

Home Networking

A Practical Guide

By

Kevin Svec

ASCLi Group Member

February 2007

Home Networking – A Practical Guide

Introduction

It seems like most everyone is moving into the 21st century. Owning a computer was just the start. Then we added dial-up Internet service which allowed us to surf the web, and share emails. And, not too long ago, high-speed Internet hit the scene in an affordable fashion. Now, we want that super fast download of our favorite video from YouTube.

Not long after installing your high-speed connection, your significant other, son, daughter or your other computer wants to share that connection. Seems easy enough, doesn't it? Or, is it just a pipe dream? Let's listen to what the geek said at BestBuy or Fry's Electronics...

First, will you want to connect your laptop wirelessly? If so, then you will need to purchase either a Linksys or Netgear wireless router. Oh, does your laptop have 802.11b or g? You know, it might be just as well for you to get the new Netgear 54g Turbo router. That way you will be just one step ahead of the game. Unless of course, you wish to live on the bleeding-edge...Then you will need to get the Belkin Pre-N wireless router. Your speeds will be really fast, and you can extend the distance between your laptop and your router. Well, since you decided on the lower model, the WRTG-54 wireless router by Linksys, I only have one more question. Will you be connecting any other computers to this unit? If so, then do you require any Ethernet cards or cables for your other computers?

So you begin to think that this must be pretty since this kid is just spewing out information like water. You inform him that you believe your other computers have connections for connecting to a network, and that you will only need a couple of cables. The geek helps you gather all the necessary equipment & cables. His next comment is the kicker..." Well sir, just take your time, read the quick start guides and hook up your computers to your new network." Read the quick start guides, you say to yourself. That seems simple enough; and you head home with your bag of goodies.

Now you get home, tear everything open, look at the quick start guide and think, now what? Maybe I'll call my buddy Bob who seems to know everything about computers. He must know something about this contraption!

Another possible scenario might be that you do follow the directions, get more confused, spend hours connecting and disconnecting and connecting once more until you finally get it all to work. You obviously did something right; your computers are connected to the Internet. But there is one question lurking...Am I protected from the outside world?

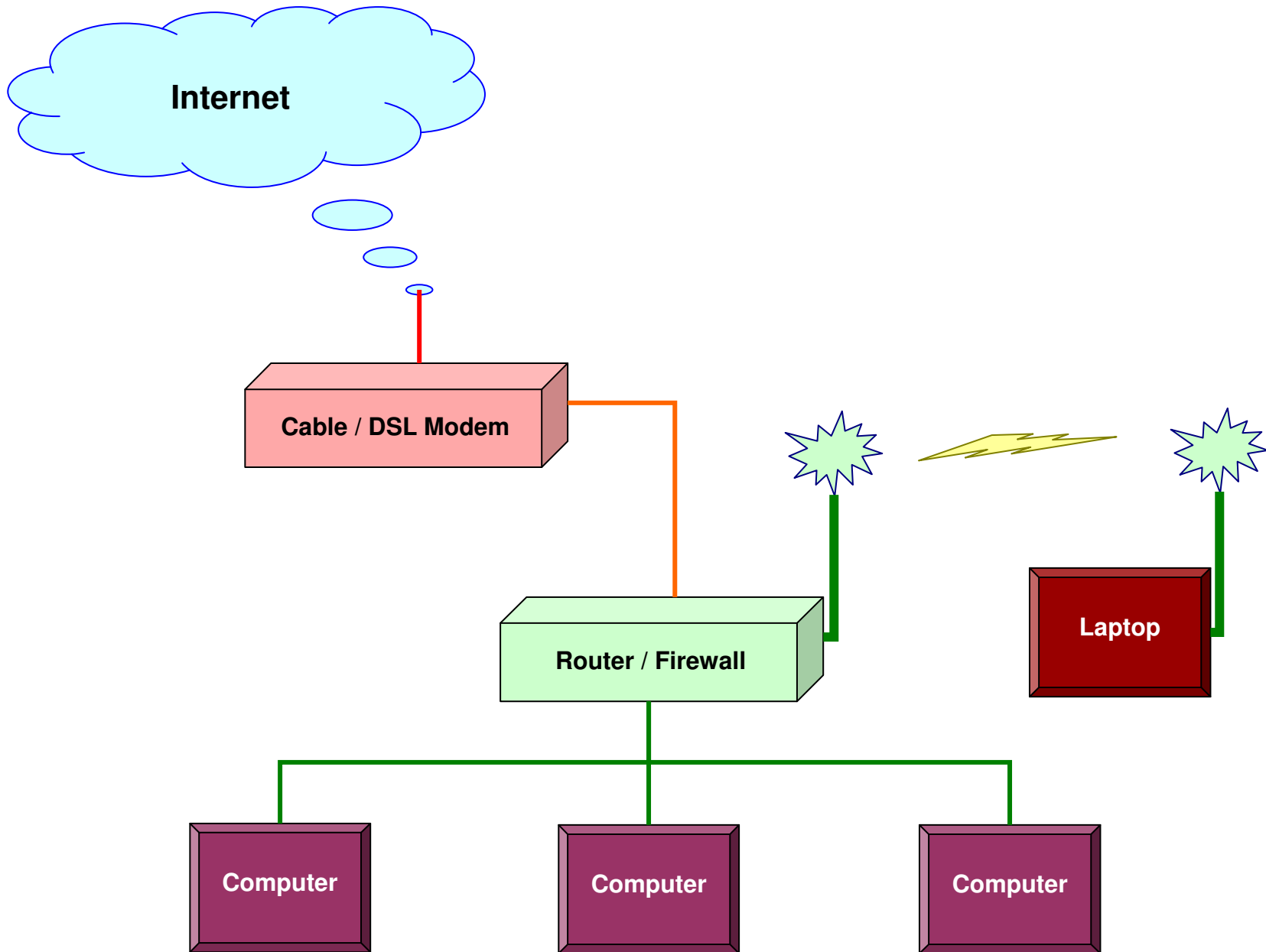
A Typical Network

Most Internet service providers include your high speed modem with the service contract. The majority of these modems are single computer connections, while a few others, mostly DSL providers, will include a multi-computer router. It is important to understand that you should not trust your ISP's modem/router to protect your computer from any outside intruders. It is your responsibility to protect yourself from these dangers. A second router/firewall should be installed between your high speed modem and your internal network or computer. On the next page, you will find a diagram of a typical Internet connection and home network. (See diagram A)

This typical network has a high speed modem, a wireless router/firewall and a group of computers sharing the one Internet connection. Other possibilities do exist for inter-connecting the computers for file sharing or even printer sharing. More sophisticated home networks now include wired/wireless connections to multi-media units for audio, video or Internet access for component services (TiVo is one good example.) Since router pricing is coming down to all-time lows, it is best to purchase a unit that will grow with technology for at least five years. See the chart below for a list of wireless technologies.

Protocol	Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)	Range (Outdoor)
Legacy	1997	2.4-2.5 GHz	1 Mbit/s	2 Mbit/s	?	?
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	25 Mbit/s	54 Mbit/s	~25 meters	~75 meters
802.11b	1999	2.4-2.5 GHz	6.5 Mbit/s	11 Mbit/s	~35 meters	~100 meters
802.11g	2003	2.4-2.5 GHz	25 Mbit/s	54 Mbit/s	~25 meters	~75 meters
802.11n	2007 (unapproved draft)	2.4 GHz or 5 GHz bands	200 Mbit/s	540 Mbit/s	~50 meters	~125 meters

Diagram A



It might seem like 802.11n might be the way to go, but it is not. This standard has yet to be ratified by the IEEE consortium. The estimated effective date is not until May 2009. As such, none of the router manufacturer's units like to "play nice" together. You must match all your equipment, and maintain vigilant firmware updates on your equipment to in order to keep pace and stay secure. A good, solid recommendation would be to purchase a 802.11g router. Some of these routers have a turbo mode which can burst wireless download speeds up to 108 Mbps, although not sustained. If you decide on the turbo models, it is best to match your router and wireless adapters. The purpose of this document is not to get you confused, but rather have a greater understanding of the basic principals of home networking.

Router Setup

Once you have all the necessary components to build your home network, it is time to do a little reading and necessary planning. Read those quick start guides and user guides for all your equipment. It is easier to read the information first and not be as intimidated with the equipment, than to dive in and become frustrated and wanting to pack everything back into its original boxes for return.

Most quick start guides are the same for routers. There are a couple of simple connections, the power connector, the WAN port and one or more LAN ports. WAN is an acronym for Wide Area Network. The WAN is your connection to the Internet. LAN is an acronym for Local Area Network. The LAN is what you are trying to create. Each of your computers will connect to one of the LAN ports with a cable or wirelessly. In the past, it was necessary to have a special cable to connect your high speed modem to the WAN port on the router. Almost all modern routers have auto sensing WAN ports to allow for standard "straight" or inter-connecting "cross-over" cables. Either type of cable will work for your inter-connection between the router and the modem. However, you will only require standard "straight" cables for the connections between your router and computers.

After you have completed your wired connections, it is time to power on the router/firewall for configuration settings. The router will come pre-configured from the factory, and it is highly recommended that you modify all security settings for the router to help ensure a safe and secure LAN. Without attempting to explain all router configurations, below is a general list of settings that should help assist with the basic network setup.

- **Know the IP Address Assignment by Your ISP's Modem**

Most standard ISP modems deliver what is known as a Dynamic IP Address. If your modem utilizes this feature, then you will not need to make any modifications for your WAN connection's IP address. If your modem utilizes Static IP Addressing, then you will need to know the IP Address, DNS IP Address and Gateway for your modem. Refer to your ISP's documentation for this part of the configuration.

- **Determine Your Internal IP Address Schema**

Typical home networks will utilize either the 192.168.0.x or 192.168.1.x schemas. There are others, and your router may already have one selected. For typical home networks, using the pre-defined router default will be sufficient.

- **Dynamic (DHCP) or Static IP Address Assignments**

It is highly recommended that you utilize DHCP for your home network. It will require less configuration time, and will keep address conflicts to a minimum. Static IP address assignments are mainly used on more complex configurations for advanced users.

- **Wireless Network Name (SSID)**

The router will have a default SSID configured. Changing the name will help reduce your security risk, but only slightly. Also, do not utilize a name that may give away your personal identity. A good SSID is one that is vague ("home" or "homewireless") or very unique ("iBhiding" or "l3av3m3al0n3") in nature. Only you will need to know.

- **Broadcast SSID**

It is best to turn this off. It will not completely mask your identity, but it will help reduce your exposure. Keep in mind, you will not be able to locate your home network by traditional means of "finding a wireless network in my area".

- **Wireless Security (WEP, WPA, WPA-PSK, WPA-2)**

Old standards would dictate that you utilize WEP at this point. However, **WEP** (Wired Equivalent Privacy) can be easily broken if you do not change the WEP key on a regular basis. WEP keys are typically 13 (64 bit) or 26 (128 bit) hexadecimal characters in length. Be sure you write this key down on paper somewhere, as it will be necessary for connecting any wireless computers to your router.

WPA (WiFi Protected Access) is more robust, and simpler to maintain.

WPA-PSK (WiFi Protected Access – Pre-Shared Key) has the same benefits of WPA, but now you utilize a pass-phrase key for increasing the security encryption lock.

WPA-2 is a second level WPA protocol. This protocol is slightly more secure than the previous two.

- **Username and Password**

Be sure to change both of these items. If you don't, and someone breaks into your router from outside, they can make changes to your system, and possibly open your LAN to further attacks. Utilize something unique and strong, but write it down along with all your other configuration settings.

Computer Setup

Now that you have completed your setup on the router, let's talk about the configurations on each of your computers. The wired connection will be the simplest to configure. (The configuration discussion to follow is based on a typical computer running Windows XP.) Providing the network connection has not been disabled, Windows will automatically configure the network.

It may be necessary to check the configuration once you have completed the cable connection. This is done by clicking on "Start/Run". Type "CMD" and press "Enter" or click "OK". A command prompt will appear. Now type "IPCONFIG /ALL". A listing of current network settings will appear. You should notice an address of "192.168.0.100" or something similar. (The address depends on the router's configuration for the LAN.) The Gateway and DNS settings should read the same "192.168.0.1". (Again, this depends on the router's configuration.) Two simple tests can be performed to verify the connection. First try to PING your router. Type "PING 192.168.0.1" and press "Enter". You should receive a response. Now type "PING google.com" and press "Enter". You should receive a response.

The first PING command will test the connection between your computer and the router. The second PING command will test the connection between your computer and the Internet.

If you received proper responses from these tests, you can close the CMD window. Now try to open your browser and go to a website.

Sharing Files and Printers

This next section will assist you with sharing files and printers between your different computers. File sharing was the original reason why most people networked their computers. How nice it is to transfer files from one computer to another. Or to have one computer with large amounts of HD space and be able to utilize that storage from computers that do not have the space. This method also allows for a single instance of a file instead of copying that file to every computer, especially with very large multi-media files.

This next section is an excerpt from Microsoft's Q article 304040, which you can access at <http://support.microsoft.com/kb/304040>.

SUMMARY

With Microsoft Windows XP, you can share files and documents with other users on your computer and with other users on a network. There is a new user interface (UI) named Simple File Sharing and a new Shared Documents feature. This article describes the new file sharing UI and discusses the following topics:

- *How to turn Simple File Sharing on and off.*
- *How to manage and configure levels of access to shares and files.*
- *Guidelines for file sharing in Windows XP.*
- *How to troubleshoot file sharing problems.*

Windows XP Home Edition-based computers always have Simple File Sharing enabled.

INTRODUCTION

On a Windows XP-based computer, you can share files among both local and remote users. Local users log on to your computer directly through their own accounts or through a Guest account. Remote users connect to your computer over the network and access the files that are shared on your computer.

You can access the Simple File Sharing UI by viewing a folder's properties. Through the Simple File Sharing UI, you can configure both share and NTFS file system permissions at the folder level. These permissions apply to the folder, all the files in that folder, child folders, and all the files in the child folders. Files and folders that are created in or copied to a folder inherit the permissions that are defined for their parent folder. This article describes how to configure access to your files based on permission levels. Some of the information that this article contains about these permission levels is not documented in the operating system files or the Help file.

MORE INFORMATION

With file sharing in Windows XP, you can configure five levels of permissions. Level 1 is the most private and secure setting, and Level 5 is the most public and changeable (non-secure) setting. You can configure Levels 1, 2, 4, and 5 by using the Simple File Sharing UI. To do this, right-click the folder, and then click **Sharing and Security** to open the Simple File Sharing UI. To configure Level 3, copy a file or folder into the Shared Documents folder under **My Computer**. This configuration does not change when you turn on or turn off Simple File Sharing.

Turning on and turning off Simple File Sharing

Simple File Sharing is always turned on in Windows XP Home Edition-based computers. By default, the Simple File Sharing UI is turned on in Windows XP Professional-based computers that are joined to a workgroup. Windows XP Professional-based computers that are joined to a domain use only the classic file sharing and security interface. When you use the Simple File Sharing UI (that is located in the folder's properties), both share and file permissions are configured.

If you turn off Simple File Sharing, you have more control over the permissions to individual users. However, you must have advanced knowledge of NTFS and share permissions to help keep your folders and files more secure. If you turn off Simple File Sharing, the Shared Documents feature is not turned off.

To turn Simple File Sharing on or off in Windows XP Professional, follow these steps:

1. Double-click **My Computer** on the desktop.
2. On the **Tools** menu, click **Folder Options**.
3. Click the **View** tab, and then select the **Use Simple File Sharing (Recommended)** check box to turn on Simple File Sharing. (Clear this check box to turn off this feature.)

Managing levels of access to shares and to files

You can use Simple File Sharing to configure five different levels of access to shares and files:

- **Level 1:** My Documents (Private)
- **Level 2:** My Documents (Default)
- **Level 3:** Files in shared documents available to local users
- **Level 4:** Shared Files on the Network (Readable by Everyone)
- **Level 5:** Shared Files on the Network (Readable and Writable by Everyone)

NOTES

- By default, files that are stored in My Documents are at Level 2.
- Levels 1, 2, and 3 folders are available only to a user who is logging on locally. Users who log on locally include a user who logs on to a Windows XP Professional-based computer from a Remote Desktop (RDP) session.
- Levels 4 and 5 folders are available to users who log on locally and remote users from the network.

The following table describes the permissions:

Access Level	Everyone (NTFS/File)	Owner	System	Administrators	Everyone (Share)
Level 1	n/a	Full Control	Full Control	n/a	n/a
Level 2	n/a	Full Control	Full Control	Full Control	n/a
Level 3	Read	Full Control	Full Control	Full Control	n/a
Level 4	Read	Full Control	Full Control	Full Control	Read
Level 5	Change	Full Control	Full Control	Full Control	Full Control

Level 1: My Documents (Private)

The owner of the file or folder has read and write permission to the file or folder. Nobody else may read or write to the folder or the files in it. All subfolders that are contained in a folder that is marked as private remain private unless you change the parent folder permissions.

If you are a Computer Administrator and create a user password for your account by using the User Accounts Control Panel tool, you are prompted to make your files and folder private.

Note The option to make a folder private (Level 1) is only available to a user account in its own My Documents folder.

To configure a folder and all the files in it to Level 1, follow these steps:

1. Right-click the folder, and then click **Sharing and Security**.

2. Select the **Make this Folder Private** check box, and then click **OK**.

Local NTFS Permissions:

- Owner: Full Control
- System: Full Control

Network Share Permissions:

- Not Shared

Level 2 (Default): My Documents (Default)

The owner of the file or folder and local Computer Administrators have read and write permission to the file or folder. Nobody else may read or write to the folder or the files in it. This is the default setting for all the folders and files in each user's My Documents folder.

To configure a folder and all the files in it to Level 2, follow these steps:

1. Right-click the folder, and then click **Sharing and Security**.
2. Make sure that both the **Make this Folder Private** and the **Share this folder on the network** check boxes are cleared, and then click **OK**.

Local NTFS Permissions:

- Owner: Full Control
- Administrators: Full Control
- System: Full Control

Network Share Permissions:

- Not Shared

Level 3: Files in shared documents available to local users

Files are shared with users who log on to the computer locally. Local Computer Administrators can read, write, and delete the files in the Shared Documents folder. Restricted Users can only read the files in the Shared Documents folder. In Windows XP Professional, Power Users may also read, write, or delete any files in the Shared Documents Folder. The Power Users group is only available in Windows XP Professional. Remote users cannot access folders or files at Level 3. To permit remote users to access files, you must share them out on the network (Level 4 or 5).

To configure a file or a folder and all the files in it to Level 3, start Microsoft Windows Explorer, and then copy or move the file or folder to the Shared Documents folder under My Computer.

Local NTFS Permissions:

- Owner: Full Control
- Administrators: Full Control
- Power Users: Change
- Restricted Users: Read
- System: Full Control

Network Share Permissions:

- Not Shared

Level 4: Shared on the Network (Read Only)

Files are shared for everyone to read on the network. All local users, including the Guest account, can read the files, but they cannot modify the contents. Any user can read and change your files.

To configure a folder and all the files in it to Level 4, follow these steps:

1. Right-click the folder, and then click **Sharing and Security**.
2. Click to select the **Share this folder on the network** check box
3. Click to clear the **Allow network users to change my files** check box, and then click **OK**.

Local NTFS Permissions:

- Owner: Full Control
- Administrators: Full Control

- System: Full Control
- Everyone: Read

Network Share Permissions:

- Everyone: Read

Level 5: Shared on the network (Read and Write)

This level is the most available and least secure access level. Any user (local or remote) can read, write, change, or delete a file in a folder shared at this access level. Microsoft recommends that this level be used only for a closed network that has a firewall configured. All local users including the Guest account can also read and modify the files.

To configure a folder and all the files in it to Level 5, follow these steps:

1. Right-click the folder, and then click **Sharing and Security**
2. Click to select the **Share this folder on the network** check box, and then click **OK**.

Local NTFS Permissions:

- Owner: Full Control
- Administrators: Full Control
- System: Full Control
- Everyone: Change

Network Share Permissions:

- Everyone: Full Control

Note All NTFS permissions that refer to Everyone include the Guest account.

All the levels that this article describes are mutually exclusive. Private folders (Level 1) cannot be shared unless they are no longer private. Shared folders (Level 4 and 5) cannot be made private until they are unshared.

If you create a folder in the Shared Documents folder (Level 3), share it on the network, and then permit network users to change your files (Level 5), the permissions for Level 5 are effective for the folder, the files in that folder, and the child folders. The other files and folders in the Shared Documents folder remain configured at Level 3.

Note The only exception is if you have a folder (*SampleSubFolder*) that is shared at Level 4 inside a folder (*SampleFolder*) that is shared at Level 5. Remote users have the correct access level to each of the shared folders. Locally logged-on users have writable (Level 5) permissions to the parent (*SampleFolder*) and child (*SampleSubFolder*) folders.

Guidelines

Microsoft recommends that you only share folders on the network that remote users on other computers must access. Microsoft recommends that you do not share the root of your system drive. When you do this your computer is more vulnerable to malicious remote users. The **Sharing** tab of the drive's **Properties** dialog box contains a warning when you try to share a root folder (for example, C:\). To continue, you must click the **If you understand the risk but still want to share the root of the drive, click here** link. Only computer administrators can share the root of the drive.

Files on a read-only device such as a CD-ROM shared at Level 4 or 5 are only available if the CD-ROM is in the CD-ROM drive. Any CD-ROM that is in the CD-ROM drive is available to all users on the network.

A file's permission may differ from the containing folder if one of the following conditions is true:

- You use the **move** command at a command prompt to move a file into the folder from a folder on the same drive that has different permissions.
- You use a script to move the file into the folder from a folder on the same drive that has different permissions.
- You run Cacls.exe at a command prompt or a script to change file permissions.
- Files existed on the hard disk before you installed Windows XP.
- You changed a file's permissions while Simple File Sharing was turned off on Windows XP Professional.

Note NTFS permissions are not maintained on file move operations when you use Windows Explorer with Simple File Sharing turned on.

If you turn on and turn off Simple File Sharing, the permissions on files are not changed. The NTFS and share permissions do not change until you change the permissions in the interface. If you set the permissions with Simple File Sharing enabled, only Access Control Entries (ACEs) on files that are used for Simple File Sharing are affected. The following ACEs in the Access Control List (ACL) of the files or folders are affected by the Simple File Sharing interface:

- Owner
- Administrators
- Everyone
- System

Behavior that is affected when Simple File Sharing is turned on

- The Simple File Sharing UI in the properties of a folder configures both share and file permissions.
- Remote users always authenticate as the Guest account.

For additional information, click the following article number to view the article in the Microsoft Knowledge Base:

[302927](#) Computer Management displays user account names when logged on as Guest

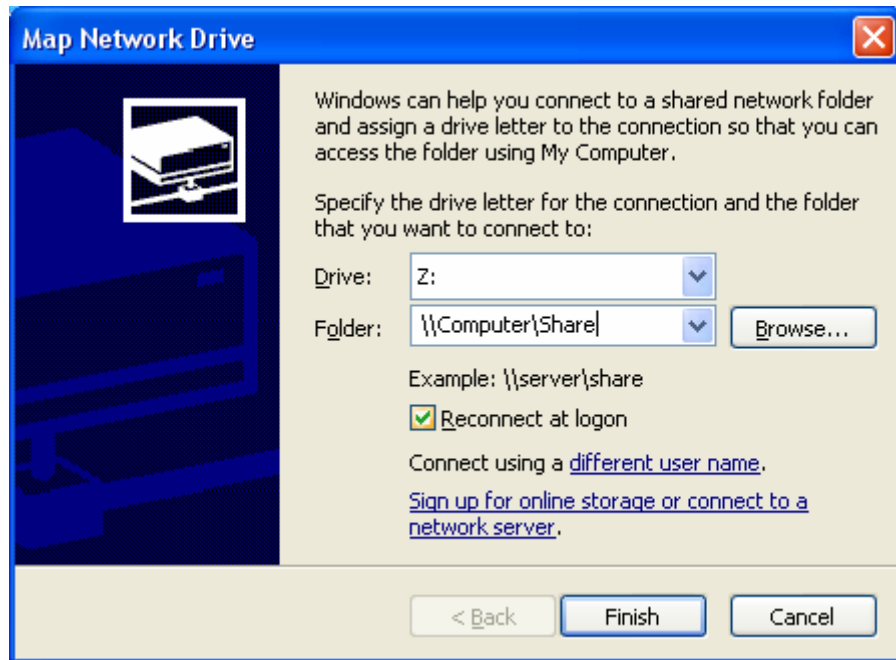
- Windows Explorer does not retain permissions on files that are moved in the same NTFS drive. The permissions are always inherited from the parent folder.
- On Windows XP Professional-based computers that have Simple File Sharing turned on and Windows XP Home Edition-based computers, the Shared Folders (Fsmgmt.msc) and Computer Management (Compmgmt.msc) tools reflect a simpler sharing and security UI.
- In the Computer Management and Shared Folders consoles, the **New File Share** command is unavailable when you right-click the **Shares** icon. Also, if you right-click any listed share, the **Properties** and **Stop Share** commands are unavailable.

Behavior that is not caused by turning on Simple File Sharing

- In Windows XP Home Edition, the Computer Management snap-in does not display the **Local Users and Groups** node. The Local Users and Groups snap-in cannot be added to a custom snap-in. This behavior is a limitation of Windows XP Home Edition. It is not caused by Simple File Sharing.
- If you turn off the Guest account in the **User Accounts** Control Panel tool, only the guest's ability to log on locally is affected. The account is not disabled.
- Remote users cannot authenticate by using an account that has a blank password. This authentication is configured separately.
- Windows XP Home Edition cannot join a domain. It can only be configured as a member of a workgroup.

Connecting to your shared files from the other computers doesn't need to be difficult. From My Computer or Windows File Explorer, browse "My Network Places" to locate the host computer. You will need to locate the computer through either your Workgroup computers (From My Computer) or through the Entire Network (File Explorer). Once you locate the computer, continue to browse down the tree to locate the shared folder.

This shared folder can be converted to a drive letter to make things simpler by right-clicking on the shared folder and selecting "Map Network Drive". Below is an example of the "Map Network Drive" dialog box.



Choosing "Reconnect at logon" will connect this shared folder back to the drive letter that you specify here. This is very helpful for the need of persistent connections. (I.e. Your multi-media folder from which you listen to music every day.) Select the drive letter you wish to map and click "Finish". You can now access that share from the mapped drive letter within any application.

Sharing your printer(s) is much simpler. Windows XP has made printer sharing as simple as clicking one button. You'll need to open your printers and faxes dialog box. Click Start/Printers and Faxes. You can either highlight the printer you wish to share and select "Share This Printer" on the left, or right-click on the printer you wish to share and select "Sharing...". Both will lead to the sharing dialog box where you click the radio button "Share this printer". A share name will be automatically filled into the text box. You can either accept this name or change it to your liking. Once you are satisfied with a name, click "OK" at the bottom of the dialog box. Your printer is now shared.

Setup this shared printer on the other computers by adding a new printer. Choose "Network Printer" and browse for the shared printer on the network. (See Diagram B) on the next page.

Diagram B

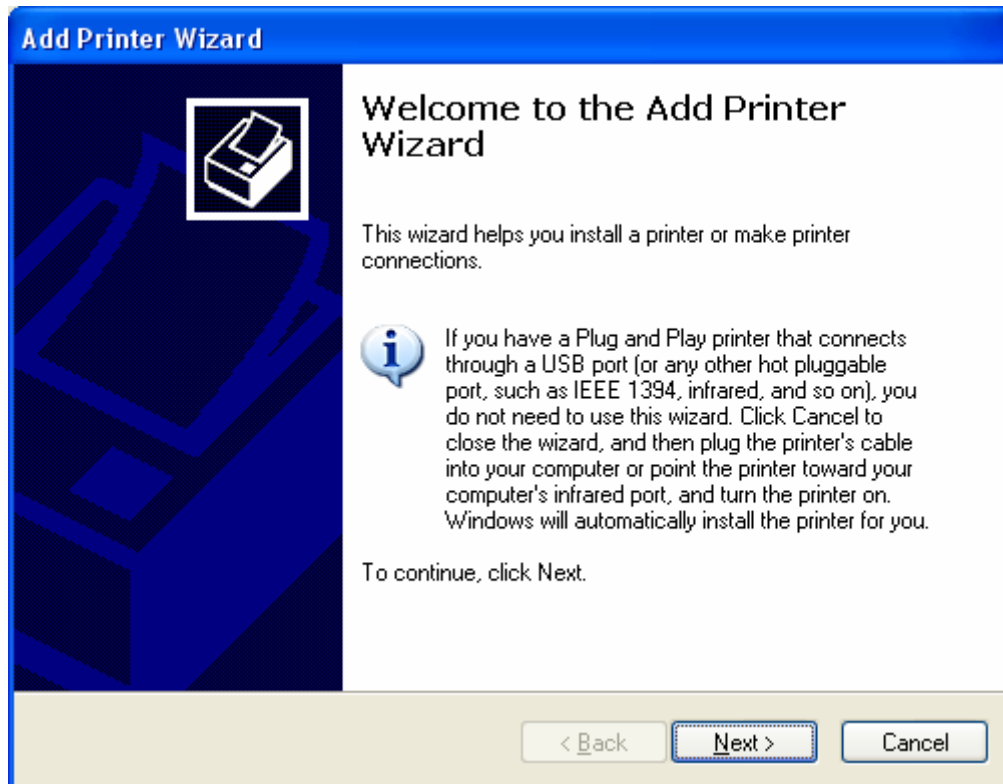
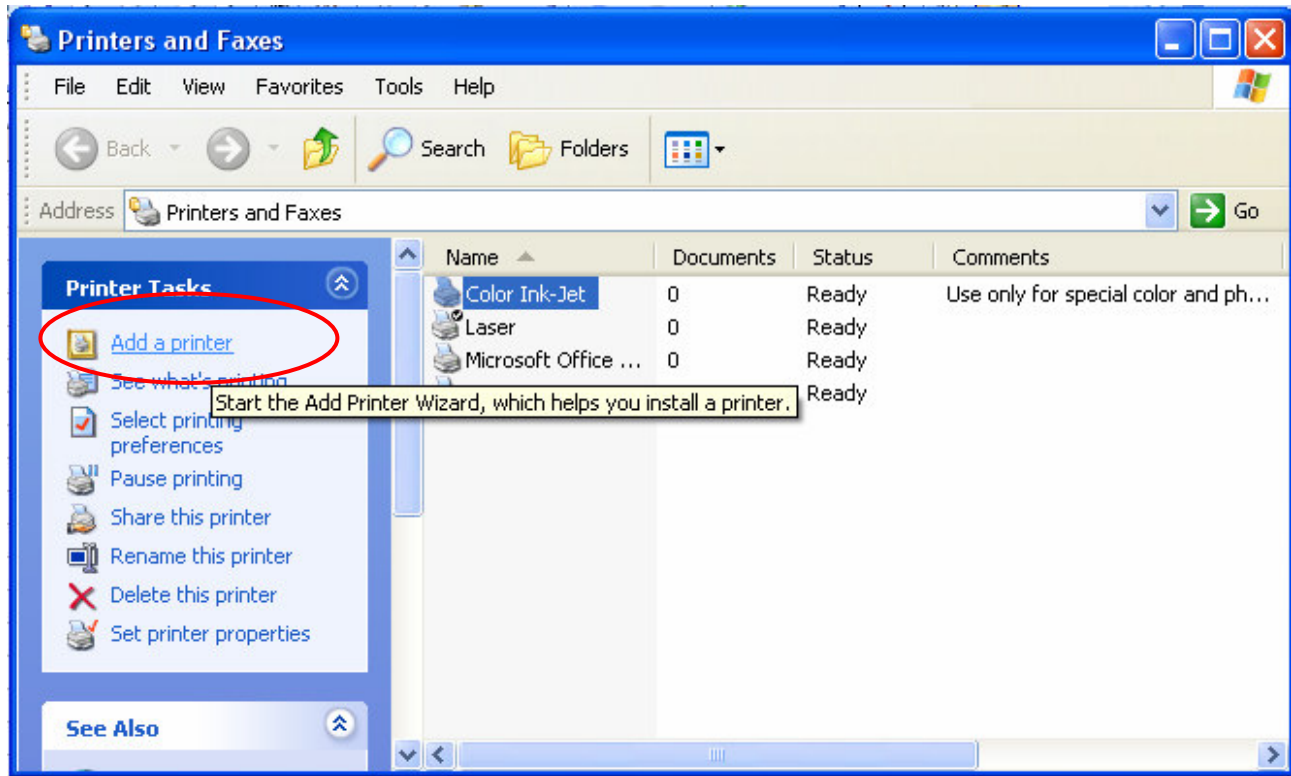


Diagram B

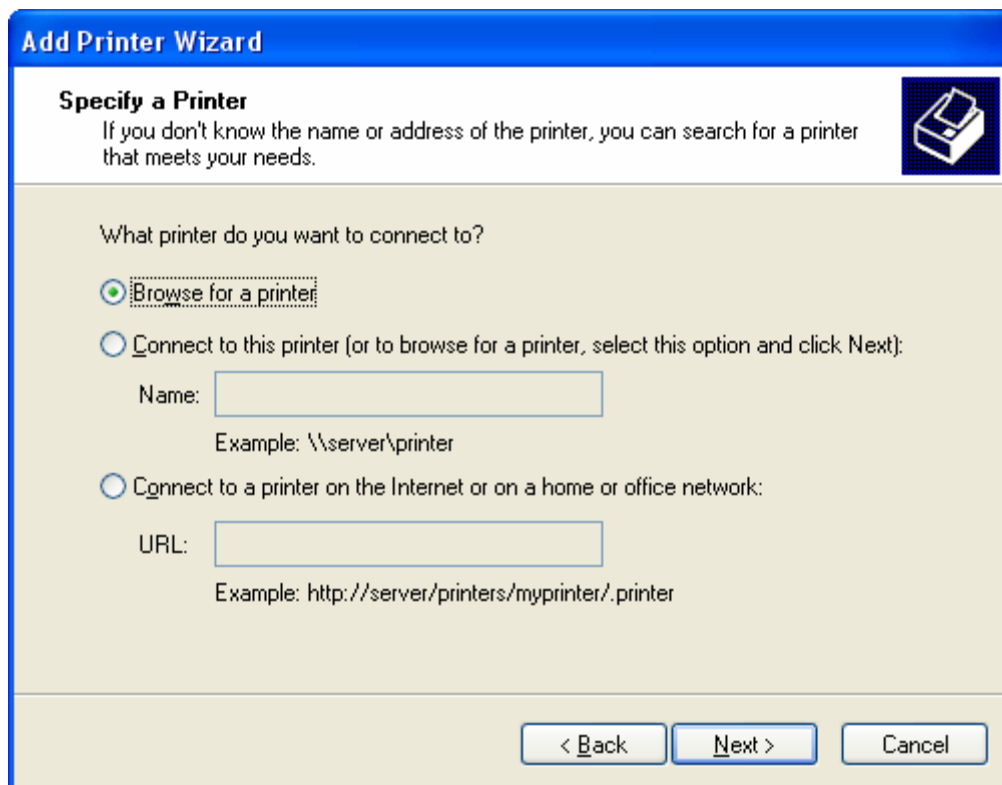
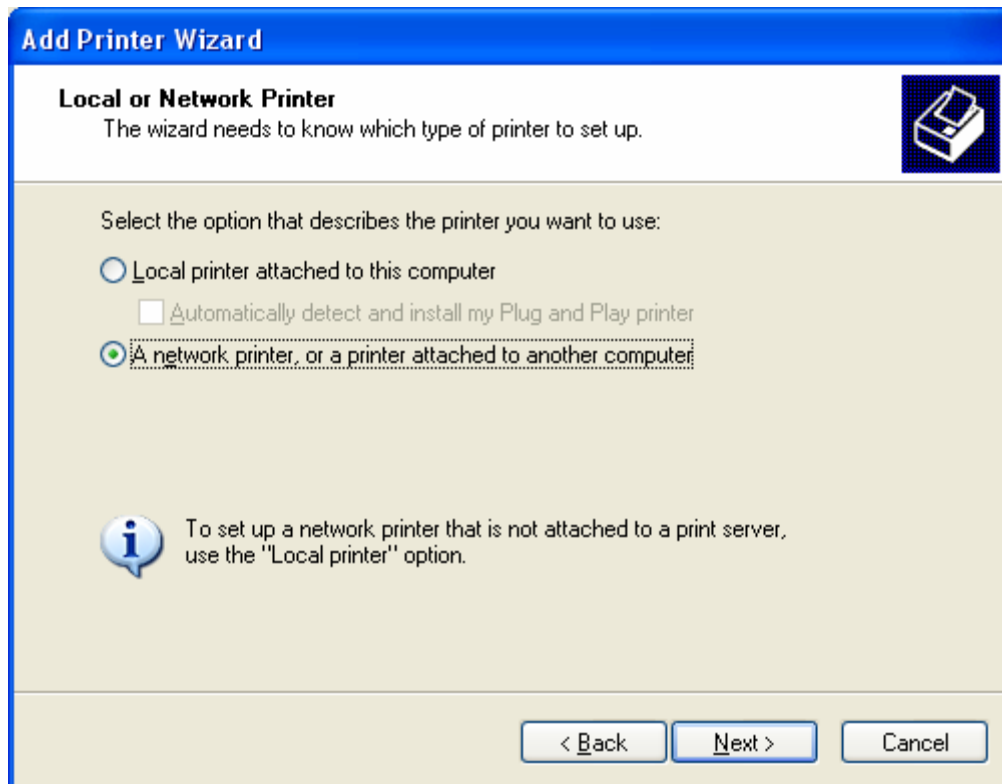
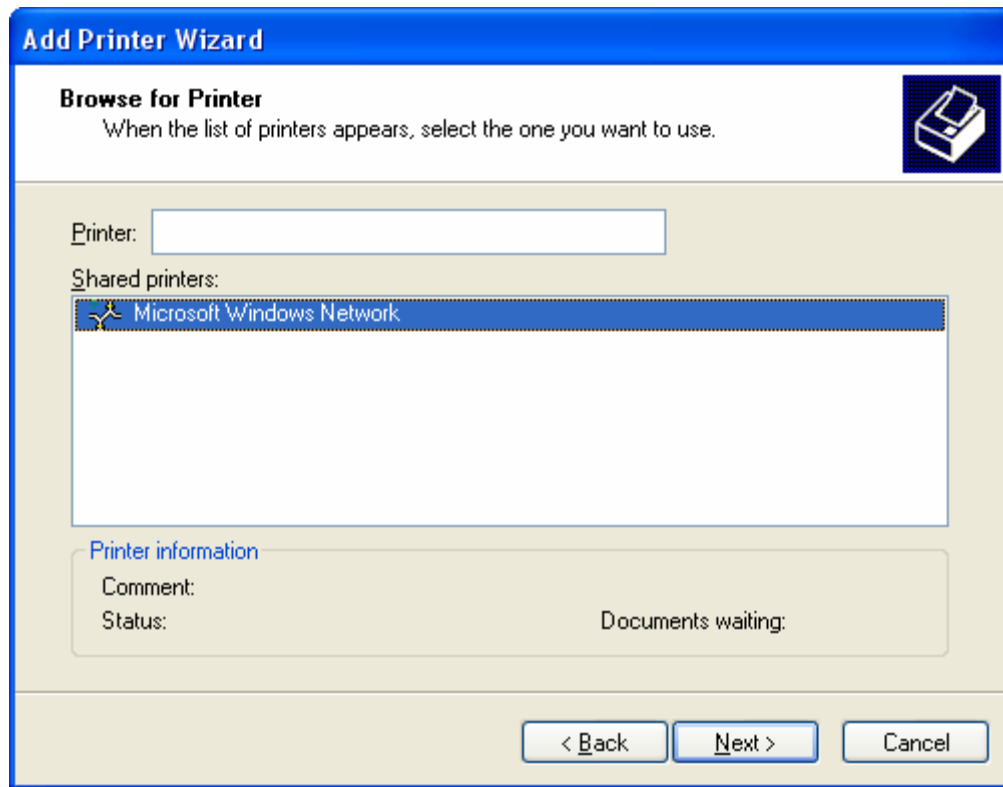


Diagram B



Locate the printer on the network and highlight that printer. Click Next. The final dialog boxes will complete the printer installation.

Glossary

- **Access Point**

Provides a bridge between Ethernet wired LANs and the wireless network. Access Points are the connectivity point between Ethernet wired networks and devices equipped with a wireless LAN adapter card.

- **Ad-Hoc**

A network framework provided by IEEE 802.11 standard set in which all communications between wireless clients are made without the use of an Access Point (AP). This mode sometimes is referred as a peer-to-peer mode.

- **Firewall**

A firewall is a hardware or software solution to enforce security policies. In the physical security analogy, a firewall is equivalent to a door lock on a perimeter door or on a door to a room inside of the building - it permits only authorized users such as those with a key or access card to enter. A firewall has built-in filters that can disallow unauthorized or potentially dangerous material from entering the system. It also logs attempted intrusions.

- **IP Address**

(Internet Protocol Address) This is a series of numbers separated by decimals to indicate a particular unique address for a computer, router, switch or other network capable device. Each of the series, known as Octets, will range from 1 to 254. There are four octets per address.

- **Router**

A device that determines the next network point to which a data packet should be forwarded enroute toward its destination. The router is connected to at least two networks and determines which way to send each data packet based on its current understanding of the state of the networks it is connected to. Routers create or maintain a table of the available routes and use this information to determine the best route for a given data packet.

- **SSID**

SSID is an acronym for Service Set Identifier. The SSID is a sequence of up to 32 letters or numbers that is the ID, or name, of a wireless local area network. The SSID is set by a network administrator and for open wireless networks; the SSID is broadcast to all wireless devices within range of the network access point. A closed wireless network does not broadcast the SSID, requiring users to know the SSID to access the network.