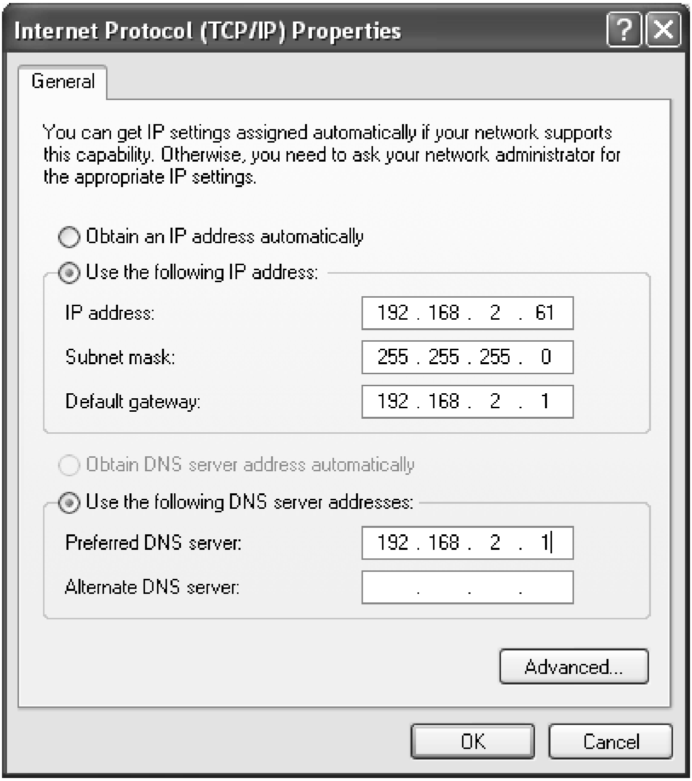
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

OK | Cancel

→ 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: . . .

→ 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 126.

Please note:

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

→ Enter the subnet mask 255.255.255.0 in the ***Subnet mask*** box.

→ Enter the IP address for the router in the ***Standard-Gateway*** box.

Please note:

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

→ Select ***Use the following DNS server addresses***.

> **Please note:**
>
> DNS (Domain Name System) allows IP addresses to be assigned to a PC or domain names.

→ Enter the IP address for the router in the ***Preferred DNS server*** box.

→ Click ***OK*** or ***Cancel*** to close each window.

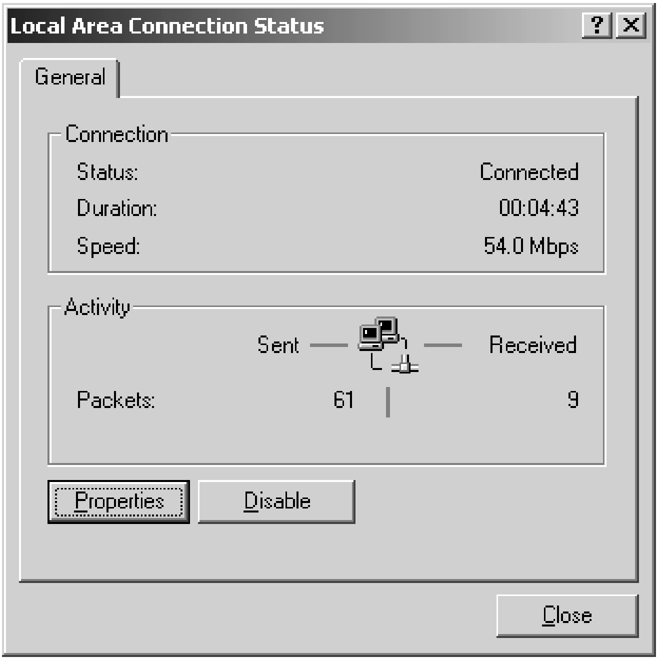
→ Restart your network.

Windows 2000

To set a static IP address for your PC:

→ Click ***Start*** – ***Settings*** – ***Control Panel***.

→ Double click the ***Network and Dial-up Connections*** icon and then ***Local Area Connection***.



Connection

Status: Connected

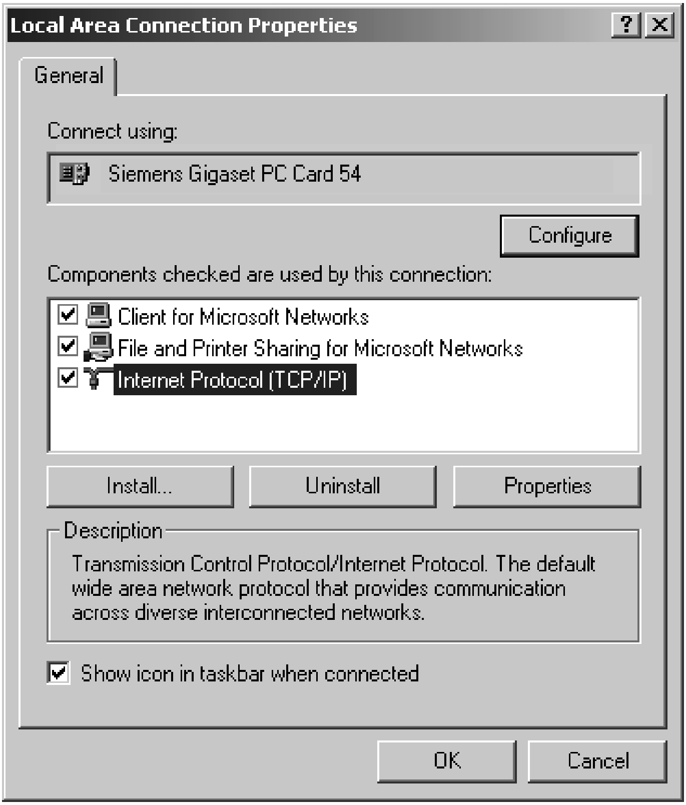
Duration: 00:04:43

Speed: 54.0 Mbps

Activity

	Sent	Received
Packets:	61	9

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



Local Area Connection Properties

General

Connect using:

Siemens Gigaset PC Card 54

Components checked are used by this connection:

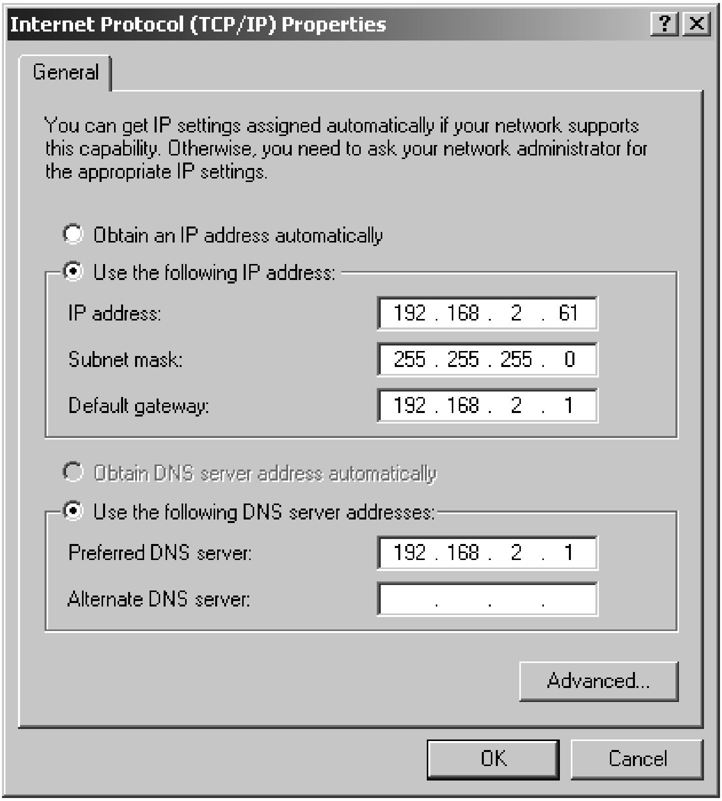
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

→ 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:	. . .

→ 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 126.

Please note:

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

→ Enter the subnet mask 255.255.255.0 in the ***Subnet mask*** box.

→ Enter the IP address for the router in the ***Standard-Gateway*** box.

Please note:

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

→ Select ***Use the following DNS server addresses***.

Please note:

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

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

Glossary

Access point

An Access Point, such as the Gigaset Appl, 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 Appl 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 Appl 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 Appl 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.

Dynamic IP address

A dynamic IP address is assigned to a network component automatically via DHCP. This means that the IP address of a network component can change with every login or at certain intervals.

See also: Static IP address

DynDNS

Dynamic DNS

Domain Name Service (DNS) is used to assign Domain names and IP addresss. For Dynamic IP addresss this service is now enhanced with the so-called Dynamic DNS (DynDNS). This permits the use of a PC with a changing IP address as a Server on the Internet. DynDNS ensures that a service on the Internet can always be addressed under the same Domain name regardless of the current IP address.

Encryption

Encryption protects confidential information against unauthorised access. With an encryption system data packets can be sent securely over a network. The Gigaset Appl 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).

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 Appl has a Private IP address and a Public IP address.

IP address pool

The Gigaset Appl'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 SE 105 dsl/cable to set up both a wired local Ethernet network and also as wireless network as per the IEEE 802.11g standard.

Local IP address

See Private IP address

MAC address

Media Access Control

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

Mbps

Million bits per second

Specification of the transmission speed in a network.

MRU

Maximum Receive Unit

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

MTU

Maximum Transmission Unit

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

NAT

Network Address Translation

NAT is a method for implementing IP addresses (mostly Private IP addresses) in a network on one or more Public IP addresses on the Internet. With NAT several network components in a LAN can share the router's public IP address to connect to the Internet. The network components of the local network are hidden behind the router's IP address registered on the Internet. As a result of this security function NAT is frequently used as part of the network Firewall. If you want to make services on a PC on the local network available on the Internet despite NAT, you can configure the Gigaset Appl 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 Appl directs data packets from the Internet that are addressed to a particular Port to the corresponding port of the appropriate network component. This enables servers on the local network to offer services on the Internet without them needing a Public IP address.

See also: Virtual server

PPPoE

Point-to-Point Protocol over Ethernet

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

PPTP

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

Private IP address

The private IP address is 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 Appl, 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 Appl, have a public and a Private IP address.

Re-key Interval

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

Remote Management

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

Roaming

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

Router

A router directs data packages from one local network (LAN) to another via the fastest route. A Router permits the connecting of network with different network technologies. For example, it can link a local network with Ethernet or WLAN technology to the Internet.

See also: Bridge, Switch, Hub, Gateway

Server

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

SMTP

Simple Mail Transfer Protocol

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

SSID

Service Set Identifier

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

Static IP address

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

Subnet mask

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

The subnet mask administered by the Gigaset Appl 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 form the basis for every PC-to-PC connection. TCP provides applications with a reliable transmission link in the form of a continuous data stream. TCP/IP is the basis on which services such as WWW, Mail and News are built. There are other protocols as well.

Tunneling

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

UDP

User Datagram Protocol

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

UPnP

Universal Plug and Play

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

URL

Universal Resource Locator

Globally unique address of a Domain on the Internet.

Virtual server

A virtual Server provides a service on the Internet that runs not on itself but another network component. The Gigaset Appl 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 Appl complies with Standard 802.11g.

WPA

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

WPA-PSK

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

Index

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

Siemens Aktiengesellschaft
www.siemens-mobile.com/gigaset

No.: A31008-E105-B103-2-7619