

Networking Technologies



Networking

Sr. No.	Particulars	Page No's
1.	Cabling & Crimping of Network	1
2.	Installing Windows 98	9
3.	Installing Windows 7	25
4.	Installing Windows Server 2008	35
5.	Basics of Networking	45
6.	Control Panel & Sub Options	55
7.	IP Addressing & Implementation	67
8.	Configuring LAN Network	91
9.	DNS, Active Directory Services Configuration	110
10.	Remote Connectivity & Drive Mapping	133
11.	Print Management	151
12.	Backup & Restore	165
13.	Transmission Media (Cable)	168
14.	Networking Topologies	179
15.	Networking Devices	191
16.	OSI Reference Model	204
17.	Network Protocols	216
18.	Troubleshooting LAN Network	223

Wireless LAN (Wi-Fi)

19.	Introduction to Wireless technology	255
20.	Wireless LAN Topologies	261
21.	Radio Frequency (RF)	274
22.	IEEE 802.11 Standards	289
23.	802.11 Network Security Architecture	292
24.	Wi-Fi Network Configuration	301
25.	Troubleshooting WLAN	325

Practical Session

Sr. No.	Practical Session	Lecture No.	Page No
1	Crimping of Cables	Lec. 1	333
2	Client/Server Configuration	Lec. 11	334
3	Different type of Remote Management Tools	Lec. 12	337
4	Network Troubleshooting	Lec. 21	339
5	Configuring Access Point	Lec. 25	341

Chapter - 1

Cablling & Crimping

Network Cabling

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following sections discuss the types of cables used in networks and other related topics.

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable
- Cable Installation Guides
- Wireless LANs

twisted-pair Cable

Twisted-pair cable is a type of cabling that is used for telephone communications and most modern Ethernet networks. A pair of wires forms a circuit that can transmit data. The pairs **are** twisted to provide protection against crosstalk, the noise generated by adjacent pairs. When electrical current flows through a wire, it creates a small, circular magnetic field around the wire. When two wires in an electrical circuit are placed close together, their magnetic fields are the exact opposite of each other. Thus, the two magnetic fields cancel each other out. They also cancel out any outside magnetic fields. Twisting the wires can enhance this cancellation effect. Using cancellation together with twisting the wires, cable designers can effectively provide self-shielding for wire pairs within the network media.

Two basic types of twisted-pair cable exist: unshielded twisted pair (UTP) and shielded twisted pair (STP). The following sections discuss UTP and STP cable in more detail.

Unshielded twisted pair (Utp) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks (See fig. 1).

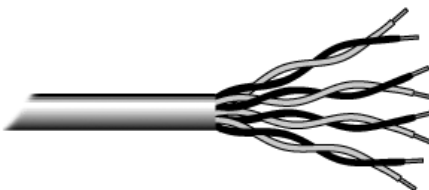


Fig.1. Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire (additional categories are emerging).

Categories of Unshielded twisted pair

Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair) 1000 Mbps (4 pair)	100BaseT Ethernet Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

Unshielded twisted pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.



Fig. 2. RJ-45 connector

Shielded twisted pair (Stp) Cable

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables. Shielded twisted pair cable is available in three different configurations:

1. Each pair of wires is individually shielded with foil.
2. There is a foil or braid shield inside the jacket covering all wires (as a group).
3. There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig. 3). The metal shield helps to block any outside interference from coaxial cable.

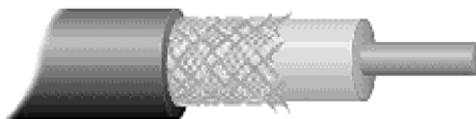


Fig. 3. Coaxial cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial.

- 1) Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters.
- 2) Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See fig. 4). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors

on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather

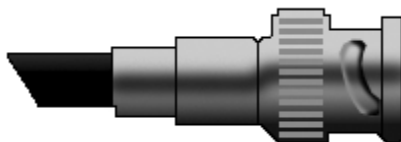


Fig. 4. BNC connector

Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 5). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is The center core of fiber cables is made from glass or plastic fibers (see fig 5). A plastic coating then cushions the fiber center, and kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of teflon or PVC.

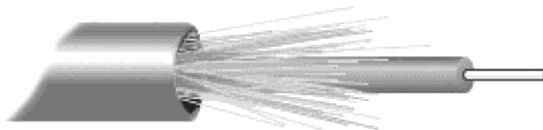


Fig. 5. Fiber optic cable

There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

ethernet Cable Summary

Specification	Cable Type
10Baset	Unshielded Twisted Pair
10Base2	Thin Coaxial
10Base5	Thick Coaxial
100Baset	Unshielded Twisted Pair
100BaseFX	Fiber Optic

100BaseBX	Single mode Fiber
100BaseSX	Multimode Fiber
1000BaseT	Unshielded Twisted Pair
1000BaseFX	Fiber Optic
1000BaseBX	Single mode Fiber
1000BaseSX	Multimode Fiber

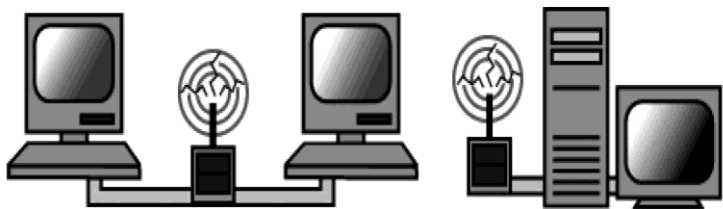
Installing Cable - Some Guidelines

When running cable, it is best to follow a few simple rules:

- Always use more cable than you need. Leave plenty of slack.
- Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.

Wireless LaNs

More and more networks are operating without cables, in the wireless mode. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.



Wireless networks are great for allowing laptop computers or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables. The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-

sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network. Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

Wireless standards and speeds

The Wi-Fi Alliance is a global, non-profit organization that helps to ensure standards and interoperability for wireless networks, and wireless networks are often referred to as WiFi (Wireless Fidelity). The original Wi-Fi standard (IEEE 802.11) was adopted in 1997. Since then many variations have emerged (and will continue to emerge). Wi-Fi networks use the Ethernet protocol.

Standard	Max Speed	typical range
802.11a	54 Mbps	150 feet
802.11b	11 Mbps	300 feet
802.11g	54 Mbps	300 feet

advantages of wireless networks:

Mobility - With a laptop computer or mobile device, access can be available throughout a school, at the mall, on an airplane, etc. More and more businesses are also offering free Wi-Fi access.

Fast setup - If your computer has a wireless adapter, locating a wireless network can be as simple as clicking "Connect to a Network" -- in some cases, you will connect automatically to networks within range.

Cost - Setting up a wireless network can be much more cost effective than buying and installing cables.

expandability - Adding new computers to a wireless network is as easy as turning the computer on (as long as you do not exceed the maximum number of devices).

Disadvantages of wireless networks:

Security - Wireless networks are much more susceptible to unauthorized use. If you set up a wireless network, be sure to include maximum security. You should always enable WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access), which will improve security and help to prevent virtual intruders and freeloaders.

Interference - Because wireless networks use radio signals and similar techniques for transmission, they are susceptible to interference from lights and electronic devices.

Inconsistent connections - how many times you have hears "Wait a minute, I just lost

my connection?” Because of the interference caused by electrical devices and/or items blocking the path of transmission, wireless connections are not nearly as stable as those through a dedicated cable.

power consumption - The wireless transmitter in a laptop requires a significant amount of power; therefore, the battery life of laptops can be adversely impacted. If you are planning a laptop project in your classroom, be sure to have power plugs and/or additional batteries available.

Speed - The transmission speed of wireless networks is improving; however, faster options (such as gigabit Ethernet) are available via cables. In addition, if set up a wireless network at home, and you are connecting to the Internet via a DSL modem (at perhaps 3 Mbps), your wireless access to the Internet will have a maximum of 3 Mbps connection speed.

CRIMPING

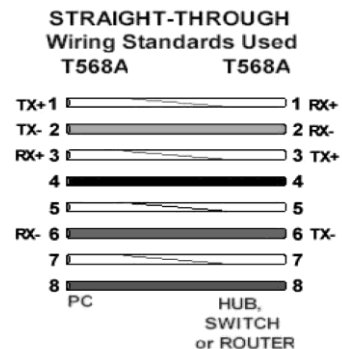
Crimping is a method of firmly attaching a terminal or contact end to an electrical conductor by pressure forming or reshaping a metal barrel, together with the conductor. The forming of a satisfactory crimp depends on the correct combination of conductor, crimp barrel and tool. When applied with a properly matched tool a union would be established which has both good electrical and mechanical characteristics. The tool will provide these requirements consistently and reliably with repeat ability assured by quality cycle controlled tooling. The electrical resistance of a properly designed and controlled crimp joint should be equal to, or less than, the resistance of an equal section of wire. Specifications state the requirements in terms of mill volt drop at a designated current.

The mechanical strength of a crimped joint and hence its pull-out force (tensile strength), varies with the deformation applied. Therefore, by properly shaping the deformation of a high pull-out force can be achieved, i.e. the crimp die of the tool determines the crimp configuration and deformation. The dies in the tool determine the completed crimp configuration which is generally an element of contact and/or connector design. Some of the design considerations are:

- a) The type of contact, its size, shape, material and function,
- b) The type and size of wires to be accommodated,
- c) The type of tooling into which the configuration must be built.

1) **Straight-through Wiring Using the 568a Standard**

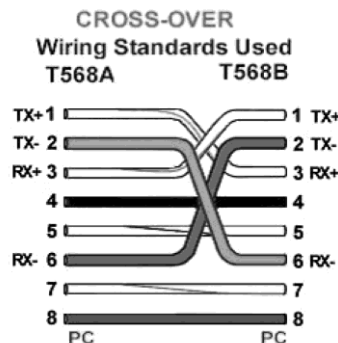
The flat wiring diagram, above, shows the 568A color code standard as the wiring for the PC side of the cable and the same 568A standard for the Hub, Switch or Router side of things (assuming that the Hubs, Switches or Routers are wired internally to perform the cross-over function). The illustration



depicts the wiring arrangement before insertion into an RJ45 connector prior to crimping.

2) **Cross-Over Wiring Using the 568a to 586B Standards**

The flat wiring illustration, above, shows cross-over cable wiring using the 568A color code standard as the wiring for the PC side of things and the 568B standard for wiring to the other PC. Note that in both cases, all eight wires are shown but only four are actually needed. Pins 4, 5, 7, and 8 and the blue and brown pairs are not used in either standard. Contrary to common tech-lore and what you may have read elsewhere, these pins and wires are not used or required to implement 100BASE-TX duplexing. In fact, they can be used for other purposes such as a single line phones or even operating two separate Ethernet channels, provided care is taken to assure that these wire pairs are isolated from the other wires.



In practice, making actual RJ45 Patch cables is not physically that simple. The connections of the pairs to the pins in the RJ45 jack aren't wire pair by wire pair. Instead, the orange pair of wires is not adjacent and the blue pair is upside-down. In fact..Flattening out the cables in the correct order for insertion into the RJ45 jack.

Before crimping is by far the most complex part of the job of making twisted pair Ethernet patch cables. One cannot use flat-untwisted telephone cable for a network cable that runs any appreciable distance. One must use a pair of twisted wires to connect a set of transmitter pins to their corresponding receiver pins. One cannot use a wire from one pair and another wire from a different pair.

Connect the cable with PC end and other one at HUB or Switch or PC to PC as required for checking the connectivity.

Now you will find a connectivity icon in the right side of bottom, next to date & Time "**Local area is connected**".

Chapter – 2

Installing Windows 98

Introduction

Microsoft announced with this new system software Version 4.10 the revised version of Windows 95. The operating system Windows 98 contains as innovation mainly detail improvements and bug fixes. The hardware component is enhanced with USB support improved and the operation of several monitors is possible now. Windows 98 is prepared for DVD movies, For the view of DVD Movies separate software must be installed.

As a file system for the installation of Windows 98 FAT32 is recommended. If the access to other file systems is needed are tools of third party manufacturers required which usually offer free software with read access. Such tools are available for NTFS and the Linux file system ext2. For the professional file system NTFS exists a driver of Sysinternals which is integrated after the installation in the operating system. For the successful installation system files are needed by Windows NT. Windows 98 can be updated to DirectX 9.0 and the Internet Explorer 6.

Features of Windows 98

- Extended support for the connection to networks
- Integrated Internet Explorer 4.0
- web optimized, networking through VPN
- Internet Connection Sharing (ICS)

area of application

- Home user
- PC Games
- Office use
- Network client

System environment

- Minimum Hardware Requirements: 16 Mbyte RAM, 300 Mbyte hard disk storage
- Active Desktop for the Web integration in Windows
- New driver model WDM (Win32 Driver Model), developed for the same driver base for Windows NT and 98 in 1996
- Task planer, time controlled start from programs
- Maintenance assistant, hard disk maintains
- Game interface DirectX 5.0

- Multi monitoring Support (up to 4)
- File system FAT16, better use FAT32, access to NTFS and Linux ext2 file system with 3rd Party tools
- Preemptive multitasking for 32-bit applications
- Cooperative multitasking for 16-bit programs
- ACPI Power save mode partly supported (except of Suspend to Disk)
- X86 CPUs and compatible

Step-by-step on how to perform a Fresh Install of Windows 98. What you are going to need for this:

- 1) Windows 98 CD
- 2) Windows 98 Product ID/Key
- 3) About 1-2 Hours

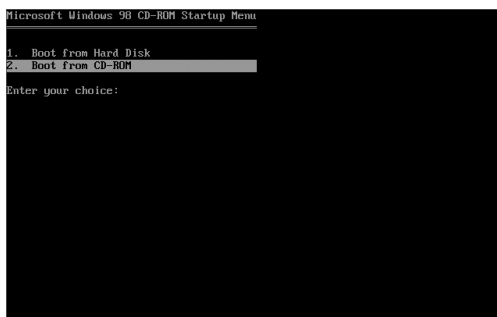
The screen shots on this page are taken from a Windows 98SE OEM install using only the CD, on a unpartitioned Hard Drive. If you already have Windows 98 installed, you can skip to (Step 07) and continue on or skip to (Step 13), to delete the partition and start at (Step 01). If you can't find your Windows 98 Product Key then skip to (Step 14) before doing any of this.

Installing Windows 98

(Step 01)

You need to make sure that you have the BIOS/Startup, so that the CDROM drives boots before the Hard Drive. To do this, you need to enter the BIOS/Startup by pressing: ESC, F1, F2, or DEL. Usually during POST (boot up) there should be something on the bottom stating on how to enter the BIOS/Startup. Press the button that it says to press or try one of the above until you enter BIOS/Startup Menu. Now using the arrow keys, there should be a tab that says, Startup/Boot Order. Under that should be a list with a list of options, make the 1st Boot - Floppy/3.5 Floppy, 2nd Boot - CDROM, 3rd Boot - Hard Drive, 4th Boot - Other. Place the CD in the CDROM Drive, save and exit the BIOS settings.

(Step 02)



After exiting the BIOS the computer will restart. You will get the above screen after the computer finishes POST. Select Boot from CD.

(Step 03)

```
Microsoft Windows 98 Startup Menu
-----
1. Start Windows 98 Setup from CD-ROM.
2. Start computer with CD-ROM support.
3. Start computer without CD-ROM support.

Enter a choice: 3

F5=Safe mode  Shift+F5=Command prompt  Shift+F8=Step-by-step confirmation [N]
```

After selecting Boot from CD the above screen will come up. Select Start computer without CD-ROM support.

(Step 04)

```
A:\>fdisk_
```

When it finishes loading, you will see the above screen with A:\. Type fdisk and then press enter. This is how the screen should look:

a:\fdisk

(Step 05)

```
Your computer has a disk larger than 512 MB. This version of Windows
includes improved support for large disks, resulting in more efficient
use of disk space on large drives, and allowing disks over 2 GB to be
formatted as a single drive.

IMPORTANT: If you enable large disk support and create any new drives on this
disk, you will not be able to access the new drive(s) using other operating
systems, including some versions of Windows 95 and Windows NT, as well as
earlier versions of Windows and MS-DOS. In addition, disk utilities that
were not designed explicitly for the FAT32 file system will not be able
to work with this disk. If you need to access this disk with other operating
systems or older disk utilities, do not enable large drive support.

Do you wish to enable large disk support (Y/N).....? [Y]
```

You will come to the screen above. Press Enter.

```
Microsoft Windows 98
Fixed Disk Setup Program
(C)Copyright Microsoft Corp. 1983 - 1998

FDISK Options

Current fixed disk drive: 1

Choose one of the following:

1. Create DOS partition or Logical DOS Drive
2. Set active partition
3. Delete partition or Logical DOS Drive
4. Display partition information

Enter choice: [1]

Press Esc to exit FDISK
```

After that you will come to this screen, press 1 then Enter.

```
                Create DOS Partition or Logical DOS Drive

Current fixed disk drive: 1

Choose one of the following:

1. Create Primary DOS Partition
2. Create Extended DOS Partition
3. Create Logical DOS Drive(s) in the Extended DOS Partition

Enter choice: [1]

Press Esc to return to FDISK Options
```

You will then come to this screen, press 1 then Enter.

```
                Create Primary DOS Partition

Current fixed disk drive: 1

Do you wish to use the maximum available size for a Primary DOS Partition
and make the partition active (Y/N).....? [Y]

Press Esc to return to FDISK Options
```

Now the program will check the Hard Drive, and then will make the partition. Press Y then Enter.

```


You MUST restart your system for your changes to take effect.
Any drives you have created or changed must be formatted
AFTER you restart.

Shut down Windows before restarting.

Press Esc to exit FDISK.
```

After that is done you will come to this screen, press ESC. You will then come back to the black screen with A:\. Press **Ctrl+alt+Del**. This will restart the computer.

(Step 06)

You will then come back to the Boot Select Screen. Select Boot from CD-ROM.

(Step 07)

```
MSCDEX Version 2.25
Copyright (C) Microsoft Corp. 1986-1995. All rights reserved.
  Drive D: = Driver OEMCD001 unit 0

A:\>D:\WIN98\format C:

WARNING, ALL DATA ON NON-REMOVABLE DISK
DRIVE C: WILL BE LOST!
Proceed with Format (Y/N)?_
```

Select Start computer with CD-ROM support. The computer will now have CDROM support; you will come to the black screen with the A:\. Now type D:\WIN98\format C:

This is how the screen will look:

a:\D:\WIN98\format C:

You will be asked if you want to proceed with the format. Press Y, and then Enter. Depending on the size of the Hard Drive, this may take a while. After it is done formatting, press Enter (Do not enter a label).

(Step 08)

```
WARNING, ALL DATA ON NON-REMOVABLE DISK
DRIVE C: WILL BE LOST!
Proceed with Format (Y/N)?y

Formatting 16,37.73M
Format complete.
Writing out file allocation table
Complete.
Calculating free space (this may take several minutes)...
Complete.

Volume label (11 characters, ENTER for none)?

  16,362.73 MB total disk space
  16,362.73 MB available on disk

    8,192 bytes in each allocation unit.
  2,094,429 allocation units available on disk.

Volume Serial Number is 2541-18EC

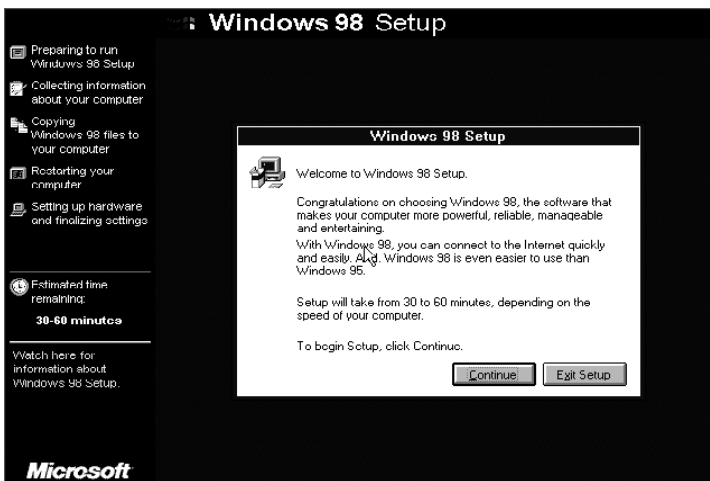
A:\>D:\WIN98\setup
```

Now it is time to start the install of Windows 98. After pressing Enter, you should be at the A:\. Now type D:\WIN98\setup. This is how the screen should look:

a:\D:\WIN98\setup

Before the install can start the Windows 98 setup need to check the Hard Drive. Press Enter, this also takes long time depending on the size of the Hard Drive.

(Step 09)



After scandisk has finish, and the files have been copied, you will come to this screen. Click Continue.



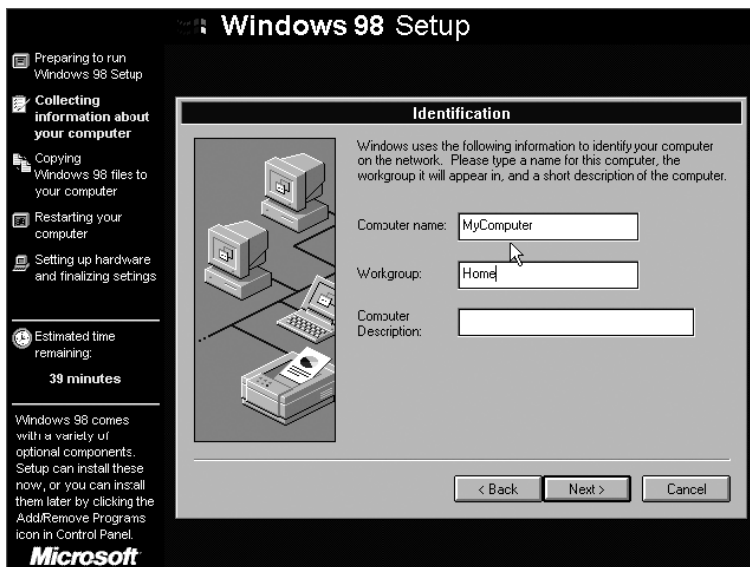
Select C:\Windows, and then click next.



Select Typical, and then click next.



Select Install the most common components, then click next.



This here is optional; change the values for Computer Name, Workgroup.

Computer Name: My Computer

Workgroup: Home

after you have made the changes, click next.



Select your location, click Next.



Click Next, you can choose to make a Windows 98 Startup Disk, if so then insert a floppy then click OK, if not the click Cancel.

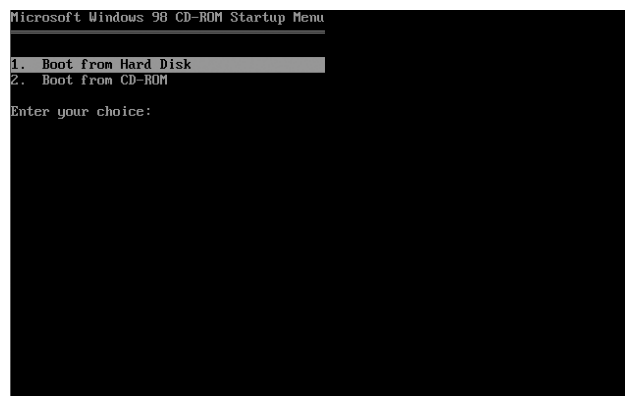


After the Startup Disk is completed, if you choose to make it, click Next to start copying Windows 98 files.



After the files have finished copying, remove the Windows 98 Startup Disk, and click OK to restart the computer.

(Step 10)



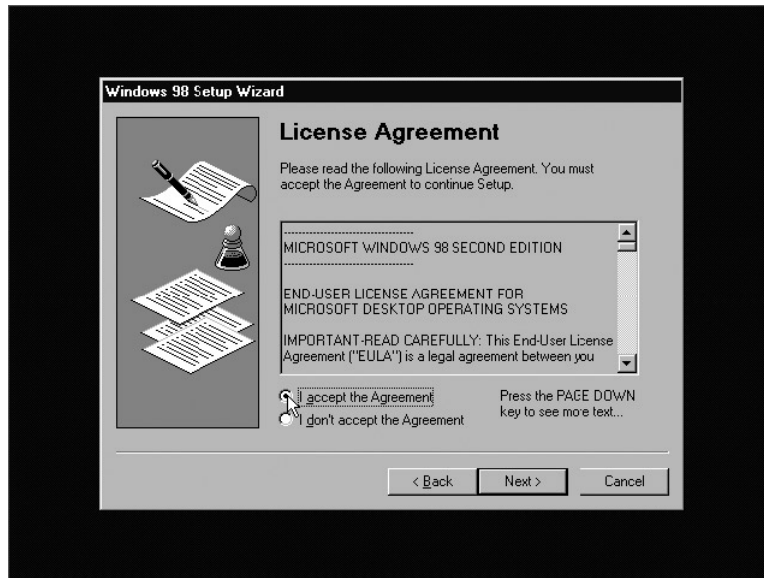
You will come to the Boot Select Screen, select Boot from Hard Drive.



The next screen you will see will be the Windows 98 Splash Screen.



Enter the User Information, and then click Next.



Read and agree to the EULA, then click Next.



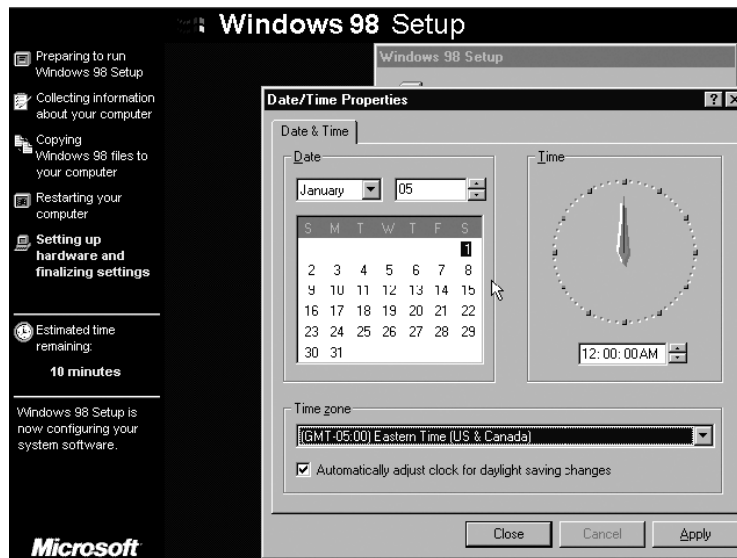
Enter the Windows 98 Product ID/Key, and then click Next.



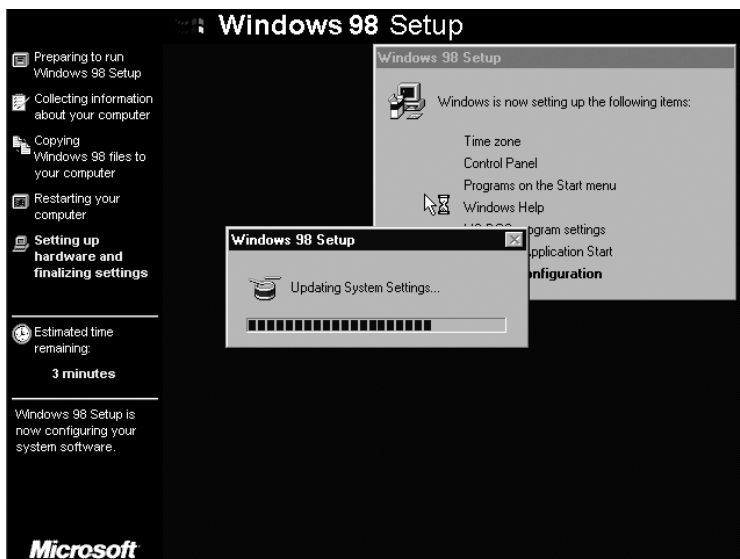
Click Finish.

(Step 11)

The computer will restart, select Boot from Hard Drive. The Windows 98 Splash Screen will come up. Windows is now finishing the last minute settings.



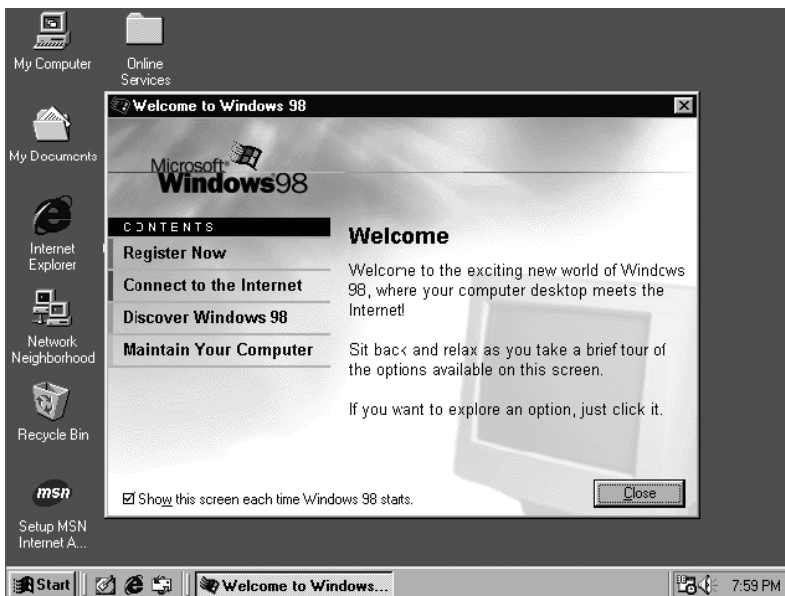
During those last minute settings, you will need to set the clock. Once done, click Apply then OK.



The Windows Install is also most complete, and after it finishes the computer will restart.

(Step 12)

For the last time the Boot Select Menu will come up, select Boot from Hard Drive. The Windows 98 Splash Screen will appear; after it goes away Windows will install any drivers need.



Congratulations, you have installed Windows 98.

Deleting partitions (Step 13)

To delete a partition, when at the **a:** type **fdisk**. This is how it should look:

a:\fdisk

When in the fdisk program press **enter**. Press **3**, if there are any **Logical** they have to be deleted before the **extended**. Before the **Logical** partition can be deleted the **extended** partition has to be deleted. When all of the partitions have been deleted then exit the fdisk program and restart the computer by pressing **Ctrl+alt+Del**. To finish the install of Windows 98 goto **(Step 02)**, read the last sentence.

reCoverING WINDoWS proDuCt Key

(Step 14) To recover the Windows Product Key:

Start -> run -> type **regedit** This will open the **registry editor**. From there navigate to:

hKey_LoCaL_MaChIne\Software\Microsoft\Windows\Current version

Click on the **Current version** folder, and on the right pane there will be a key that says **product Key**. Here will be a 25 digit key (both numbers and letters), copy it down. If you still can't find it, then:

edit -> Find Type **product Key** in the find box and click **Find Next**.

Chapter – 3

Installing Windows 7

Introduction

After the disappointment of Windows Vista and a lot of beta testing, Windows has finally released Windows 7. Vista, arguably Microsoft's biggest failure, fared even worse than Windows Me and promised to be all the things that Window users were asking for. Windows 7 is indeed everything that users wanted from Windows Vista but to a greater extent. Vista users should upgrade to Windows 7 as it includes enhancements from the Vista program as well as many additional features that makes it worthwhile.

Why should upgrade

There are many reasons that people choose to upgrade, but two tend to be the most common-speed and sexy new features. Windows 7 is exactly that, a package that offers many exciting new features that don't hinder the speed. The operating system has a footprint only marginally bigger than that of Windows XP. Windows XP came into existence in a time when computers had only a fraction of the memory that computers have today. When Windows XP was launched in 2001, users could only dream of all the exciting new features that Windows 7 has to offer and at a faster speed as well.

Windows 7 Features

One of the first's things that Windows 7 users will note is the enhanced Graphic User Interface, other than the speed. The graphic user interface is the part of the operating structure that makes all the zeros and ones behind the scene make sense. In Windows 7, the entire GUI has been turned upside down and made more efficient. Some of the features users liked from Vista, like the aero glass, still exist, but now the task bar operates like the "Dock" feature made popular by Mac OSX.

While making it easy to access minimized windows, this useful feature also provides point-and-click access to your favorite files, documents, programs etc. Windows 7 also boasts enhanced preview ability. This means that, whereas in Windows Vista hovering over a minimized window would show a small snapshot of the window, Windows 7 now has a "peek" feature that opens your snapshot up to full screen for a second so that the user can actually see what the minimized window contains. Users can also press the windows key + T to scroll through the windows that are open, similar to a "filmstrip."

Windows 7 also allows users to open a file by dragging over the application. Screens can be minimized by bumping the top of the screen with the window and a new "shake" feature allows a user to minimize all screens except the active one by "shaking" the window. Some of the popular Windows programs, such as Paint, have been made more user-friendly by adding the Ribbon feature, a feature that popularized in Office 2007, as standard on all Microsoft applications and applets. Although Windows 7 uses fewer

resources, it is still more user-friendly. It could not be an easier decision to upgrade Vista to Windows 7 with all these great features and surprises in store.

planning the Installation

As with any OS installation, we must first plan the installation process. When you run the Windows 7 Setup program, you must provide information about how to install and configure the operating system. Thorough planning can make your installation of Windows 7 more efficient by helping you to avoid potential problems during installation. An understanding of the configuration options will also help to ensure that you have properly configured your system.

Here are some of the most important things you should take into consideration when planning for your Windows 7 installation:

- Check System Requirements
- Check Hardware and Software Compatibility
- Determine Disk Partitioning Options
- Complete a Pre-Installation Checklist

Microsoft states the minimum recommended specs for Windows 7:

- 1 GHz 32-bit or 64-bit processor
- 1 GB of system memory
- 16 GB of available disk space
- Support for DirectX 9 graphics with 128 MB memory (to enable the Aero theme)
- DVD-R/W Drive
- Internet access (to activate and get updates)

32-bit or 64-bit Version

You need to decide whether to install the 32-bit or 64-bit version of Windows 7. The Windows 7 installation disc package includes both 32-bit and 64-bit versions of Windows 7. Basically, the 64-bit version of Windows handles large amounts of random access memory (RAM) more effectively than a 32-bit system. So if you plan on using Windows 7 on a computer with more than 3 GB of RAM, I would strongly suggest using the 64-bit version. Most programs designed for the 32-bit version of Windows will work on the 64-bit version of Windows, and if they don't, you can always use Windows XP Mode.

Note: Either way, you cannot use an existing 32-bit version of a previous OS to perform an in-place upgrade to a 64-bit version of Windows 7, and you'll need to format and install a fresh copy. Also, you cannot use an existing 64-bit version of a previous OS to perform an in-place upgrade to a 32-bit version of Windows 7.

type of Installation

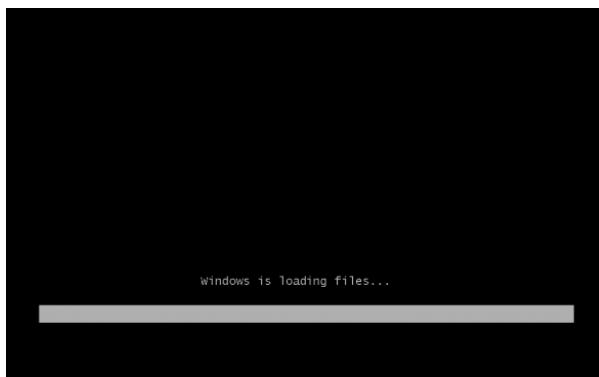
Basically, there are 2 approaches to installing Windows 7:

1. **Upgrade** (In-place upgrade) - This option replaces your current version of Windows with Windows 7, and keeps your files, settings, and programs in place on your computer.
2. **Custom** (“fresh” installation) - This option replaces your current version of Windows with Windows 7, but doesn’t preserve your files, settings, and programs. It’s sometimes referred to as a clean installation for that reason.

As always, a fresh installation is much better and I strongly recommend taking that track. Even if you’ve got an existing Windows XP/Vista OS on your computer, I would strongly recommend that you format it and install a fresh copy of the OS.

Beginning the Installation process

When installing on a physical computer insert your Windows 7 DVD media into your DVD drive and reboot your computer. If you’re asked to press a key to boot from DVD or CD, press any key. A black window will appear momentarily while the DVD content is read.



Note: These screenshots are taken from a Windows 7 Ultimate installation performed on a virtual machine running on VMware Workstation. I will be using an .ISO file mounted on the VMs CD/DVD drive.

Next, a **Starting Windows** screen will appear.



Note: If the Windows installation page doesn't appear and you're not asked to press a key to start from DVD or CD, you might have to specify that your computer uses its DVD or CD drive as the startup device.

the Installation process

Like in Windows Vista & Windows Server 2008, and unlike previous versions of Windows, a window 7 does not have a noticeable text phase of the setup process, and it will boot directly into the Graphical User Interface (GUI) mode.

After a few moments you will see the first prompt:



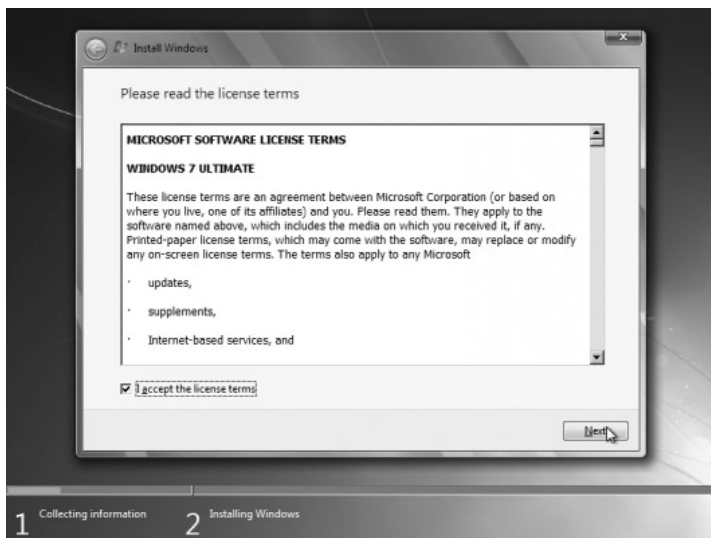
Click "Next" unless you want to change some regional settings for the installation process.



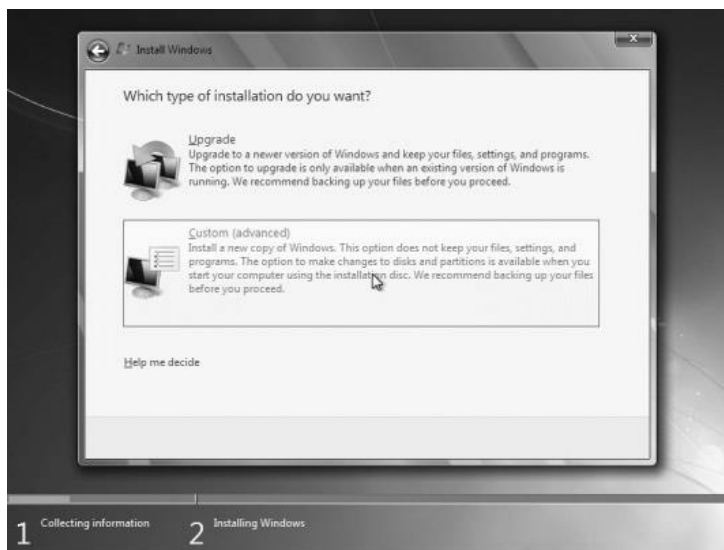
Click on the “Install now” button.

Note: If you’re using the installation media to repair an existing installation of Windows 7.

Next, accept the license terms and click on “Next”.



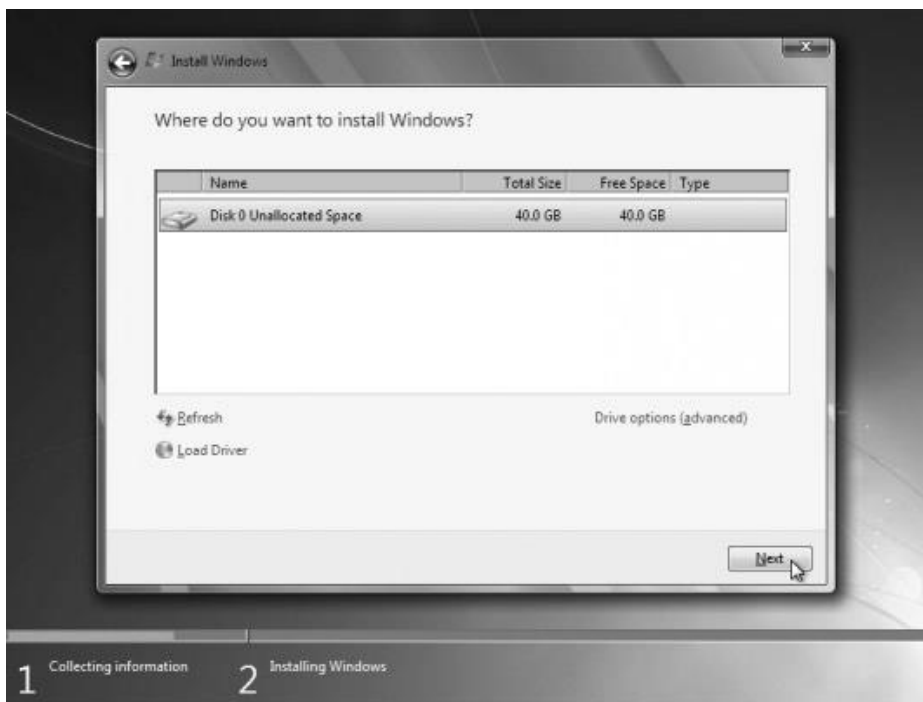
Next, unless you’re upgrading an existing Windows installation, press the Custom (Advanced) installation type button. Note that in this case, the Upgrade button is disabled because this specific installation if performed on a new computer without any previous operating system on it.



The next phase is to pick the installation partition. Since this computer has a new hard disk that hasn't been formatted before, you will only have the option to create a new partition on it.

If you don't want to specify a specific partition to install Windows on, or create partitions on your hard disk, click Next to begin the installation. If you already have another existing partition with enough free space and want to install the Windows 7 on that partition to create a multiboot configuration, select the partition you want to use, and then click Next to begin the installation. If you want to create, extend, delete, or format a partition, click Drive options (advanced), click the option you want, and then follow the instructions.

Since I don't need to perform any additional task I will just click on the "Next" button. The installation process will then create a partition on all the available disk space, and format it.



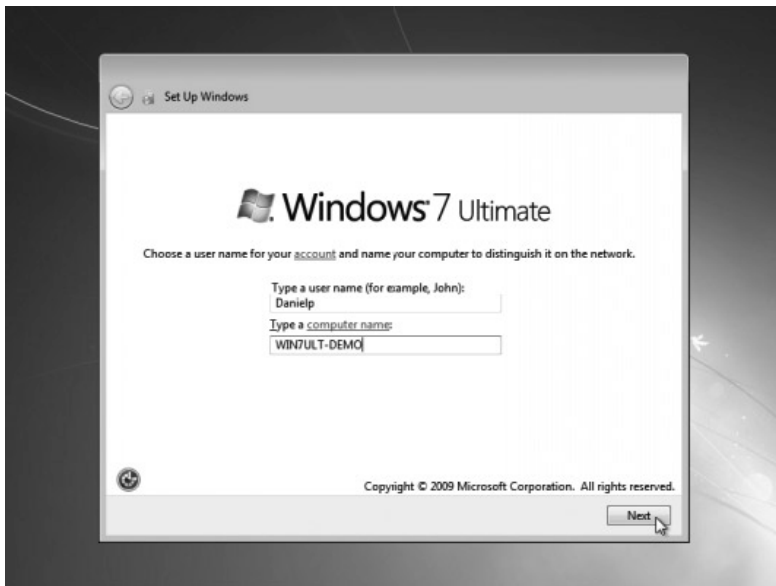
The setup process will now begin to copy files from the installation DVD media to the hard disk.



Process could take a while depending on the type of hardware your computer uses.

The computer will reboot, and the next thing you'll see is the prompt to set the user's and computer's name. By default, the computer's name will be username-PC, where username is the username you've entered.

Note: The user you're creating will be the only user currently available on the system. Like Vista, the built-in Administrator's account is disabled. Click on "Next".



Enter the user's password. Remember this password, as it will be the ONLY user on the system, and unless you create an additional user or enable the built-in administrator account, if you forget this password you'll need to crack it to gain access to the system. The best option would be to choose a complex password made of at least 7 characters or more (something like Pssw0rd or MY pa\$\$w0rd). You must also enter a password hint.

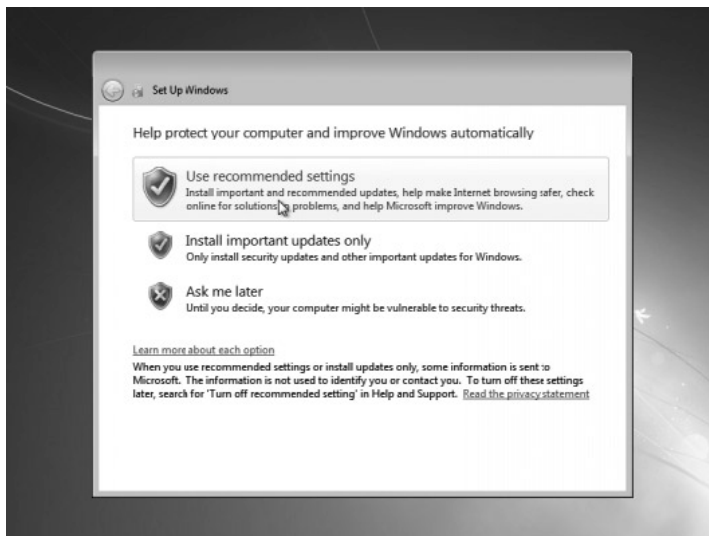
Click on "Next".



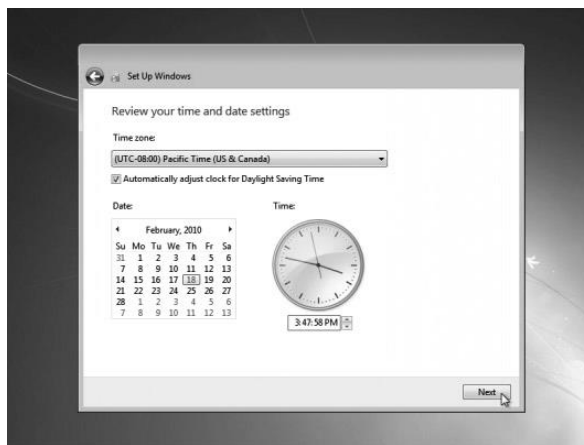
Next, type in your product key. If you do not have the product key at hand you can still click "Next", and proceed with the installation. You will be asked to enter the product key after Windows is installed.



Choose what sort of protection your computer gets. The recommended settings are best for someone that doesn't plan to hide their computer behind a corporate firewall (and even then, in some cases, this would be the best option). If you plan to install a 3rd-party firewall later you can opt to be prompted later. Note that this setting will also have effect on how the computer uses the Microsoft Windows Update (Automatic Updates) features.



Choose your time zone and location and click on "Next".



Select your network location type. This setting can be changed later, but do note that choosing a profile will have effect on the Windows Firewall and sharing settings. Click on "Next".



Windows will finalize the settings and your desktops will appear as follows.



This concludes the Windows 7 installation. Next, you would probably want to update your computer with the latest hot fixes and/or patches from Microsoft.

Chapter – 4

Windows server 2008

Introduction

Installing Windows Server 2008 is pretty straightforward and is very much like installing Windows Vista, but I thought I'd list the necessary steps here for additional information. For those of you who have never installed Vista before, the entire installation process is different than it used to be in previous Microsoft operating systems, and notably much easier to perform.

Using Vista's installation routine is a major benefit, especially for a server OS. Administrators can partition the system's hard drives during setup. More importantly, they can install the necessary AHCI or RAID storage drivers from a CD/DVD or even a USB thumb drive. Thus, error-prone floppies can finally be sent to the garbage bin.

Windows Server 2008 can also be installed as a Server Core installation, which is a cut-down version of Windows without the Windows Explorer GUI. Because you don't have the Windows Explorer to provide the GUI interface that you are used to, you configure everything through the command line interface or remotely using a Microsoft Management Console (MMC). The Server Core can be used for dedicated machines with basic roles such as Domain controller/Active Directory Domain Services, DNS Server, DHCP Server, file server, print server, Windows Media Server, IIS 7 web server and Windows Server Virtualization virtual server.

To use Windows Server 2008 you need to meet the following hardware requirements:

Component	requirement
Processor	• Minimum: 1GHz (x86 processor) or 1.4GHz (x64 processor) • Recommended: 2GHz or faster Note: An Intel Itanium 2 processor is required for Windows Server 2008 for Itanium-based Systems
Memory	• Minimum: 512MB RAM • Recommended: 2GB RAM or greater • Maximum (32-bit systems): 4GB (Standard) or 64GB (Enterprise and Datacenter) • Maximum (64-bit systems): 32GB (Standard) or 2TB (Enterprise, Datacenter and Itanium-based Systems)
Available Disk Space	• Minimum: 10GB • Recommended: 40GB or greater Note: Computers with more than 16GB of RAM will require more disk space for paging, hibernation, and dump files
Drive	DVD-ROM drive
Display and Peripherals	• Super VGA (800 x 600) or higher-resolution monitor • Keyboard • Microsoft Mouse or compatible pointing device

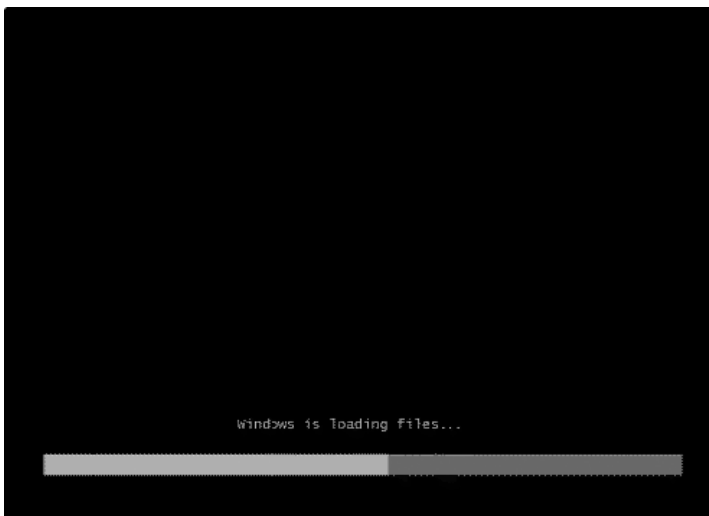
OS can be upgraded to:

The upgrade paths available for Windows Server 2008 shown in the table below:

If you are currently running:	You can upgrade to:
Windows Server 2003 Standard Edition (R2, Service Pack 1 or Service Pack 2)	Full Installation of Windows Server 2008 Standard Edition Full Installation of Windows Server 2008 Enterprise Edition
Windows Server 2003 Enterprise Edition (R2, Service Pack 1 or Service Pack 2)	Full Installation of Windows Server 2008 Enterprise Edition
Windows Server 2003 Datacenter Edition (R2, Service Pack 1 or Service Pack 2)	Full Installation of Windows Server 2008 Datacenter Edition

Installing Windows Server 2008

1. Insert the appropriate Windows Server 2008 installation media into your DVD drive. If you don't have an installation DVD for Windows Server 2008, you can download one for free from Microsoft's Windows 2008 Server Trial website.
2. Reboot the computer.



3. When prompted for an **installation language** and other regional options make your selection and press **next**.



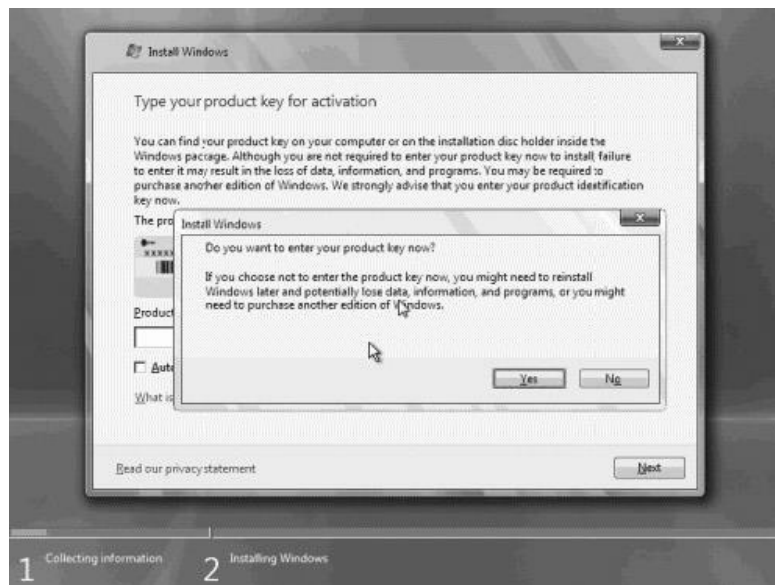
4. Next, press **Install Now** to begin the installation process.



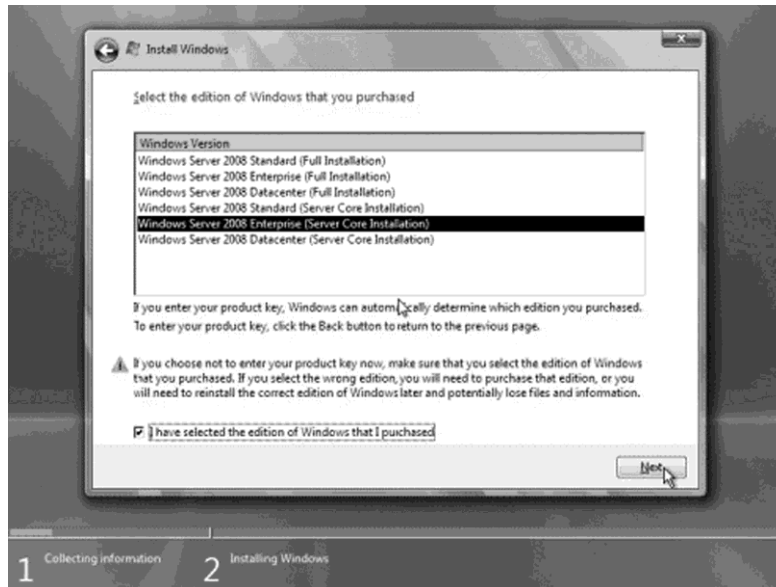
5. Product activation is now also identical with that found in Windows Vista. Enter your **product ID** in the next window, and if you want to automatically activate Windows the moment the installation finishes, click **Next**.



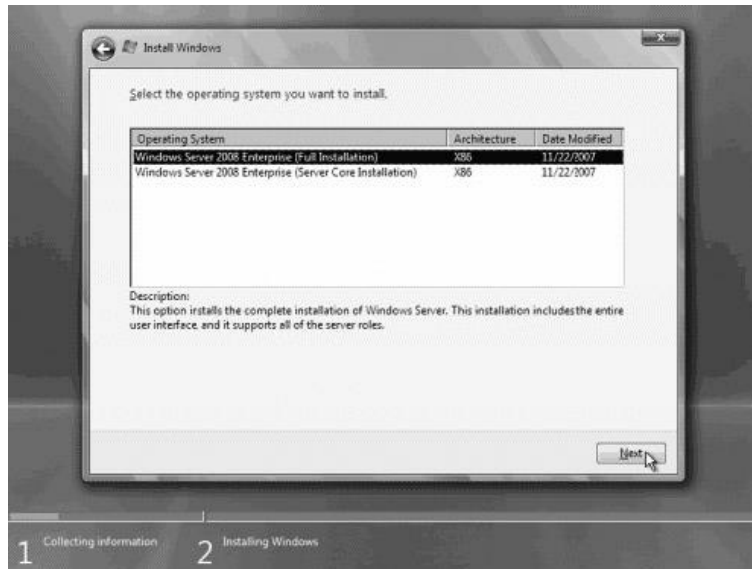
If you do not have the Product ID available right now, you can leave the box empty, and click Next. You will need to provide the Product ID later, after the server installation is over. Press No.



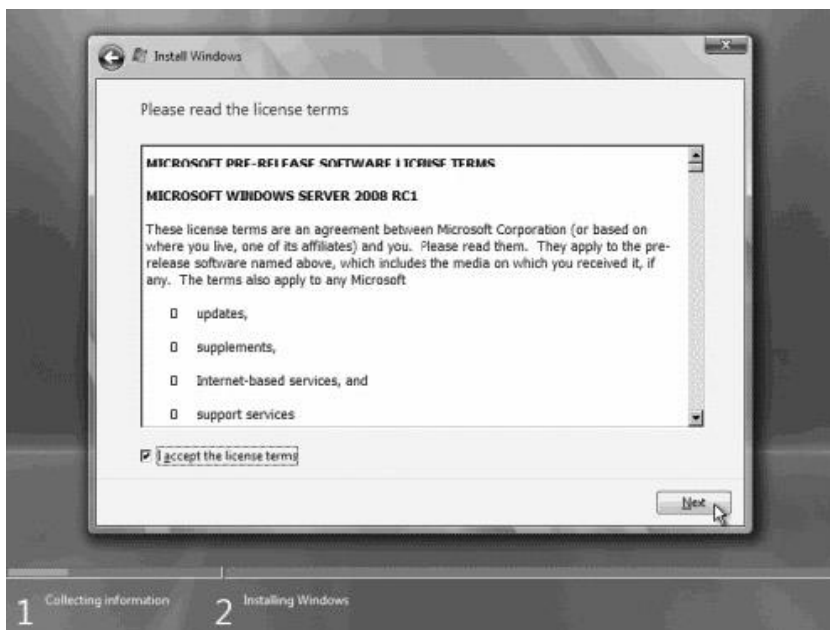
6. Because you did not provide the correct ID, the installation process cannot determine what kind of Windows Server 2008 license you own, and therefore you will be prompted to **select your correct version** in the next screen, assuming you are telling the truth and will provide the correct ID to prove your selection later on.



7. If you did provide the right Product ID, select the **Full version** of the right Windows version you're prompted, and click **next**.



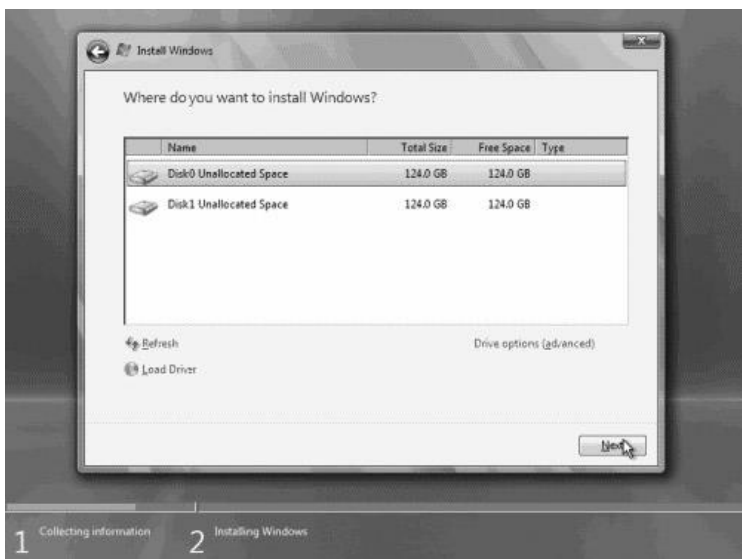
8. Read and accept the license terms by clicking to select the **checkbox** and pressing **Next**.



9. In the “Which type of installation do you want?” window, click the only available option – **Custom (advanced)**.

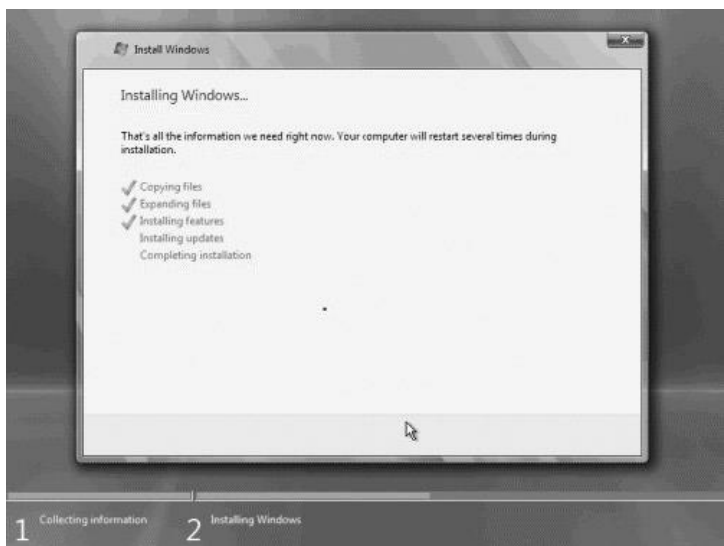


10. In the “Where do you want to install Windows?”, if you’re installing the server on a regular IDE hard disk, click to select the **first disk**, usually **Disk 0**, and click **Next**.



If you're installing on a hard disk that's connected to a SCSI controller, click Load Driver and insert the media provided by the controller's manufacturer. If you must, you can also click Drive Options and manually create a partition on the destination hard disk.

11. The installation now begins, and you can go and have lunch. Copying the setup files from the DVD to the hard drive only takes about one minute. However, extracting and uncompressing the files takes a good deal longer. After 20 minutes, the operating system is installed. The exact time it takes to install server core depends upon your hardware specifications. Faster disks will perform much faster installs... Windows Server 2008 takes up approximately 10 GB of hard drive space.



The installation process will reboot your computer, so, if in step #10 you inserted a floppy disk (either real or virtual), make sure you remove it before going to lunch, as you'll find the server hanged without the ability to boot (you can bypass this by configuring the server to boot from a CD/DVD and then from the hard disk in the booting order on the server's BIOS)

12. Then the server reboots you'll be prompted with the new Windows Server 2008 type of login screen. Press **Ctrl+Alt+Del** to log in.



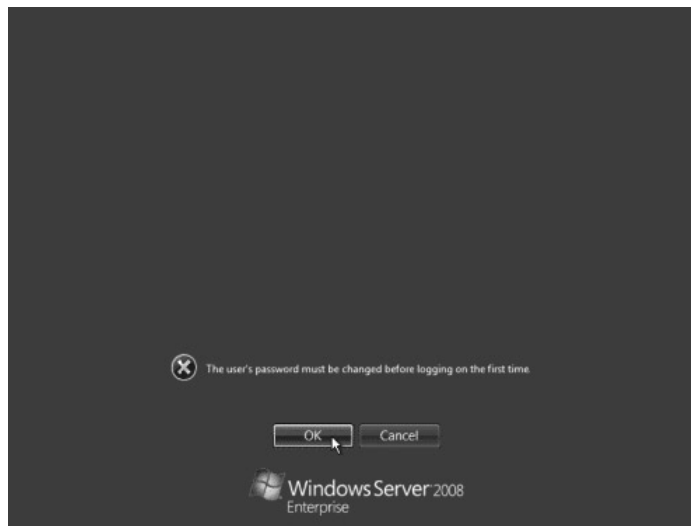
13. Click on **Other User**.



14. The default **administrator** is **blank**, so just type **administrator** and press **enter**.



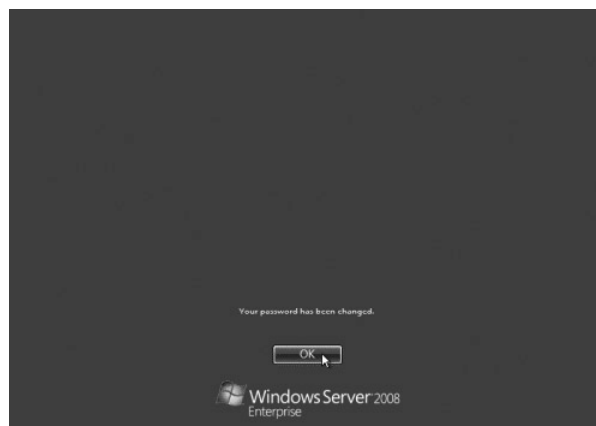
15. You will be prompted to change the user's password. You have no choice but to press **Ok**.



16. In the password changing dialog box, leave the **default password blank** (duh, read step #15...), and enter a new, complex, at-least-7-characters-long new password twice. A password like "top-secret" is not valid (it's not complex), but one like "T0pSecreT!" sure is. Make sure you remember it.



17. Someone thought it would be cool to nag you once more, so now you'll be prompted to accept the fact that the password had been changed. Press **Ok**.



18. finally, the desktop appears and that's it, you're logged on and can begin working. You will be greeted by an assistant for the **initial server configuration**, and after performing some initial configuration tasks, you will be able to start working.

Chapter - 5

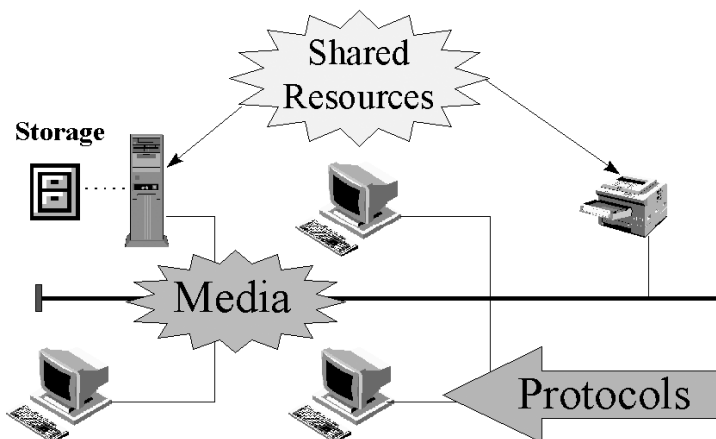
Basics of Networking

Introduction

The 1980s brought about a revolution in the computer industry. Prior to this time, most data processing was performed on mini and mainframe systems. In 1981, IBM introduced the first microcomputer designed specifically for business applications. This led to an explosion in computer usage and a revolution from centralized information management to distributive, and later, collaborative computing. This chapter introduces the concepts of computer networking and elements of services provided by computer networks today.

What is a Network

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.



The two basic types of networks include:

- Local Area Network (LAN)
- Wide Area Network (WAN)

You may also see references to a Metropolitan Area Networks (MAN), a Wireless LAN (WLAN), or a Wireless WAN (WWAN).

Local area Network

A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a writing lab, school, or building. Rarely are LAN computers more than a mile apart. In a typical LAN configuration, one computer

is designated as the file server. It stores all of the software that controls the network, as well as the software that can be shared by the computers attached to the network. Computers connected to the file server are called workstations. The workstations can be less powerful than the file server, and they may have additional software on their hard drives. On many LANs, cables are used to connect the network interface cards in each computer; other LANs may be wireless.

Wide area Network

Wide Area Networks (WANs) connect larger geographic areas, such as Florida, the United States, or the world. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of network.

Using a WAN, schools in Florida can communicate with places like Tokyo in a matter of minutes, without paying enormous phone bills. A WAN is complicated. It uses multiplexers to connect local and metropolitan networks to global communications networks like the Internet. To users, however, a WAN will not appear to be much different than a LAN.

advantages of Network

- **Speed.** Networks provide a very rapid method for sharing and transferring files. Without a network, files are shared by copying them to memory cards or discs, then carrying or sending the discs from one computer to another. This method of transferring files (referred to as sneaker-net) can be very time-consuming.
- **Cost.** Networkable versions of many popular software programs are available at considerable savings when compared to buying individually licensed copies.
- **Security.** Files and programs on a network can be designated as “copy inhibit,” so that you do not have to worry about illegal copying of programs. Also, passwords can be established for specific directories to restrict access to authorized users.
- **Centralized Software Management.** One of the greatest benefits of installing a network at a school is the fact that all of the software can be loaded on one computer (the file server). This eliminates that need to spend time and energy installing updates and tracking files on independent computers throughout the building.
- **resource Sharing.** Sharing resources is another advantage of school networks. Most schools cannot afford enough laser printers, fax machines, modems, scanners, and CD players for each computer. However, if these or similar peripherals are added to a network, they can be shared by many users.
- **electronic Mail.** The presence of a network provides the hardware necessary to install an e-mail system. E-mail aids in personal and professional communication for all school personnel, and it facilitates the dissemination of general information to the entire school staff. Electronic mail on a LAN can enable students to communicate with teachers and peers at their own school. If the LAN is connected to the Internet, students can communicate with others throughout the world.
- **Flexible access.** School networks allow students to access their files from computers throughout the school. Students can begin an assignment in their classroom, save part of it on a public access area of the network, then go to the media center

after school to finish their work. Students can also work cooperatively through the network.

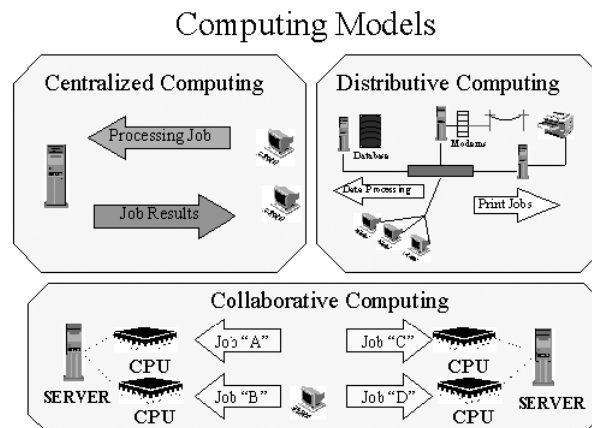
- **Workgroup Computing.** Collaborative software allows many users to work on a document or project concurrently. For example, educators located at various schools within a county could simultaneously contribute their ideas about new curriculum standards to the same document, spreadsheets, or website.

Disadvantages of Network

- **expensive to Install.** Although a network will generally save money over time, the initial costs of installation can be prohibitive. Cables, network cards, routers, and software are expensive, and the installation may require the services of a technician.
- **requires administrative time.** Proper maintenance of a network requires considerable time and expertise. Many schools have installed a network, only to find that they did not budget for the necessary administrative support.
- **File Server May Fail.** Although a file server is no more susceptible to failure than any other computer, when the files server “goes down,” the entire network may come to a halt. When this happens, the entire school may lose access to necessary programs and files.
- **Cables May Break.** The Topology chapter presents information about the various configurations of cables. Some of the configurations are designed to minimize the inconvenience of a broken cable; with other configurations, one broken cable can stop the entire network.
- **Must Monitor Security Issues.** Wireless networks are becoming increasingly common; however, security can be an issue with wireless networks.

Computing Models

Every computer network is configured in one of three basic designs. These three designs are based on how resources will be shared and managed.



Centralized Computing

Centralized Computing is the oldest design. Mainframe computers use this form of computing. One computer performs all of the processing. Dumb terminals, stations with no CPUs, are used to request services from the mainframe. The mainframe is used to store all the data.

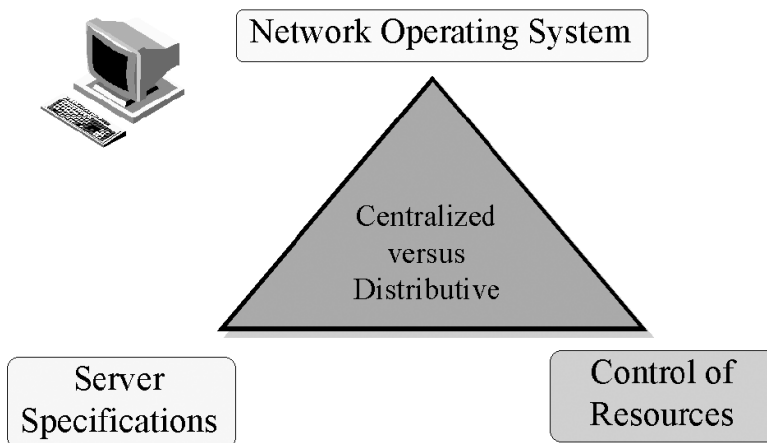
Distributed Computing

Distributed computing uses multiple smaller computers to achieve the same processing goals as the mainframe. Personal computers are an example of distributed computing. Each computer has its own processor and can handle any request. By networking personal computers, you allow resources to be shared across the network.

Collaborative Computing

Collaborative computing is the latest and most complicated computing model. The collaborative model involves multiple computers working together to accomplish related or independent tasks. The new line of Intel CPUs provides a new technology called symmetric multiprocessing (SMP), designed specifically for collaborative processing.

Network Services Management Model



The management of network services can be distributed, centralized, or a combination of both management models. The decision of which network service management model to use is based on three factors:

Network Operating Systems

Network operating systems are classified as server centric or peer-to-peer. Server centric operating systems include Novell NetWare, Windows NT server, and Banyan Vines. Peer-to-peer operating systems include Novell Personal NetWare, Microsoft Windows for Workgroups, Microsoft Windows 95, and Artisoft LANtastic.

Server Specialization

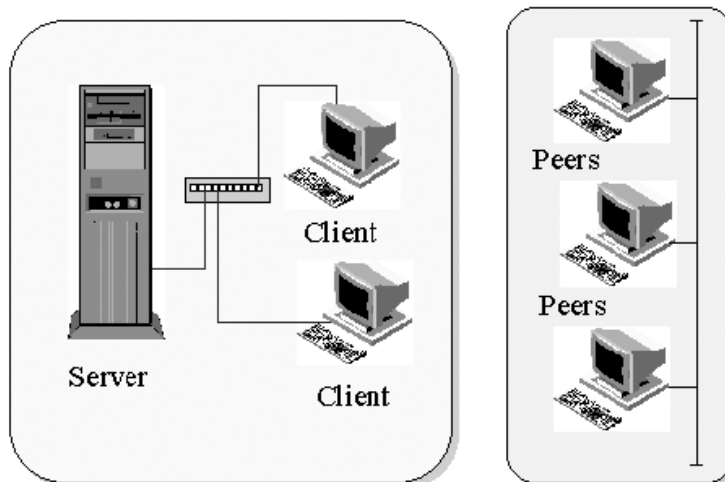
Server specialization occurs when a file server is dedicated to a specific network service. For example, a file server can be dedicated as a communication server or a messaging server. These file servers are optimized to take advantage of the services they provide.

Control of resources

If resources are centralized, a specific computer is used for providing network services. Distributed resources allow many computers to provide multiple services. Distributed resources work better with small networks.

Service providers and requesters

Service Providers and Requesters



In a computer network, computers are categorized as clients, servers, or peers.

Clients

A client is a computer that requests services from another computer called a server. The software that runs on a client is different from the software running on a server or peer.

Servers

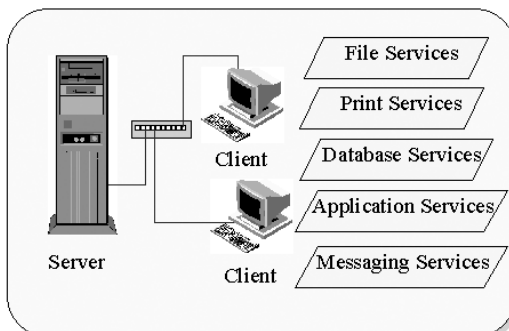
A server is a computer that provides services to and shares resources with clients. Servers can be server centric. Restrictions can be placed on what requests can be made or what services can be provided.

peers

Peers are computers that can function as clients and servers. Special software enables peer networks to share resources or access another computer's resources. Computers functioning as peers are considered parts of a peer-to-peer network.

Note: In today's networks, a computer can coexist in both client-server and peer-to-peer environments.

What are Network Services?



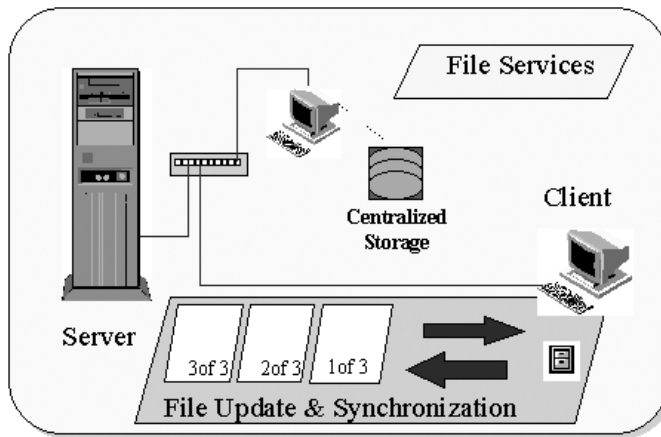
Network services are the capabilities provided by networked computers. Computers can provide five common network services.

- File services
- Print services
- Database services
- Application services
- Message services

Most of these services are provided by the network operating system (NOS). The NOS is a special operating system that coordinates resource sharing and provides services to clients.

Network File Services

Network File Services



File services include network applications designed to save, load, or manipulate data files stored on the network. File services can help provide the following.

- File archiving
- File update synchronization
- File transfer
- File storage and migration

1. **File archiving**

File archiving provides a method for data files to be backed up. One advantage is that multiple network file servers can be backed up with a single tape backup unit.

2. **File Update Synchronization**

This service solves a problem found with mobile computers. For example, a network server contains a database file used by traveling salespeople. The salespeople copy the file to their laptops, which they keep with them. When someone makes a change to the database on the server, the salespeople's databases are now out of synchronization. The synchronization process takes server and laptop changes and merges them to create an up-to-date database. Most of the changes made are based on comparison of time and date stamps to files and records.

3. **File transfer**

File transfer allows data to be copied from one location to another. This replaces an old method called "sneakernet." Sneakernet was the process of copying a file to disk and walking over to the other computer and copying the file to that computer. Large files may not fit on disk. In addition, compressing and copying files can be cumbersome. With file transfer services, this process is much faster.

4. **File Storage and Migration**

File storage services are critical because they allow data to be saved across the network. Data can be saved to three types of devices.

- **On-line storage**

An example of on-line storage is the hard drive. Hard drives in a server can be used to save network data.

- **Off-line storage**

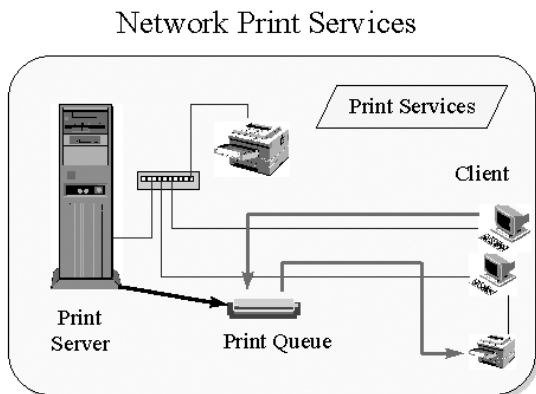
Off-line storage devices include tape backups. Backups are a necessary component for recovering from a hard drive crash. Tape backups should be stored off-site to prevent their loss from fire or catastrophe.

- **Nearline storage**

Nearline storage devices include tape jukeboxes. Data that have not been used for a while can be moved to a nearline device, freeing space on the server hard drive and allowing data to be accessed at a later time. Files moved to nearline devices appear to reside on the server. When a file on a nearline device is accessed, the file is copied back to the hard drive and the file is accessed.

- Data migration** refers to moving data from one storage medium to another. With migration, the network administrator can set up migration to move files based on the age of a file, owner of the file, size of the file, and so on.

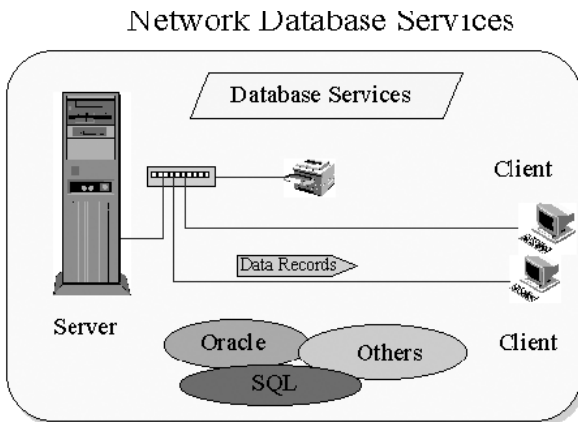
Network print Services



Print services include network applications designed to control and manage access to printers and fax equipment on the network. Print services provide the following benefits:

- Reduce the number of printers within the company.
- Place printers in convenient locations for users.
- Efficiently share specialized printers like high speed printers.
- Computerize the transmission and reception of faxes, reducing the amount of paper used (in some cases).
- Eliminate distance restraints of printer cables connected to a specific computer.
- Handle jobs sent to the same printer by queuing them.

Network Database Services



Database services provide server-based file storage and retrieval for clients. Database services also provide the following benefits:

- Improved data security.
- The ability to organize data logically between organizational departments.
- Reduced access time for clients accessing databases on servers.
- Replication.
- Coordination of distributed data.

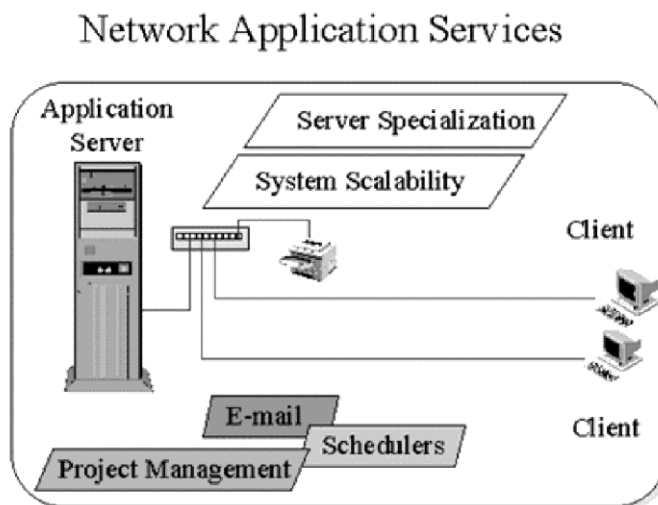
replication

Replication synchronizes databases across multiple computers. When one computer's database is updated, the changes are automatically made to the other computer's database. When changes to the database occur, the records within the database are date and time stamped. The other copies of the database compare the time and date stamps and make the necessary changes so the file is in sync. Novell's NetWare v4.x operating system incorporates replication with the NDS database.

Distributed data

The purpose of distributed data is to split a database and spread it across multiple computers. The database management system works to make the database appear as a whole database, even though it is split in multiple copies.

Network application Services



Application services are used by network clients. Application services provide scalability, growth, and specialized server capability.

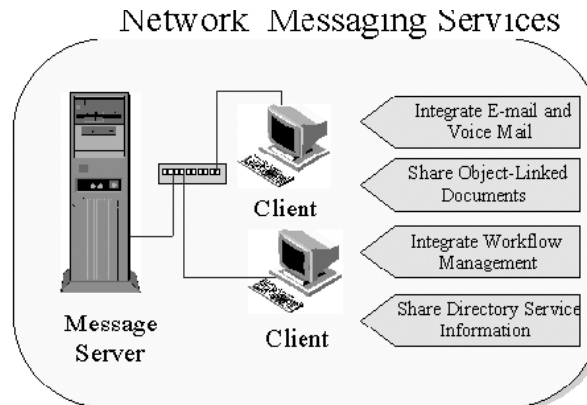
Scalability and Growth

If more processing power is needed by an application server, only the server must be upgraded. Other clients using the server do not need to be upgraded. This offers a relatively inexpensive upgrade path. If a server performing multiple functions (like a combination communication/database server) becomes overloaded, one application can be moved to another server.

Specialized Servers

Servers can be specialized to perform various services. Print servers, application servers, and communication servers are three examples. A mainframe would be much more appropriate to do a complex task than a PC would. The mainframe has much more processing power. PCs and mainframes can work together. The PC can make a request of the mainframe (send data to be computed). The mainframe performs the computation and sends the results back to the PC.

Network Messaging Services



Messaging services deal mostly with electronic mail. These services can store, deliver, and access text, binary, digitized video, graphics, and even audio data. Messaging services are similar to file services except that a message service works to provide an interaction between users. Message services provide the following:

- The ability to pass electronic messages and files between users.
- The integration of E-mail with voice mail systems.
- Data sharing through use of linked-object document applications. This allows an E-mail message to contain graphics, spreadsheets, audio, or anything that can be linked into a document.
- Workflow management applications can be used to generate forms like time cards and send them through electronic mail.
- Directory services information can be shared, allowing applications to communicate with other applications. This feature exists in NetWare v4.

Chapter - 6

Control panel & Sub Options

The Control Panel is a part of the Microsoft Windows graphical user interface which allows users to view and manipulate basic system settings and controls via applets, such as adding hardware, adding and removing software, controlling user accounts, and changing accessibility options. Additional applets can be provided by third party software.

The Control Panel has been an inherent part of the Microsoft Windows operating system since its first release (Windows 1.0), with many of the current applets being added in later versions. Beginning with Windows 95, the Control Panel is implemented as a special folder, i.e. the folder does not physically exist, but only contains shortcuts to various applets such as Add or Remove Programs and Internet Options. Physically, these applets are stored as .cpl files. For example, the Add or Remove Programs applet is stored under the name appwiz.cpl in the SYSTEM32 folder.

In recent versions of Windows, the Control Panel has two views, *Classic View* and *Category View*, and it is possible to switch between these through an option that appears on the left side of the window.

Many of the individual Control Panel applets can be accessed in other ways. For instance, *Display Properties* can be accessed by right-clicking on an empty area of the desktop and choosing *Properties*.

The classic view consists of shortcuts to the various control panel applets, usually without any description (other than the name). The categories are seen if the user uses “Details” view. The category view consists of categories, which when clicked on display the control panel applets related to the category. In Windows Vista, the category displays links to the most commonly used applets below the name of the category.



The applets listed below are components of the Microsoft Windows control panel, which allows users to define a range of settings for their computer, monitor the status of devices such as printers and modems, and set up new hardware, programs and network connections. Each applet is stored individually as a separate file (usually a .cpl file), folder or DLL, the locations of which are stored in the registry under the following keys:

- *HKLM\SOFTWARE\Microsoft\Windows\Current Version\Control Panel\Cpls* this contains the string format locations of all.cpl files on the hard drive used within the control panel.
- *HKLM\SOFTWARE\Microsoft\Windows\Current Version\Explorer\Control Panel\Namespace* this contains the location of the CLSID variables for all the panels not included as cpl files. These are commonly folders or shell applets, though Windows Vista allows physical programs themselves to be registered as well. The CLSID then allows items such as the icon, info box and category to be set and gives the location of the file to be used.

The control panel then uses these lists to locate the applets and load them into the control panel program (control.exe) when started by the user. In addition to using the control panel, a user can also invoke the applets manually via the command processor. For instance, the syntax "*Control.exe inetcpl.cpl*" or "*control.exe /name Microsoft. Internet Options*" will run the internet properties applet in Windows XP or Vista respectively. While both syntax examples are accepted on Windows Vista, only the former one is accepted on Windows XP.

Standard applet\$

accessibility Options (*Access.cpl*)

Allows users to configure the accessibility of their PC. It comprises various settings primarily aimed at users with disabilities or hardware problems.

- The behavior of the keyboard can be modified, this is aimed at people who have difficulty pressing key-combinations, or pressing a key just once. (*StickyKeys, FilterKeys and ToggleKeys*)
- Behavior of sounds can be modified. (*Sound Sentry and ShowSounds*)
- High contrast mode can be activated.
- The keyboard cursor can be customized.
- The mouse pointer can be controlled using the keyboard. (*MouseKeys*)

Note that in the next generation of Windows, the Ease of Access control panel superseded the simple access.cpl control panel in previous versions.

add new hardware (*hdwwiz.cpl*)

Launches a wizard which allows users to add new hardware devices to the system. This can be done by selecting from a list of devices or by specifying the location of the driver installation files.

add or remove programs (*appwiz.cpl*)

(Renamed “Programs and Features” in Windows Vista and later)

The Add/Remove Programs dialog allows the user to manipulate software installed on the system in a number of ways;

- Allows users to uninstall and change existing software packages, as well as indicating how much space individual programs take and how frequently they are used.
- Allows users to manually install software from a CD-ROM or Floppy Disk, and install add-ons from Windows Update.
- Allows users to change which Windows components are installed, via the Windows setup Wizard, which includes Internet Explorer, Windows Media Player and Windows Messenger.
- Finally, it allows users to specify the default applications for certain tasks, via the ‘set program access and defaults’ wizard, such as internet browsers, media players and email programs and whether access to these programs is available.

administrative tools (*control admintools*)

Contains tools for system administration, including security, performance and service configuration. These are links to various configurations of the Microsoft Management Console such as the local services list and the Event Viewer.

automatic Updates (*wuauclt.cpl*)

This is used to specify how the Automatic Updates client (*wuauclt.exe*) should download updates from the Microsoft Update Website, by default this is set to download and install daily, however this can be changed to a more suitable frequency. This also allows the user to specify whether to ask permission before downloading and/or installing updates or to simply switch off Automatic Updates all together.

date and time (*timedate.cpl*)

Allows user to change the date and time stored in the machines BIOS, change the time zone and specify whether to synchronize the date and time with an Internet Time Server and which server to use.

display (*control desktop*) (*desk.cpl*)

Allows the user to change the display characteristics of their computer;

- Allows users to change the desktop background (wallpaper) to a picture of their choice and specifies how it should be shown.
- Allows the user to change or disable the screensaver, and specify how long it takes to activate and whether to ask for a password on resume.
- Allows the user to specify the color styles of all elements within the system, primarily whether to use the Windows XP / Vista styles (blue by default in XP) or to use the classic Windows 98 / Me styles, this also allows the user to change the My Computer and Recycle Bin icons.
- Allows the user to change the screen resolution and color quality, and provides trouble shooting advice for displays.

Folder Options (*control folders*)



This item allows for configuration of how folders and files are presented in Windows Explorer. More specifically it allows the user to specify general settings like whether folders open in a new window or the existing window and whether the common tasks pane is shown, as well as more advanced tasks such as whether windows should hide critical system files and whether to show file extensions. It is also used to modify file type associations in Windows; i.e., which program opens which type of file and other settings like actions for each file type and the file extension.

Fonts (*control fonts*)

Displays all fonts installed on the computer. Users can remove fonts, install new fonts or search for fonts using font characteristics. Note that “explorer \Windows\Fonts” has the same effect.

Internet Options (*inetctl.cpl*)

Allows the user to change the way the computer manages internet connections and browser settings for Internet Explorer, it has several tags specifying different attributes;

- **General** - This specifies the homepage and color schemes and allows the user to delete internet usage history.
- **Security & Privacy** - These specify whether the computer should allow websites to undertake certain processes and download cookies, this panel also gives access to the inbuilt pop-up blocker (Windows XP SP2 and later) and the phishing controls (Internet Explorer 7).
- **Content** - Allows the parental controls and auto-complete to be configured and also specifies how to deal with certificates.
- **Connections, Programs and Advanced** - These give access to other aspects of internet settings such as the default modem connection and email client, proxy settings and other advanced configurations.

Game Controllers (*joy.cpl*)

Allows you to add, display, troubleshoot, and use advanced settings on joysticks and game controllers.

Keyboard (*control keyboard*)

Lets the user change and test keyboard settings, including cursor blink rate and key repeat rate.

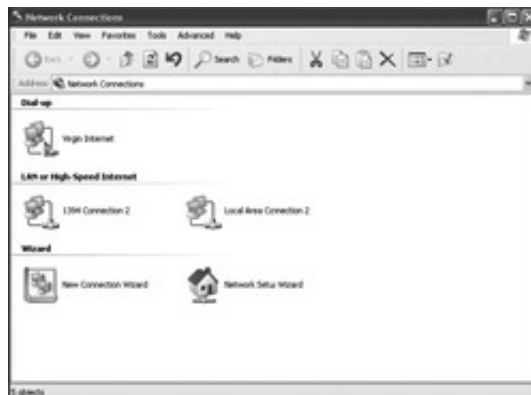
Mail (*mlcfg32.cpl*) (*mlcfg.cpl*)

Mail allows for configuration of the mail client in Windows, usually Microsoft Outlook. Microsoft Outlook Express cannot be configured with this item; it is configured through its own interface. mlcfg.cpl is used for 64 bit office applications first available with the Office 2010 release.

Mouse (*control mouse*) (*main.cpl*)

Mouse allows the configuration of pointer options, such as the double click and scroll speed, and includes visibility options such as whether to use pointer trails and whether the pointer should disappear when typing. This also allows the user to specify the pointer appearance for each task, such as resize and busy.

network Connections (*control net connections*) (*ncpa.cpl*)



Displays and allows the user to edit or create network connections such as Local Area Networks (LAN) and internet connections. It also offers troubleshooting functions in case the computer has to be reconnected to the network.

phone and Modem Options (*telephon.cpl*)

Manages telephone and modem connections.

power Options (*powercfg.cpl*)

Includes options to manage energy consumption such as;

- Specify how long it takes to switch off the display and hard drives and how long it takes for the system to enter standby, if at all.
- To decide what to do when the computer's on/off button is pressed, such as whether to shut down or to enter standby.
- Whether to allow Hibernation (some systems become unstable when restarting).
- Allows the user to configure UPS (if available).

printers and Faxes (*control printers*)

Displays all the printers and faxes currently installed on the computer, and has two main uses;

- Firstly, it shows the all the jobs queued for each printer, the file size and status of each job and which user they belong to, it also allows each job to be paused, canceled or moved up or down the list.
- Secondly, it allows the user to set the printing or faxing preferences, such as paper size and quality via the manufacturers own preferences pane and also specifies how to share the printer across a computer network , the device drivers, ports etc.

regional and language Settings (*intl.cpl*)

Various regional settings can be altered, for instance:

- The way numbers are displayed (e.g. decimal separator).
- How Currency values are displayed, including the Currency sign.
- Time and date notations, such as the date separator and whether the clock should be in 12 or 24 hours.
- Cultural location of the user's computer (The time zone is set in Date and Time).
- Language;
 - Input language.
 - Keyboard layout (mapping between key strokes and characters).
 - Display language for Menus and Dialog Boxes.
- Whether files necessary for Asiatic language support must be installed.
- Installed code pages.

Security Center (*wscui.cpl*)

Renamed "Action Center" in Windows 7

First added in Windows XP with Service Pack 2, Security Center gives the user access to the inbuilt Windows security components, as well as providing information about any existing antivirus software such as McAfee or Zone Alarm. It includes access to Windows Update, where users can specify whether the computer should check for updates regularly (also available through the Windows Update panel), and options for managing internet security settings. It also includes links to internet articles about PC security and current virus threats and notifies the user when the PCs security is compromised.

Sounds and audio devices (*mmsys.cpl*)

This panel contains various audio-related functions;

- Change the speaker volume and type and specify whether to show the volume icon in the notification area.
- Change the sounds played for the system or specific programs when a certain event occurs, i.e. Windows Startup or Critical Stop.
- Change default devices for music playback, recording, voice recognition, MIDI etc.
- Change the Sound card settings and whether to use Hardware acceleration.
- Display the audio devices installed on the computer, and allows them to be configured.

Speech (*Sapi.cpl*)

This applet has two main functions, the first is specify settings for Speech synthesis, allowing the user to select the voice the computer should use to narrate text and how fast it should read. The second is to specify settings for Speech recognition, allowing the user to set up different profiles detailing how the computer should deal with an individual's dialect, for instance;

- The amount of grammatical errors in a person's voice (punctuality sensitivity).
- The speed at which the person speaks and the time delay between words.

This also allows the user to access the voice recognition training wizard, in which an individual 'teaches' the computer to recognize a person voice interactively using the microphone.

System (*Sysdm.cpl*)

This is used to view and change core system settings, a user can for instance:

- Display general information on the user's machine such as the amount of RAM, CPU speed and type, the version of Windows the system is using and the manufacturer.
- Edit the computer name in a network workgroup.
- Manage and Configure hardware devices, and view information such as the manufacturer, user access and driver version of any hardware device installed on the system via Device Manager.
- Enable/Disable system features such as automatic updates and System restore monitoring.
- Specify advanced features such as performance logs, virtual memory settings and roaming profiles.

taskbar and Start Menu (*rundll32.exe shell32.dll,Options_RunDLL 1*)

Allows the user to change the behavior and appearance of the task bar and Start Menu;

- Specifies whether to use Windows XP/Vista or Classic 9x/Me styles on the taskbar and start menu.
- Whether the taskbar should Auto-Hide.
- Whether to show the clock in the notification area.
- Allows the user to manage the tray icons.
- Advanced options such as whether to show Printers & Faxes in the start menu and whether to display My Documents as a menu or as a link to a new window.

User accounts (*nusrmgr.cpl*)

This allows the user to configure their account and other accounts used in the system, should they have sufficient privileges. They can change their username and password, their picture (if enabled) and their .net passport. If the current user has an administrator's account they can also add, delete and modify other user accounts as well as make changes to core system settings. This panel also specifies whether the guest account should be active and whether to use the Welcome screen while Windows loads.

peripheral devices

These are options in the control panel that show devices connected to the computer. They do not actually offer a direct interface to control these devices, but rather offer basic tasks such as removal procedures and links to wizards (Printers & faxes is the exception).

Such Applets include;

- Scanners and Cameras
- Game Controllers
- Portable Media Devices

Other MICrOSOFt-dIStRiBUted appletS**bluetooth devices (*bthprops.cpl*)**

Available with Bluetooth enabled systems running XP SP2 or later, this enables users to configure a Bluetooth connection, showing a list of all Bluetooth devices interacting with the system, an addition to the following items;

Allowing users to create incoming and outgoing 'virtual' COM Ports, which allow devices to have dedicated connections to the system.

Allowing users to specify general bluetooth characteristics such as whether the computer is discoverable and the computers name which is broadcast.

Color (*color.cpl*)

Enables a more advanced control of color settings within Windows than is available in 'display', suitable for developers and visual specialists it allows users to create and load International Color Consortium compliant color profiles, associate screen color with printers and cameras and view a 3D graphics plot of the color gamut. By default this applet is not installed, however it can be installed for free from the Microsoft Website^{[dead link](#)}

Infrared (*irprops.cpl*)

Similar to the Bluetooth applet, this is used to configure how the computer manages any wireless infrared ports installed, including options such as connectivity and security.

CSnW (*nwc.cpl*)

The Client Service for NetWare applet is used to select a default tree and context in a

Novell Directory Services (NDS) environment, or the NetWare server used most frequently in a non-NDS environment.

Requirement: Installing the Client Service for NetWare.

Software explorers

Part of Windows Defender, allows users to view detailed information about software that is currently running on the computer that can affect the users' privacy or the security of the computer.

Third-party applets

Third-party software vendors have released many applets. Although it is impossible to mention all of them, some of them are listed here:

Icon	File name	description
AC3 Filter	ac3filter.cpl	Configures speaker configuration and other parameters of the AC3 decoder filter.
Adobe Gamma	Adobe Gamma.cpl	For altering the screen display with Adobe Systems Imaging Software such as Photoshop.
Adobe Version Cue CS2	VersionCueCS2.cpl	To configure Adobe Version Cue.
Application paths	apppaths.cpl	Sets application paths, start-up commands and system services, coded by Gregory Braun.
Autodesk Plotter Manager	plotman.cpl	Adds, remove and changes plotters properties for AutoCAD products.
AvantGo Connect	agcpl.cpl	Synchronizes mobile versions (called "channels") of websites to a smartphone or PDA, see AvantGo.
Avira Antivirus Personal Edition	avconfig.cpl	Configures Avira Antivirus program.
BACKPACK Finder	bpcpl.cpl	To configure the Micro Solutions Backpack CD driver.
BDE Administrator	bdeadmin.cpl	To configure the Borland Database Engine.
Boot Camp Control Panel		Setting for Mac OS X based computers
Clear Case	cc.cpl	To configure IBM Rational Clear Case.
Color Settings	3dcc.cpl	Changes the look and feel of Windows, see http://jote.pai.net.pl/jn/3dcc/ ^[dead link]
Compaq Diagnostics	cpqdiag.cpl	To view information a computer's hardware and software configuration, legacy application.
Control Panel	controlp.cpl	Control Panel Customization Toy, coded by Ali Lokhandwala.
Control Version System	cvsnt.cpl	Control Panel Customization Toy, by Brian Berliner. david d 'zoo' zuhn, Jeff Polk. Tony Hoyle

Creative Element Power Tools		To configure Creative Element Power Tools, a free-to-try program providing access to additional Windows tools.
Corel Versions	verscpl.cpl	Configures Corel versions.
DANS	danetsvc.cpl	Configures the Shaffer Solutions Disk Access Network Services, NFS client for Windows.
Disk Access	dacfg.cpl	Configures how the Shaffer Solutions Disk Access makes connections to remote NFS servers.
Folder size	FolderSize.cpl	Folder Size for Windows shows the size of folders in Windows Explorer.
FirebirdSQL Service Manager	fmmgr.cpl	Configures Firebird (database server) service options.
HP Jetadmin	jetadmin.cpl	HP Jetadmin configures and monitors HP printers.
HP Lock	Hplock.cpl	A Windows 95 utility to lock the PC keyboard, mouse and on/off switch in one click on legacy HP Vectra.
Icon Packager	ipcpl.cpl	To customize Windows icons and cursors, see Icon Packager.
ImDisk Virtual Disk Driver	imdisk.cpl	Administration of ImDisk Virtual Disk Driver.
Intel Extreme Graphics	igfxcpl.cpl	To change advanced settings on systems using Intel GPUs
IP Office Voicemail Pro	ims.cpl	To configure Avaya IP Office Voicemail Pro.
Java	jplicpl32.cpl	For changing settings with Java Runtime Console.
JInitiator 1.x.y.z	pluginpl1xyz.cpl	To configure Oracle's JInitiator, note x.y.z is version numbers.
MSConfig	MSConfig.cpl	Launches the Microsoft System Configuration Utility.
Multisite	ms.cpl	To configure IBM Rational Clear Case Multisite.
Nero Burn Rights	NeroBurnRights.cpl	For specifying who is allowed to use the CD burner with Nero.
nVIDIA Control panel	nvidia.cpl	To change advanced settings on systems using nVIDIA GPUs
Pointer Devices	tbctplnl.cpl	To configure the Touch-Base Universal Pointer Device Driver (UPDD).
QuickTime	quicktime.cpl	For specifying settings of the Apple Quicktime Player.
RealPlayer	prefscpl.cpl	To configure the RealPlayer preferences, older versions.
Realtek AC97 Audio Control Panel	alsndmgr.cpl	To configure the Realtek audio controller.
RESTRick Control Panel	rest2.cpl	Windows Tuning and system restrictions setup, by Rtsecurity.
Safarp	safarp.cpl	Safarp is a small and fast alternative to the Add or Remove Programs applet.

Send To Toys	sendtotoys.cpl	To configure the Send To right click system menu in Microsoft Windows.
Services and Devices	pserv.cpl	From p-nand-q to manage Windows services and devices and uninstall applications.
SNTP Service	sntpserc.cpl	From Dillobits Software, to manage the SNTP client service.
Startup	startup.cpl	Control programs that run at system start-up, coded by Mike Lin.
Symantec Live Update	s32lucp2.cpl	Configures the Symantec Live Update update service.
System Information	Sancpl.cpl	Launches SiSoftware Sandra utility.
System Info for Windows	siw.cpl	Launches the SIW application.
Trust-No-Exe	trustnoexe.cpl	Configures the Beyond Logic Trust-No-Exe executable filter.
VMware Tools	VMControlPanel.cpl	To configure VMware Tools.
WIBU-KEY	wibuke32.cpl	To configure the WIBU-KEY Software Protection.
Win logos	wnlgo.cpl	To change the windows start-up and shutdown screens in Windows 98 or ME, coded by Ali Lokhandwala.
X-Setup Pro	xqdcXSPApplet.cpl	Launches X-Setup Pro, a Windows tweaker application.

Chapter – 7

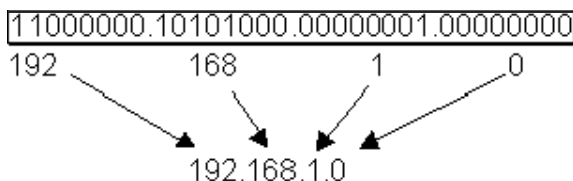
Ip addressing & Implementation

Introduction

Each computer on a TCP/IP based network (including the Internet) has a unique, numeric address called an IP address (IP stands for Internet Protocol), enabling data packages to be addressed to this specific recipient.

What is an Ip address?

An IP address consists of four so-called octets separated by dots. The octet is a binary number of eight digits, which equals the decimal numbers from 0 to 255. To make IP addresses easier to read and write, they are often expressed as four decimal numbers, each separated by a dot. This format is called “dotted-decimal notation”.



An IP address in its binary and dotted-decimal notation

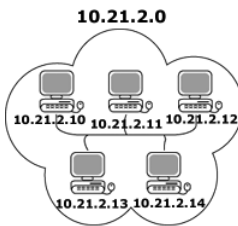
In a local area network based on TCP/IP, an IP address must be assigned to each host (computer or device) in the network. The IP address must be unique to each host. (If two hosts were given the same address, the data to these hosts would be picked up randomly by one of them – be it the intended receiver or not – causing network irregularities.)

In addition, a device that serves as router to another network contains two or more network adaptors and belongs to two or more networks. In this case, each adaptor must be assigned a unique IP address on each network.

Part of an IP address designates the network, while another part designates the individual host. The network number field is also referred to as the ‘network prefix’.



The two parts of an IP address

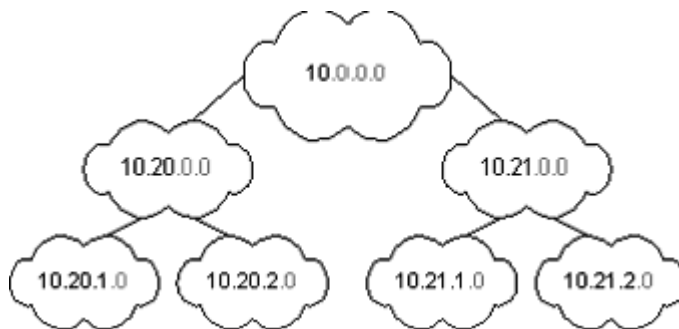


Exactly where the network part ends and the host part begin is calculated by routers, using a so-called subnet mask as a deciphering key.

All hosts on a given network share the same network number, but each of them must have a unique host number:

The host portion of the IP address is unique to each host.

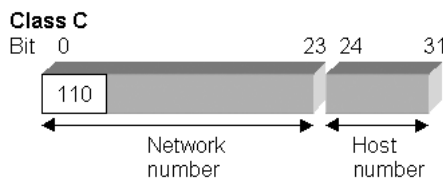
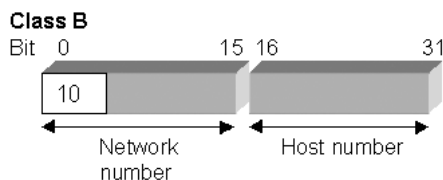
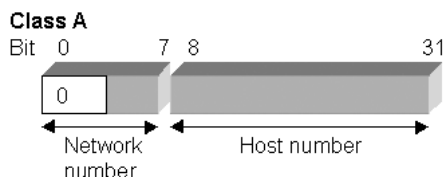
The network portion of an IP address is inherited down through a network hierarchy, as illustrated below.



Each cloud symbolizes a network segment

Classes of Ip addresses

In order to provide the flexibility required to support differently sized networks, IP addresses come in three *classes*, A, B, and C. Every class fixes the boundary between the network portion and the host portion of the IP address at a different point. This makes them appropriate for different size networks.



Class C addresses allow 254 hosts per network and are typically used by smaller and middle-sized companies. Class B networks allow a maximum of 16,384 hosts, while Class A networks allow more than 16 million hosts. As a consequence, Class A networks are only used by really large organizations.

Calculating the number of possible hosts requires a closer look at the IP classes in their binary form. (The binary system is a base-2 number system, just like the base-10 number system is known as the decimal number system). It is done as follows:

- In a Class C network only the last octet is used to designate the hosts. The maximum decimal number that you can write using eight bits is 256 (2^8). The host calculation now requires that 2 is subtracted, because two host addresses must be reserved for a network address and a broadcast address (for a further explanation of network and broadcast addresses, see the section on 'Subnets'). Ergo the maximum number of hosts on a Class C network is $256-2=254$.
- A class B network allows a maximum of 16,384 hosts ($2^{16}-2$) per network (two octets designate the hosts).
- A class A network allows up to 16,777,214 ($2^{24}-2$) hosts per network (three octets are used to designate the hosts).
- There are five classes of the IP addresses such as A, B, C, D and E and only 3 classes are in the use. Class D IP addresses are reserved for the multicast group and cannot be assigned to hosts and the E class IP addresses are the experimental addresses and cannot be assigned to the people. Every IP address consists of 4 octets and 32 bits. Every participating host and the devices on a network such as servers, routers, switches, DNS, DHCP, gateway, web server, internet fax server and printer have their own unique addresses within the scope of the network.
- TCP/IP protocols are installed by default with the Windows based operating systems. After the TCP/IP protocols are successfully installed you need to configure them through the Properties Tab of the Local Area Connection.

Class D

The binary addresses for the class D starts with 1110 and the IP addresses range can be between 224 to 239. An example of the class D IP address is 230.50.100.1

Class e

The binary address can start with 1111 and the decimal can be anywhere from 240 to 255. An example of the class E IP address is 245.101.10.10

It is very important to know that all the computers in the same network segment should have the IP addresses for the same class i.e. form A, B or C.

The table below shows the range of dotted-decimal values that can be assigned to each of the three address classes. An x represents the host number field of the address which is assigned by the network administrator.

Address class notation	IP address range in dotted-decimal
A (/8 prefixes)	1.xxx.xxx.xxx through 126.xxx.xxx.xxx
B (/16 prefixes)	128.0.xxx.xxx through 191.255.xxx.xxx
C (/24 prefixes)	192.0.0.xxx through 223.255.255.xxx

Class A networks are also referred to as '/8's' (pronounced slash eight's or just eight's) since they have an 8-bit network prefix (one octet is used to designate the network). Following the same convention, Class B networks are called '/16s' and Class C networks '/24s'.

Ip addressing tips

- A Network ID cannot be All 0s
- A host ID cannot be All 1 because this represents a broadcast address for the local network.
- Each host must have a unique host portion of the IP address.
- All hosts on the same network segment should have the same network id.
- A host address cannot be 127 because 127 have been reserved for the loop back functionalities.

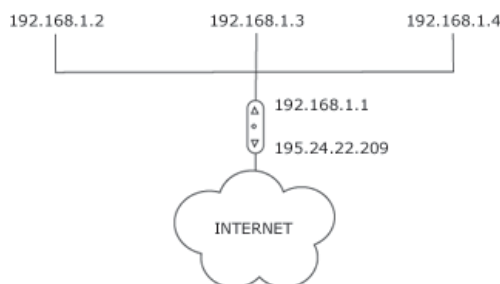
Globally routable and private network Ip addresses

There are two *types* of IP addresses – those which are globally routable (included in the routing tables on the Internet), and those which have been set aside for private networks. It is generally recommended that organizations use IP addresses from the blocks of private network addresses for hosts that require IP connectivity within their company network, but do not require external connections to the global Internet.

The system with non-routable IP addresses was introduced to help prevent a future shortage of IP addresses due to the explosive growth of the Internet. Because addresses belonging to these address blocks are not routed through the Internet routing system, the same numbers can be used at the same time by many different organizations.

There are no official rules for when to use which of the three private network IP address blocks, but generally the one of the most suitable size is used. For obvious reasons there is no need to use 10.x.x.x if it is unthinkable that your LAN will ever grow to more than 254 hosts. However, when using private addresses the network administrator can be liberal on the usage of the addresses when assigning them to the different parts of a network, as the strict rules that govern public IP address assignment do not apply. Hosts with private network IP addresses cannot communicate directly with the Internet, because the Internet refuses to receive and transmit data with such origin or destination address. For a host with a private network IP address to be allowed to communicate with the Internet, it must have its data stream to the Internet handled by an intermediary host, which can act as an 'Internet representative' for the private host. The intermediary host must have ways to relay data between the global Internet and the host on the private network. Therefore it must have a globally routable IP address that it uses when communicating with the

Internet and a private network IP address that is used for communication with the private host. There are a number of different types of intermediary hosts that fit this description. The most common types of intermediary hosts are proxy servers, firewalls and firewalls with NAT (Network Address Translation).



A NAT router translating private network IP addresses to globally routable IP addresses

An advantage of using private network addresses is that it makes it easier for organizations to change their Internet service provider without having to renumber their IP addresses. If private network addresses are not used, renumbering when changing ISP is necessary because globally routable IP addresses are “owned” by the Internet service provider that the company has “leased” the IP addresses from. It is possible to buy and own IP addresses, but this only applies to very large organizations that need in the magnitude of 40,000 globally routable IP addresses.

Using private network IP addresses also gives a company a measure of security. Globally routable IP addresses are advertised in the routing tables on the Internet, making the system vulnerable to hackers. When private IP network addresses are used, however, the intermediary host (such as a firewall with NAT) will work as a barrier against unwanted visits from the Internet.

The current version of IP, IP version 4, defines a 32-bit address, which means that there are only 2^{32} (4,294,967,296) addresses available globally. Over the past few years, the number of available IP addresses on the Internet has started to run out, as the number of companies and people wishing to go on-line has exploded. As a consequence, a new generation of IP addresses (IPv6) is currently in the works. The current IP system will not become obsolete overnight; however, as the two systems will coexist for some time after the new version has been implemented.

Differences between private and public network addressing schemes.

As to assigning addresses to devices, two general types of addresses can be used: public and private.

public addresses

Public addresses are Class A, B, and C addresses that can be used to access devices in other public networks, such as the Internet. The Internet Assigned Numbers Authority (IANA) is ultimately responsible for handing out and managing public addresses. Normally

you get public addresses directly from your ISP, which, in turn, requests them from one of five upstream address registries:

- American Registry for Internet Numbers (ARIN)
- Reseaux IP Europeans Network Coordination Center (RIPE NCC)
- Asia Pacific Registry for Internet Numbers (APNIC)
- Latin American and Caribbean Internet Address Registry (LACNIC)
- African Network Information Centre (AfriNIC)

private addresses

Within the range of addresses for Class A, B, and C addresses are some reserved addresses, commonly called private addresses. Anyone can use private addresses; however, this creates a problem if you want to access the Internet. Remember that each device in the network (in this case, this includes the Internet) must have a unique IP address. If two networks are using the same private addresses, you would run into reachability issues. To access the Internet, your source IP addresses must have a unique Internet public address. This can be accomplished through address translation. Here is a list of private addresses that are assigned in RFC 1918:

- Class A: 10.0.0.0–10.255.255.255 (1 Class A network)
- Class B: 172.16.0.0–172.31.255.255 (16 Class B networks)
- Class C: 192.168.0.0–192.168.255.255 (256 Class C networks)

Ip (Internet protoCol) aDdressInG methoDs:

static /Dynamic

Each device in an IP network is either assigned a permanent address (**static**) by the network administrator or is assigned a temporary address (**dynamic**) via DHCP software. Routers, firewalls and proxy servers use static addresses as do most servers and printers that serve multiple users. Client machines may use static or dynamic IP addresses. The IP address assigned to your service by your cable or DSL Internet provider is typically dynamic IP. In routers and operating systems, the default configuration for clients is dynamic IP.

DhCp

DHCP stands for Dynamic Host Configuration Protocol. This protocol assigns network IP addresses to clients on the network at startup. With DHCP, each client workstation does not need to be set up with a static IP address. DHCP is recommended on large networks. It would be very time consuming to manually assign a static IP address to every workstation on your network.

With static IP addressing, the IP address that you assign to a device never changes. A DHCP server contains a pool of IP addresses that it can draw from to assign to devices

that are connecting to the network. Other TCP/IP properties, such as default gateways, DNS servers, and subnet masks can also be assigned automatically.

self-assigned (apiPa (automatic private Internet protocol addressing))

Automatic Private IP Addressing (APIPA) is a feature of Windows-based operating systems (included in Windows 98, ME, 2000, and XP) that enables a computer to automatically assign itself an IP address when there is no Dynamic Host Configuration Protocol (DHCP) server available to perform that function.

Using APIPA, a Windows based client assigns itself an IP address from a range reserved for authorized private class B network addresses (*169.254.0.1 through 169.254.255.254*), with a subnet mask of **255.255.0.0**. A computer with an authorized private address cannot directly communicate with hosts outside its subnet, including Internet hosts.

APIPA is most suitable for small, single-subnet networks, such as a home or small office. APIPA is enabled by default if no DHCP servers are available on the network.

Note APIPA assigns only an IP address and subnet mask; it does not assign a default gateway, nor does it assign the IP addresses of DNS or WINS servers. Use APIPA only on a single-subnet network that contains no routers. If you're small office or home office network is connected to the Internet or a private intranet, do not use APIPA.

subnetting

A subnet is a segment of a network. Subnetting is a technique that allows a network administrator to divide one physical network into smaller logical networks and, thus, control the flow of traffic for security or efficiency reasons.

Dividing a network into several subnets can serve a number of purposes: to reduce network traffic by decreasing the number of broadcasts (if used in combination with a switch), to exceed the limitations in a local area network, for instance the maximum number of allowed hosts, or to enable employees to be able to dial in to the network from home, without opening the entire network up to unwanted visits from the Internet.

Subnets are created by using a so-called subnet mask to divide a single Class A, B, or C network number into smaller pieces, thus allowing an organization to add subnets without having to obtain a new network number through an Internet service provider. Subnets can again be subnetted into sub-subnets.

Subnets were originally invented to help solve the lack of IP addresses on the Internet.

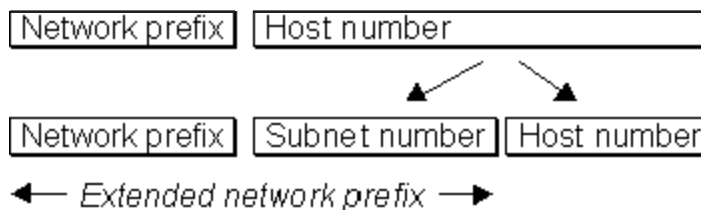
Please note: There is a fast track to getting the advantages of subnetting on local area networks without having to go through the process of calculating a subnet mask, etc.

advantages of subnetting a network include the following:

- Reducing network collision by limiting the range of broadcasts using routers
- Enabling different networking architectures to be joined

how does subnetting work?

An IP address consists of a network portion and a host portion. A subnet is created by borrowing bits from the part of the IP address which normally designates the host and using them to designate one or smaller, secondary networks (subnets) within the original network. The network prefix and subnet number in combination are called the extended network prefix (in every day talk often, somewhat confusingly, referred to as the network number).



subnet masks

A 32-bit subnet mask is used as a deciphering key to determine how an IP address is to be divided into extended network prefix and host part. It is used by routers and network devices to determine where traffic should be routed to.

Like IP addresses, subnet masks consist of four numbers of 8 bits, separated by dots. They are usually written in the corresponding decimal notation.

The typical subnet masks used for Class A, B and C addresses are as follows:

Class A subnet mask:

<i>Decimal</i>	<i>Binary</i>
255.0.0.0	11111111.00000000.00000000.00000000

Class B subnet mask:

<i>Decimal</i>	<i>Binary</i>
255.255.0.0	11111111.11111111.00000000.00000000

Class C subnet mask:

<i>Decimal</i>	<i>Binary</i>
255.255.255.0	11111111.11111111.11111111.00000000

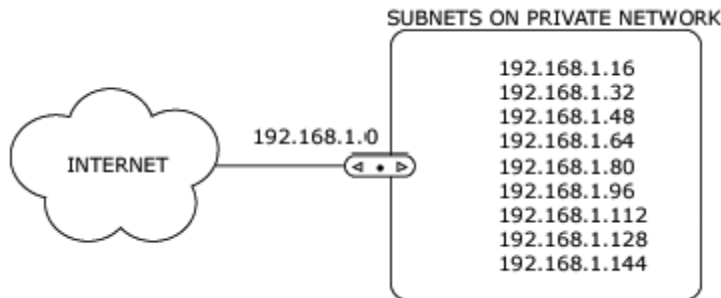
All the 0's in the subnet mask specify that this part in a corresponding IP address is the host portion, while the 1's indicate that the corresponding bits in the IP address constitute the network portion.

The three subnet masks above set the change from network to host portion at the end of a whole octet – Class A after one octet, Class B after two octets, and Class C after three. However, a subnet masks does not have to follow the address classes, but can specify a host portion that is not a whole octet.

The subnet mask 255.255.255.240 (11111111.11111111.11111111.11110000) for instance, marks the breaking point four bits into the last octet.

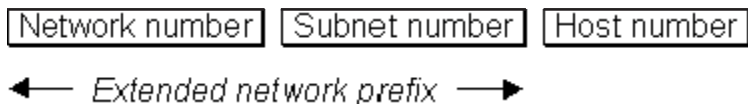
The purpose of having subnet masks defining networks is that the technical devices that the network is build from will be able to determine if traffic should be routed out of the network or kept within it. Using a mask saves the routers from having to handle the entire 32-bit address, because they can simply look at the bits selected by the mask (and thus not worry about the host portion of the address).

Internet routers use only the network number of the destination address to route traffic to a subnetted environment. Subnetting, thus, also has the advantage that it keeps the size of the routing tables on the Internet down because Internet routers only need to know the one common network address for all the individual computers and devices on the different subnets. The route from the Internet to any subnet of a network is the same, no matter which subnet the destination host is on, namely that of the mother network. From there, the local network router(s) divides the communication out into individual subnets and to the individual hosts on these subnets.



Subnetting keeps the size of the routing tables on the Internet down, as the Internet routers only use the network number of a subnetted environment to route traffic to any of the subnets.

A router within a subnetted environment uses the extended network prefix to route traffic between the individual subnets. The extended network prefix is composed of the network prefix and the subnet number.



Calculating a network number using a subnet mask

The network number is the part of the IP address that all hosts on a network share. Network numbers are entered in routing tables and used by routers to direct traffic between networks. The network number, or *extended network prefix*, of an IP address is found by using the subnet mask to mask off the host portion of the IP address.

An example:

You choose the IP address 192.168.1.1 and the subnet mask 255.255.255.0. The above IP address and subnet mask written in their binary notation looks as follows:

192.168.1.1	11000000.10101000.00000001.00000001	
		Network portion → till here
255.255.255.0	11111111.11111111.11111111.00000000	

Every bit in the IP address is compared to the corresponding bit in the subnet mask: a '1' in the subnet mask indicates that the corresponding bit in the IP address is part of the network portion, while a '0' in the subnet mask illustrates that the corresponding bit in the IP address is part of the host portion.

In the above example, the host portion is thus all the bits in the first three octets, which in decimal numbers is written 192.168.1.0.

Subnet masks written in binary notation always consist of a continuous string of 1's followed by a continuous string of 0's, e.g.

11111111.11111111.11111111.00000000 or
11111111.11110000.00000000.00000000

As a consequence, the host range that a subnet mask defines will always be either 2 (2^1 – corresponding to a situation where only the last bit defines hosts), 4 (2^2 – corresponding to a situation where the last two bits define hosts), 8 (2^3), 16 (2^4), 32 (2^5), 64 (2^6), 128 (2^7) or 256 (2^8).

In reality, 2 must be subtracted from all the numbers of hosts above to get the actual number of IP addresses available to use for hosts, because two addresses, namely the address which has all-0's in the host bits (this network) and the address which has all 1's in the host bits (broadcast), cannot be assigned to hosts. As a consequence, it is not possible to make a network that consists of fewer than four IP addresses (2 hosts + the broadcast and network addresses).

In the above example, based on the IP address 192.168.1.1 and the subnet mask 255.255.255.0, the network address (all host bits set to 0) was 192.168.1.0. The broadcast address for this network would be 192.168.1.255 as illustrated below.

Calculating a broadcast address using a subnet mask

The broadcast address is the address where all the bits in the host portion are set to 1. The broadcast address is used when you want to communicate data to all the hosts on a network. Here follows an example of how it can be calculated:

In our example above, the last 8 bits were hosts. As a consequence, the broadcast address for the network 192.168.1.0 with the subnet mask 255.255.255.0 is 11000000.10101000.00000001.11111111 (host bits set to 1) or in decimal notation: 192.168.1.255

Note: If you know the IP address segment your network consists off, the lowest IP address is the network number, while the highest IP address is the broadcast address.

Prefix length notation (CIDR notation)

For the sake of convenience, prefix length notations (CIDR notation, Classless Inter-Domain Routing notation) is often used instead of writing the subnet mask. This means that the IP address above (192.168.1.1) with the subnet mask 255.255.255.0 can also be expressed as 192.168.1.1/24. The /24 indicates the network prefix length, which is equal to the number of continuous one-bits in the subnet mask.

192.168.1.1	11000000.10101000.00000001.00000001
255.255.255.0	11111111.11111111.11111111.00000000
<i>equals</i>	
192.168.1.1/24	11000000.10101000.00000001.00000001

Calculating a subnet mask

When subnetting a network, you first need to determine two things:

- How many subnets do you need to create?
- How many host addresses do you need on each net (you should always add some extra host addresses to be used for future growth).

Once you have determined the required number of subnets and hosts, the next step is to calculate a corresponding subnet mask, which will support the desired network structure.

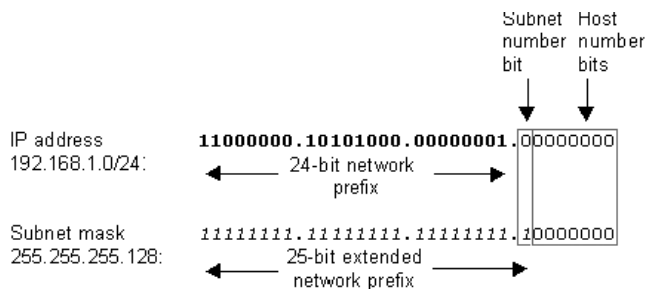
In the following you will find two examples of how the subnetting of a Class C network can be planned and the required subnet mask calculated.

Example A:

Imagine that you are setting up a network on the network number 192.168.1.0/24. You need a local area network which is going to connect a number of workstations, servers and others devices, totaling more than 80. To allow some slack, you set the number of required hosts to be 90. Now, the calculation of the subnet mask can begin. The calculation is best understood if the numbers are looked at in their binary form (see example below).

The first step is to determine the lowest number of bits required to identify 90 hosts. Since IP addresses of hosts can only be created along binary boundaries, the number of hosts must be created in blocks of powers of two – 2 (2^1), 4 (2^2), 8 (2^3), 16 (2^4) and so on. In other words, we must first determine what the lowest power is that we can lift 2 to and get a number equal to or greater than 90. Since 2^7 equals 128 and 2^6 equals 64, we need 7 bits to designate 90 hosts. This means that the host portion of the IP address must be the last 7 bits. An IP address consists of 32 bits all in all. The network portion must thus consist of $32-7=25$ bits. As every '1' in a subnet mask indicates that the corresponding bit in the IP address belongs to the network portion and every '0' indicates that the corresponding bit in the IP address is part of the host portion, the corresponding subnet mask must consist

of a series of 25 1's, followed by 7 0's (as illustrated below). Written in decimal notation, the subnet mask is 255.255.255.128.



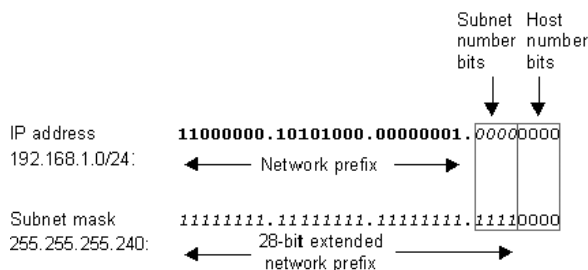
The number of subnets that can be created using this subnet mask is calculated as follows: The original network prefix was 24 bit long (192.168.1.0/24), and the extended network prefix (network prefix + subnet prefix) masked off by the subnet mask is 25 bits long. As a consequence, one bit is available to designate subnets. In other words, it is possible to create 2 (2¹) subnets of this given size using this subnet mask, should we wish to do so.

Example B:

Now pretend that through an estimation of the number of subnets and hosts that the subnet you are setting up will have to support, you have come to the conclusion that you need to define ten subnets. The largest subnet is required to support 10 hosts. You have again chosen to create the subnet on the network number 192.168.1.0/24. Now, the calculation of the subnet mask can begin.

The first step is to determine the number of bits required to define the ten subnets. Since a network address can be subnetted only along binary boundaries, subnets must be created in blocks of powers of two 2 – 2, 4, 8, 16 and so on. Thus, it is impossible to define an IP address block so that it contains exactly ten subnets. In this case, the network administrator must define a block of 16 (2⁴) and have six unused subnet addresses for future growth.

Since we need to raise 2 to the power of four (2⁴) to get 16, four bits are required to designate the sixteen subnets in the block. In this example, you are subnetting a Class C network (/24) so it will need four more bits (/28) as the extended network prefix. A 28-bit extended network prefix can be expressed in dotted-decimal notation as 255.255.255.240. This is illustrated below:



A 28-bit extended network prefix leaves 4 bits to define host addresses on each subnet. This means that each subnet with a 28-bit prefix represents a continuous block of 2^4 (16) individual IP addresses. However, since the all-0 ('this network') and the all-1's host addresses ('broadcast') must not be allocated, there are 14 (2^4-2) assignable host addresses on each subnet. We needed a maximum of 10 hosts on each subnet, so the result is satisfactory.

Defining subnet numbers

In example B above, with the ten subnets, the subnets will be numbered 0 through to 9. The 4-bit binary representation of the decimal values 0 through 9 are: 0 (0000), 1 (0001), 2 (0010), 3 (0011), 4 (0100), 5 (0101), 6 (0110), 7 (0111), 8 (1000), 9 (1001), 10 (1010).

To find the subnet number of each subnet, place the binary representation of the subnet number, e.g. 0001, into the bits in the base network address that is used to designate the subnet (see illustration below). For example, to define subnet number 8, the network administrator places the binary representation of 8 (1000) into the 4-bits in the base network address that are used to designate the subnet.

The ten subnet numbers for the example are given below. The italicized portion of each address identifies the extended network prefix, while the bold digits identify the 4 bits representing the bits in the address that are used to designate the subnet:

```

Base
network: 11000000.10101000.00000001.00000000 = 192.168.1.0/24
Subnet
number 0: 11000000.10101000.00000001.00000000 = 192.168.1.0/28
number 1: 11000000.10101000.00000001.00010000 = 192.168.1.16/28
number 2: 11000000.10101000.00000001.00100000 = 192.168.1.32/28
number 3: 11000000.10101000.00000001.00110000 = 192.168.1.48/28
number 4: 11000000.10101000.00000001.01000000 = 192.168.1.64/28
number 5: 11000000.10101000.00000001.01010000 = 192.168.1.80/28
number 6: 11000000.10101000.00000001.01100000 = 192.168.1.96/28
number 7: 11000000.10101000.00000001.01110000 = 192.168.1.112/28
number 8: 11000000.10101000.00000001.10000000 = 192.168.1.128/28
number 9: 11000000.10101000.00000001.10010000 = 192.168.1.144/28

```

An easy way to ensure that the subnets are calculated correctly is to ensure that they are all multiples of the subnet number 1 address. In this case, all subnets are multiples of 16.

assigning ip address in windows os

Each computer in a network has its own internal IP address. That IP address may be **static**, which means that it never changes. Or, as is likely if you share an Internet connection with other computers, the internal IP address may be assigned dynamically and may change from time to time.

Note: in a network configuration, the internal IP is not the same as the IP assigned by your ISP. The IP assigned by your ISP can be either static or dynamic.

When you are opening ports to allow incoming connections to your computer, your computer must be assigned a static internal IP address, to ensure that the incoming connections always go to the correct computer.

there are several steps:

- See your current IP address
- Choose a static IP address
- Assign the static IP address

Current Ip address

Find your current IP address and whether it is **static** or **dynamic**:

1. Open Windows **start** menu.
2. Select **run**. Type: **command** and click **OK**.
3. At the blinking cursor, type: **ipconfig /all** and press Enter.
4. Look for these entries near the end of the list:
 - **Dhcp Enabled**. No means your IP address is static. Yes means it is dynamic.
 - **IP Address**. This is your current IP address.
5. To exit, at the blinking cursor, type: **exit** and press Enter.

If you're current Ip address is:

- **static**, then make note of the IP address. You need the IP address when you open ports in your router or firewall.
- **Dynamic**, then assign a static IP address instead.



Choose an Ip address

Choose an IP address, and collect other information needed in order to assign a static IP address to your computer.

1. In your router administration program, find and remember this information:
 - Router (Gateway) IP address
 - Subnet Mask
 - IP addresses of your DNS servers
2. In your router administration program, find an IP address that can be assigned as a static IP. The address:
 - Must not be one that might be assigned to someone as a dynamic address.
 - Must not be one that has been assigned to another device (often these are the low numbers).
 - Must be lower than the range of dynamic addresses.

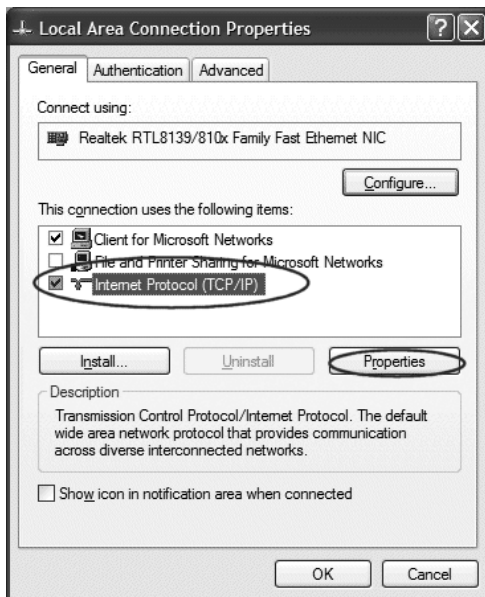
assign the Ip address

To set a static IP address:

1. Open Windows **start** menu.
2. Open **Control panel**.
3. Classic view: Open **network Connections**
4. Category view: Select **network and Internet Connections**, and then **network Connections**.
5. Double-click on your active **lan or Internet connection**.
6. Click **properties**.

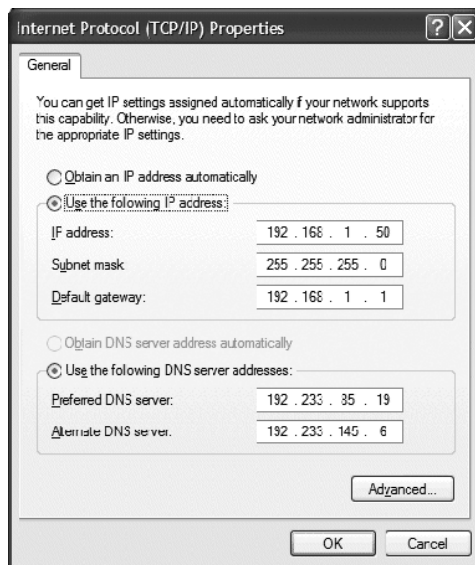
This opens the Local Area Connections Properties window.

6. In the **General** tab, highlight the **Internet protocol (TCP/IP)** item, and click **properties**.



This opens the Internet Protocol (TCP/IP) Properties window.

7. In the General tab, click **Use the following Ip address**, and enter:
 - IP address. The static IP address you want to assign to this computer.
 - Subnet mask. Subnet mask used by your router.
 - Default gateway. IP address of your router’s default gateway.



8. In **Use the following Dns server addresses**, enter all the IP addresses for the DNS servers your router uses.
9. Click **OK**.

Then:

10. Click **OK** to close each window.
11. Restart your computer.
12. Then, **check your Ip address again**, to make sure that the changes were applied.

Share files and folders over the network.


BY SHARING YOUR COMPUTER'S RESOURCES

such as its files and folders, you let other people who use your computer and other people on your network use these resources. With the Windows Vista operating system, sharing your files and folders with other users—either locally or over the network—is simple and straightforward.

This article shows you how browsing through a network folder is just like browsing through a folder on your hard disk. The information that follows includes: sharing files with public folders, sharing files and folders from any folder, using advanced sharing to create shorter network paths, stopping or changing sharing of a file or folder, setting advanced sharing properties, and how share permissions and NTFS permissions work together.


Sharing files with public folders

To share items in your Public folder and its subfolders with other users of your computer, you don't need to do a thing. By default, all users with an account on your computer can log on and create, view, modify, and delete files in the Public folders. The person who creates a file in a Public folder (or copies an item to a Public folder) is the file's Owner and has Full Control access. All others who log on locally have Modify access.

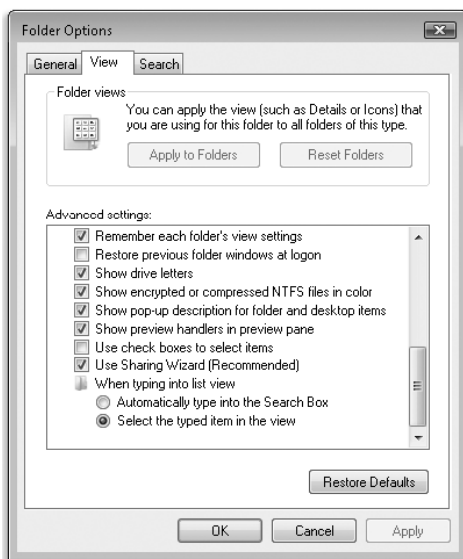
To share items in your Public folder with network users, click the **start** button , click **network**, and then click **network and sharing Center**. Turn on Public Folder Sharing (for information on how to do this, see **sharing files with the public folder**). You can't select which network users get access, nor can you specify different access levels for different users. Sharing via the Public folder is quick and easy—but it's rigidly inflexible.

Sharing files and folders from any folder

Whether you plan to share files and folders with other people who share your computer or with those who connect to your computer over the network (or both), the process for setting up shared resources is the same as long as the Sharing Wizard is enabled. We recommend that you use the Sharing Wizard even if you normally disdain wizards. It's quick, easy, and almost certain to make all of the correct settings for network shares and NTFS permissions—a sometimes daunting task if undertaken manually. Once you've configured shares with the wizard, you can always dive in and make changes manually if you want.

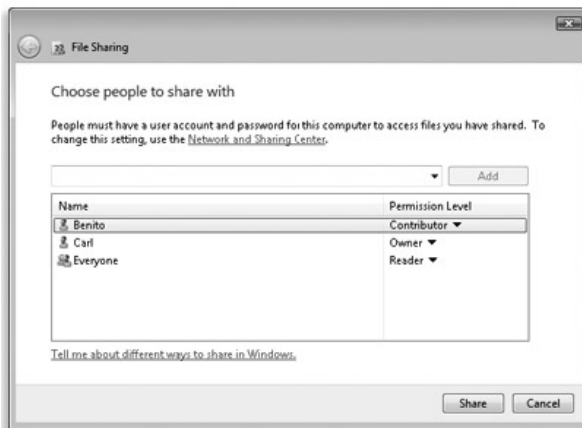
To make sure the Sharing Wizard is enabled, click the **start** button  , type “folder” in the **search** box, and then click **Folder options**. Click the **View** tab. In the **advanced settings** box, scroll down the list and make sure the **Use sharing Wizard (recommended)** check box is selected.

the process for setting up shared resources is the same as long as the sharing Wizard is enabled



With the Sharing Wizard at the ready, follow these steps to share files or folders:

1. In Windows Explorer, select the folders or files you want to share. (You can select multiple objects.)
2. In the Command bar, click **share**. (Alternatively, right-click, and then click **share**.)



With the Sharing Wizard, it's quick and easy to share files or folders with other people

3. In the file sharing box, enter the name of the user with whom you want to share files or folders, and then click **add**. You can type a name in the box or click the arrow to display a list of available names. Repeat for each person you want to add.

The list includes all of the users who have an account on your computer, plus everyone. If you want to grant access to someone who doesn't appear in the list, you need to create a user account for that person (for information on how to do this, see **Create a user account**).

note:

If you select **everyone**, and you have password-protected sharing enabled, the user must still have a valid account on your computer. However, if you have turned off password-protected sharing, network users can gain access only if you grant permission to everyone or to Guest.

4. For each user, select a permission level. Your choices are:

Reader. Users with this permission level can view shared files and run shared programs, but cannot change or delete files. Selecting **reader** in the Sharing Wizard is equivalent to setting NTFS permissions to Read & Execute.

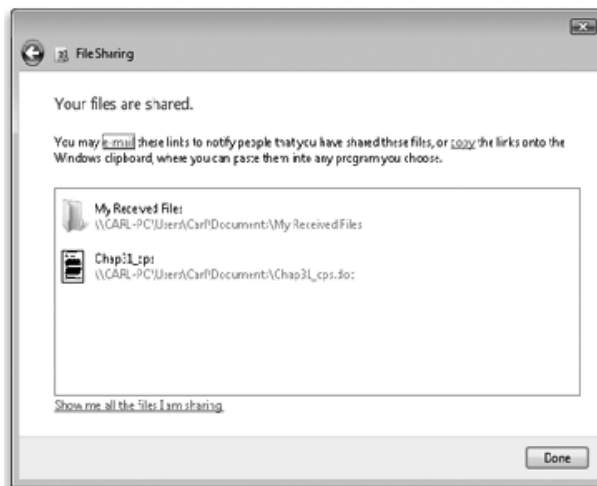
Contributor. This permission level, which is available only for shared folders (not shared files), allows the user to view all files, add files, and change or delete files that the user adds. Selecting **Contributor** sets NTFS permissions to Modify.

Co-owner. Users who are assigned the Co-owner permission have the same privileges that you do as the Owner: They can view, change, add, and delete files in a shared folder. Selecting **Co-owner** sets NTFS permissions to Full Control for this user.

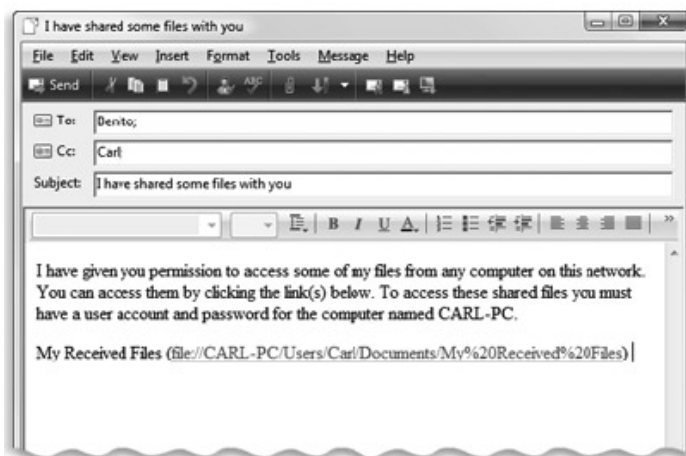
You might see other permission levels if you return to the Sharing Wizard after you set up sharing. The Custom permission level identifies NTFS permissions other than Read & Execute, Modify, and Full Control. The Mixed permission level appears if you select multiple items, and those items have different sharing settings. Owner, of course, identifies the owner of the item.

5. Click **share**. After a few moments, the wizard displays a page similar to the page shown in the following illustration.

the sharing Wizard displays the network path for each item you've shared



6. In the final step of the wizard, you can do any of the following:
- Send an e-mail message to the people with whom you're sharing. The message includes a link to the shared file or folder.



- *With the Sharing Wizard, you can send a message that includes a link to the item you want to share*
- Copy the network path to the Clipboard. This is handy if you want to send a link via instant messenger or another application.
- Double-click a share name to open the shared item.
- Open a search folder that shows all of the folders or files you're sharing.

7. When you're finished with these tasks, click **done**.

Creating a share requires privilege elevation. But, after a folder has been shared, the shared folder is available to network users no matter who is logged on to your computer—or even when nobody is logged on.

Using advanced sharing to create shorter network paths

Confusingly, when you share one of your profile folders (or any other subfolder of %SystemDrive%\Users), Windows Vista creates a network share for the Users folder—not for the folder you shared. This isn't a security problem; NTFS permissions prevent network users from seeing any folders or files except the ones you explicitly share. But it does lead to some long UNC paths to network shares.

For example, if you share the My Received Files subfolder of Documents (as shown after step 5 in the previous section), the network path is \\CARL-PC\Users\Carl\Documents\My Received Files. If this same folder had been anywhere on your computer outside of the Users folder, no matter how deeply nested, and the network path would instead be \\CARL-PC\My Received Files. Other people to whom you've granted access wouldn't need to click through a series of folders to find the files in the intended target folder.

Network users, of course, can map a network drive or save a shortcut to your target folder to avoid this problem. But you can work around it from the sharing side, too: Use advanced sharing to share the folder directly. (Do this after you've used the Sharing Wizard to set up permissions.)

Make sure the share name you create doesn't have spaces. Eliminating spaces makes it easier to type a share path that works as a link.

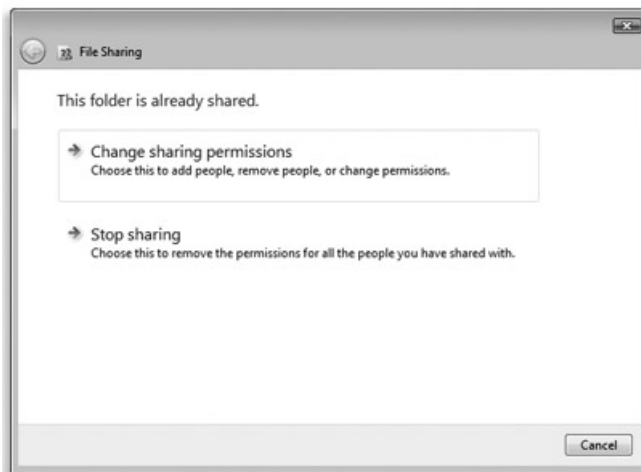
Stopping or changing sharing of a file or folder

If you want to stop sharing a particular shared file or folder, select it in Windows Explorer, and then click **share**. The Sharing Wizard appears, as shown in the following illustration.

Use the sharing Wizard to change sharing permissions or to stop sharing a file or folder

If you click **Change sharing permissions**, the wizard continues as when you created the share, except that all existing permissions are shown. You can add or remove names and change permissions.

The **stop sharing** option removes access control



entries that are not inherited. In addition, the network share is removed; the folder will no longer be visible in another user's Network folder.

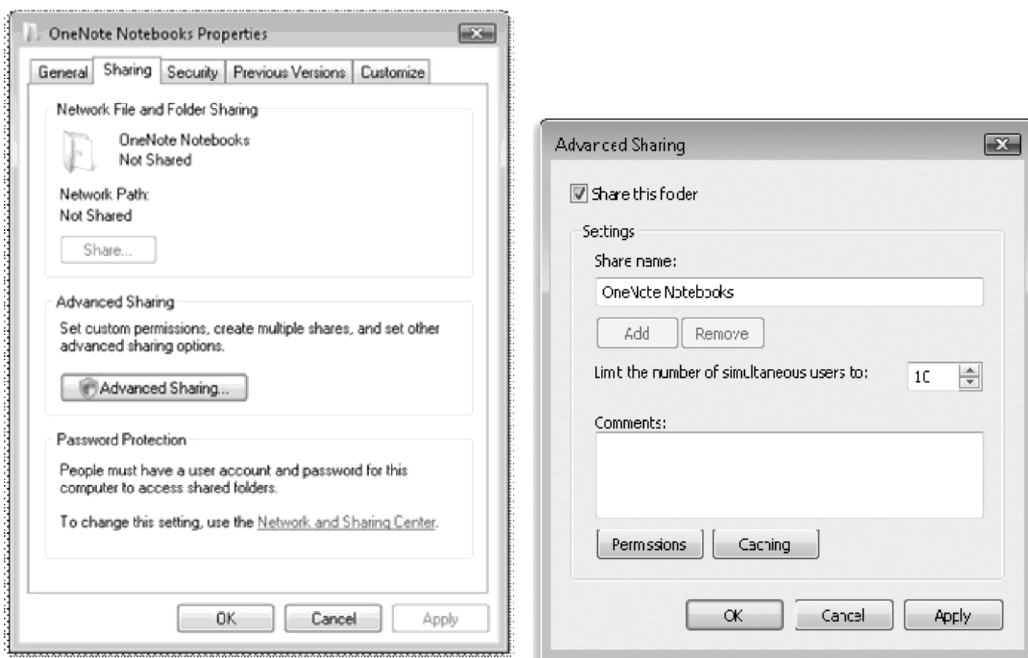
setting advanced sharing properties

If you disable the Sharing Wizard, Windows Vista reverts to a process similar to that employed by earlier versions of Windows (except the aberration in Windows XP called Simple File Sharing—nothing before or after is similar to that). Without the Sharing Wizard, you configure network shares independently of NTFS permissions.

With the Sharing Wizard disabled, when you select a folder, and then click **share**, rather than the wizard appearing, Windows opens the folder's properties dialog box and displays the **sharing** tab, as shown in the next illustration. Even with the Sharing Wizard enabled, you can get to the same place; right-click the folder, and then choose **properties**.

The Sharing tab is part of the properties dialog box for a folder, but not for files. Also, when the Sharing Wizard is disabled, the Share button appears on the Command bar only when you select a single folder. Only the Sharing Wizard is capable of making share settings for files and for multiple objects simultaneously.

The Share button summons the Sharing Wizard, but it's available only when the Sharing Wizard is enabled



Use advanced settings to create or modify a network share

To create or modify a network share using advanced settings, follow these steps:

1. On the **sharing** tab, click **advanced sharing**.
2. Select the **share this Folder** check box.
3. Accept or change the proposed share name.

If the folder is already shared, and you want to add another share name (perhaps with different permissions), click **add**, and then type the name for the new share. The share name is the name that other users will see in their own Network folders. Windows initially proposes to use the folder's name as its share name. That's usually a good choice, but you're not obligated to accept it. If you already have a shared folder with that name, you'll need to pick a different name.

4. Type a description of the folder's contents in the **Comments** box. Other users will see this description when they inspect the folder's properties dialog box in their Network folder (or when they use the Details view).
5. To limit the number of users who can connect to the shared folder concurrently, specify a number in the **limit the number of simultaneous users** box. Windows Vista permits up to 10 concurrent users. (If you need to share a folder with more than 10 users at once, you must use a server version of Windows.)
6. Click **permissions**.

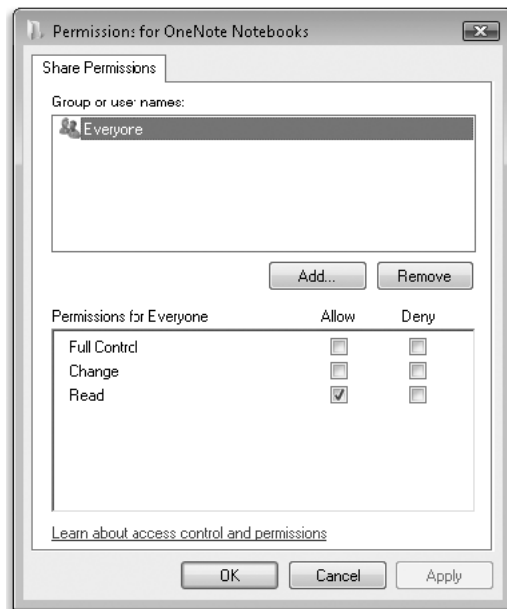
The default share permission associated with a new share is Read access to Everyone

Caution

When you share a folder, you also make that folder's subfolders available on the network. If the access permissions you set for the folder aren't appropriate for any of its subfolders, either reconsider your choice of access permissions or restructure your folders to avoid the problem.

7. In the **Group or user names** box, select the name of the user or group you want to manage. The share permissions for the selected user or group appear in the permissions box.
8. Select **allow**, **Deny**, or neither for each access control entry:

- *Full Control*. Allows users to create, read, write, rename, and delete files in the folder and its subfolders. In addition, users can change permissions and take ownership of files on NTFS volumes.



- *Change*. Allows users to read, write, rename, and delete files in the folder and its subfolders, but not create new files.
- *Read*. Allows users to read files but not write to them or delete them. If you select neither **allow** nor **Deny**, it is still possible that the user or group can inherit the permission through membership in another group that has the permission. If the user or group doesn't belong to another such group, the user or group is implicitly denied permission.
- To remove a name from the **Group or user names** box, select the name, and then click **remove**. To add a name to the list, click **add**. Enter the names of the users and groups you want to add.

9. Click **OK** in each dialog box.

how share permissions and ntfs permissions work together

The implementation of share permissions and NTFS permissions is confusingly similar, but it's important to recognize that these are two separate levels of access control. Only connections that successfully pass through both gates are granted access.

Share permissions control network access to a particular resource. Share permissions do not affect users who log on locally. You set share permissions in the Advanced Sharing dialog box, which you access from the Sharing tab of a folder's properties dialog box.

NTFS permissions apply to folders and files on an NTFS-formatted drive. They provide extremely granular control over an object. For each user to whom you want to grant access, you can specify exactly what they're allowed to do: run programs, view folder contents, create new files, change existing files, and so on. You set NTFS permissions on the Security tab of the properties dialog box for a folder or file.

It's important to recognize that the two types of permissions are combined in the most restrictive way. If, for example, a user is granted Read permission on the network share, it doesn't matter whether or not the account has Full Control NTFS permissions on the same folder; the user gets only Read access when connecting over the network.

In effect, the two sets of permissions act in tandem as gatekeepers that winnow out incoming network connections. An account that attempts to connect over the network is examined first by the share permissions gatekeeper. The account is either bounced out on its caboodle or allowed to enter with certain permissions. It's then confronted by the NTFS permissions gatekeeper, which might strip away (but not add to) some or all of the permissions granted at the first doorway.

In determining the effective permission for a particular account, you must also consider the effect of group membership. Permissions are cumulative; an account that is a member of one or more groups is granted all of the permissions that are granted explicitly to the account as well as all of the permissions that are granted to each group of which it's a member. The only exception to this rule is Deny permissions, which take precedence over any conflicting Allow permissions.

Chapter – 8

Configuring LaN Network

Workgroup vs Domain

Networking in Windows means that you would need to setup a domain or a workgroup so that all the computers connected can communicate with each other. Whether you have a domain or a workgroup is all up to your network administrator and the scale of your network. Workgroups are used when there are only a few computers in the same location that needs to be connected. Domains, on the other hand, are meant for large scale deployments where there are dozens of computers connected to the network. Even computers from outside the location can connect to the domain with the use of VPN technologies.

Workgroups are substantially easier to create compared to domains. You would simply need to connect two computers to a switch and assign them to the same workgroup; you already have a working workgroup. In order to have a domain implemented, you would need to set-up a domain controller which is the computer that authenticates and users who wants to connect and provides them the resources that are afforded them. The domain controllers are also essential in adding an extra layer of security for the system beyond the normal usual security from individual computers which is what's available in workgroups.

Although it is harder to implement a domain compared to a workgroup, it adds better scalability to the whole system which is essential for the expansion of businesses. Adding accounts or computers in a workgroup would mean that each computer needs to be configured for each account, this is time consuming and cumbersome especially when the computers number in the dozens. In a domain, the administrator can do all this on a single terminal in a very short time. Aside from scalability, domains are also very structured and you can assign what services or folders a specific account can access. This feature is not available in workgroups and anyone connected to the workgroup can access the same services and resources.

Summary:

1. Workgroups are fitted for smaller networks while Domains are used in large scale deployments like in medium and big businesses
2. Workgroups are easy to implement while domains are harder and takes longer to implement
3. The control in a domain is centralized to the domain controller which is safer while workgroups do not have this level of protection
4. Domains are very scalable while increasing the number of computers and users in a workgroup could be a lot of work
5. You can assign resources to certain accounts in domains but not in workgroups

Configure peer to peer workgroup network Step by Step Guide

Here are numerous types of network available. We will go through most of them as per certificate program require. We will start from N+. Although N+ exam don't held in practical mode as RHCE. Still it requires minimum nine months hand on experience. So if you are planning to take N+ exam be careful about practical. Here we will take a scenario.

Your boss told you that he want set up a new office where security is not a major concern what all you are supposed to do is to meet this requirement in less budget.

how will you set up this workgroup network?

- Determine your requirements
- Choose between wired and wireless media
- Map your physical network
- Map your logical network
- Create a utilization plan

We assume that you have gone through these steps and come with a plan to use 4 computers with star topology for this network.

Computers	4 With any descriptive Name
Operating system	Windows XP Professional and Vista
topology	Star
printer	One
Modem	One
Workgroup Name	Mouse

Now follow these steps:-

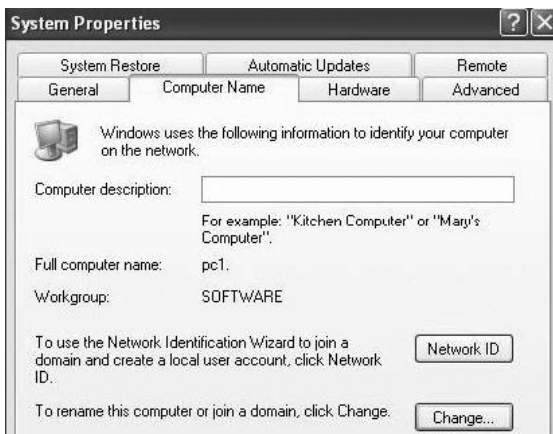
Install XP and Vista on all four computers.

Change the Name of Your Computer and workgroup When you first install windows assign itself a computer name something that looks like RAT12E2341, now would be a good time to give your computer a descriptive name:

Right-click on My Computer and select Properties, or open the System applet in the Control Panel.



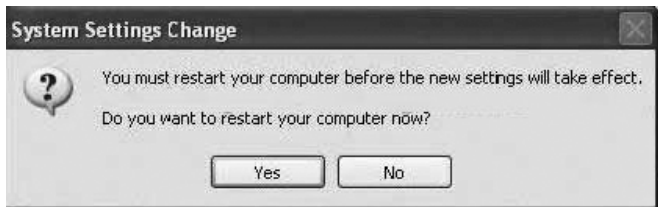
Select the Computer Name tab ==> click Change to open the Computer Name Changes dialog box.



Enter a new computer name in the Computer Name field and new workgroup name in Workgroup field and click OK.



You will be prompted to restart your computer to complete the name change. Click yes to restart your computer.



to avoid future problem follow these simple rules in choosing name

1. Computer name should be unique in a workgroup.
2. Workgroup name should be same for all computers.
3. Workgroup names may be up to 15 characters long and may contain any alphanumeric (a-z and 0-9) characters, as well as special characters except for ; : " < > * + = \ | ?.
4. Computer names can be up to 15 characters long and have the same naming restrictions as workgroups. In addition, the computer name cannot be the same as the workgroup name.

Next step is checking of LAN card that will be done first in Device manager and further in my network place → properties

LaN card in device manager

Right Click on My Computer → properties → Hardware → Device manager → Network Adaptor → Check here (also check under the other devices tag)

Situation: - Showing



Description:- Installed and working properly Situation:-Showing with Yellow sign



Description: - LAN card driver is corrupted

Solution: - *Install* LAN card driver.

Situation: - Showing with Red Cross

Description: - Either *cab/e* is unplugged or LAN card is disabled

Solution: - My network places → properties → local area connection → right click → Enable (Follow only if LAN card is disable)

Check whether network cable is plugged or not

Situation: - Not Showing



Description: - LAN card is not detected yet (Check for physical installation)

Solution: - Open the cabinet and check for physical detection

Check Bios → On board Lan Option should be enabling

Checking LaN card in Network place

How to show my network place on Desktop?

Right click on the free space of desktop → Customize desktop → check mark on my network places → Apply → Ok

My network place → properties → local area connection Situation: - Showing



Description: - Installed and working properly Situation:-Showing with red Cross



Description:-cable is unplugged

Solution:-Check whether network cable is plugged or not

Situation:-Showing with Yellow sign

Description:-LAN is working on Automatic private IP.

Solution: - assign manually IP address

Situation:-Showing with disable



Description:-LAN is disabled

Solution:-My network places → Local area connection → Right click → Enable (Follow only if LAN card is disable)

Situation:-Showing with firewall



Description:-LAN is firewall protected

Solution:-There is no need to on firewall unless you are connecting with internet.

To turn off firewall. My network place → properties → local area connection → properties →Advanced →Settings



General → Off**Next step is to check for these 4 necessary things**

- LAN cards drives
- Client for Microsoft network
- File and printer sharing services
- Internet protocols (TCP/IP)

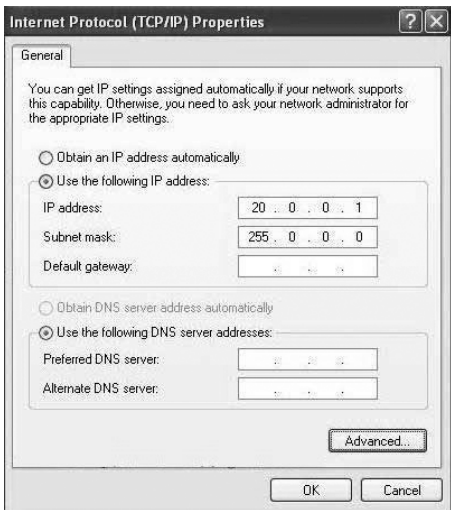


If you don't found any of these here and then install that by using install button before going further Once you have completed these steps then go to our next article.

In the first part of this article series, I showed you how to prepare for peer to peer workgroup networking. Now that the perquisite to configure the peer to peer workgroup network has been completed.

Now it's time to configure Ip address

Select the Internet Protocol (TCP/IP) and click Properties. You will be presented with the following dialog box:



Select the Use the Following IP Address option and configure the IP addresses you have been assigned by your company or you have chosen for your network

	PC1-LAN1	PC1-LAN2	PC2	PC3	PC4
IP address	192.168.1.2	192.168.1.3	192.168.1.4	192.168.1.5	192.168.1.6
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.1	192.168.1.1	192.168.1.3	192.168.1.3	192.168.1.3
Preferred DNS server	202.56.224.153	202.56.224.153	192.168.1.3	192.168.1.3	192.168.1.3
Alternate DNS server	202.56.230.6	202.56.230.6	-----	-----	-----

Important: - for your DNS Server Ip please contact your ISP

You have given your computer a unique address that will allow it to communication your network.

Keep these things always in minds whenever you deal with IP address to make communications between two computers:-

1. Network address must be same and host address must be difference
2. If network address is difference a Router will be require to make communications

Next Step: - run Set up a home or small office Network Wizard



XP have a nice feature to make your tasks much easier called set up a home or small office network wizard. By This wizard you can share internet connection, set up windows firewall. Share printer, share file and folder. To run this wizard

My Network place → properties → Set up a home or small office network wizard → Click on Next

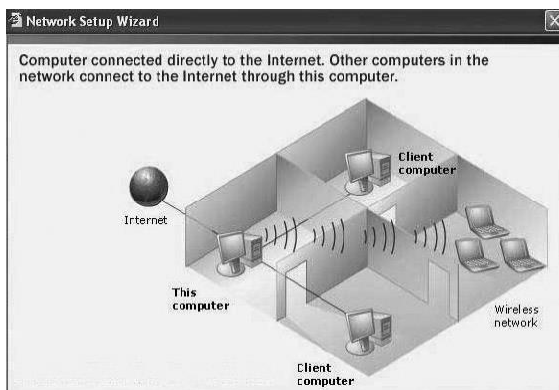
here you are asked to check all necessary components



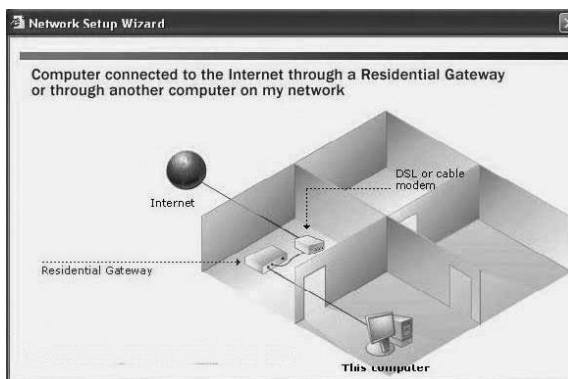
In this step select the statements that meet your internet requirement



You should choose first option when your computer is directly connected to internet as shown in figure



You should choose second option when your computer is connected to internet via other computer as shown in figure



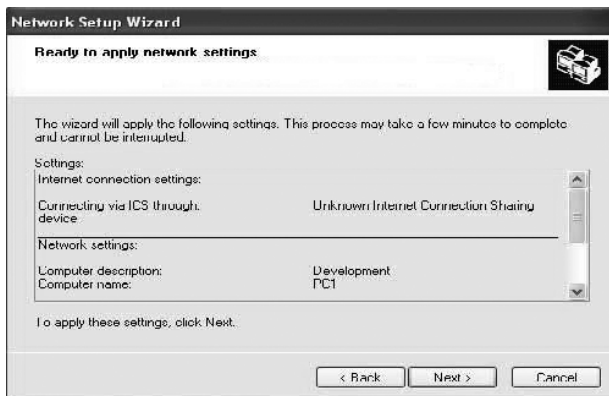
In this step you can change computer name (Not recommended, for this use my computer's properties)



Now set correct workgroup name (Default will be MShOME)



this is the summary of options you have selected if you have made any mistake go back and correct



Wizard is setting up your workgroup



Choose last options to finish this wizard



Click on finish



as the system setting has changed you should be prompt for restart Click on yes



Once you have completed these steps you are ready to move on second part towards completing Peer to Peer Workgroup Network set up.

In the first part of this article series, I showed you how to prepare for peer to peer workgroup networking. And in second article I show you how to use Xp' inbuilt setup home and small office wizard now it's time to configure Vista.

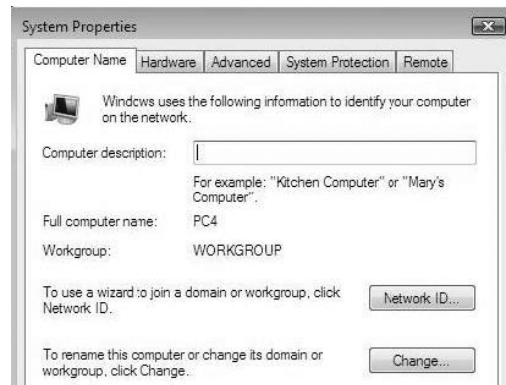
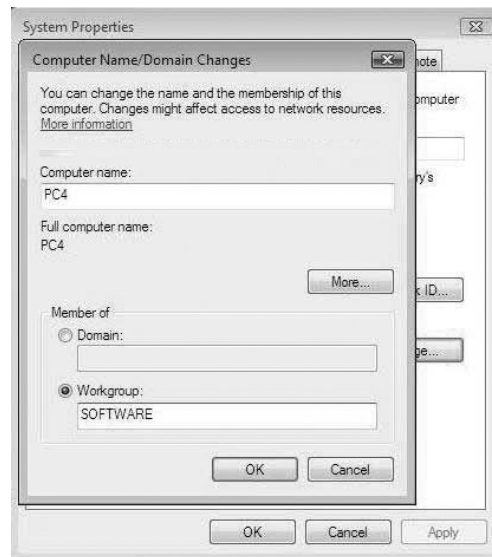
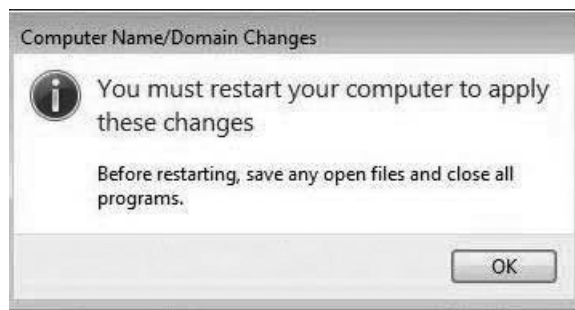
On Windows 7 Follow these Steps

On Desktop → Select My Computer → right Click → Select properties

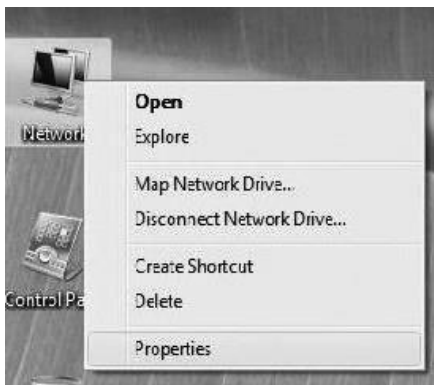


Select Change Setting (administrative permission will be require)

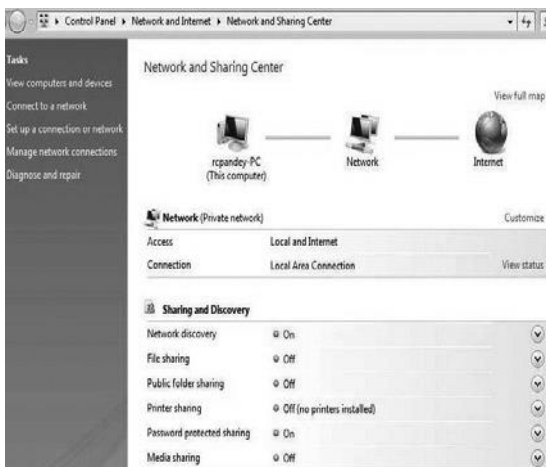


Click on Change**Change Computer name and workgroup name as per guide line given above.****Save the change (reboot will require)**

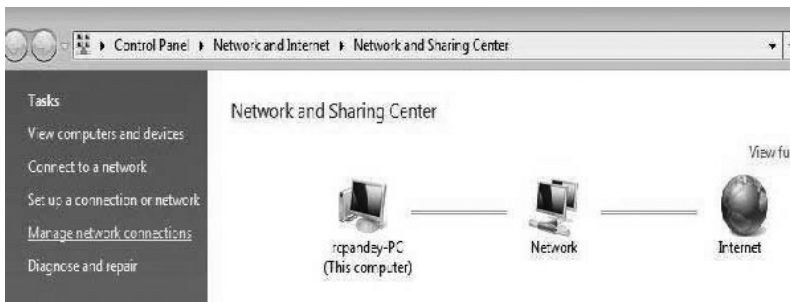
after reboot → right Click on My Network place → properties



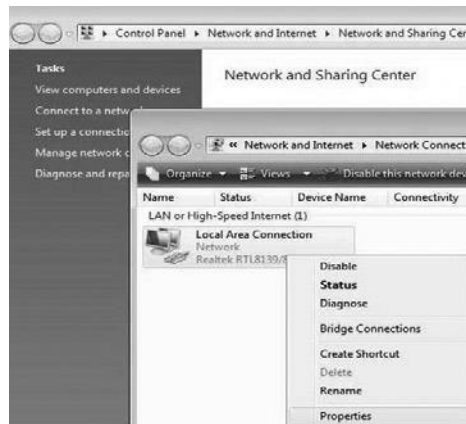
Now turn on Network discovery, File sharing, printer Sharing



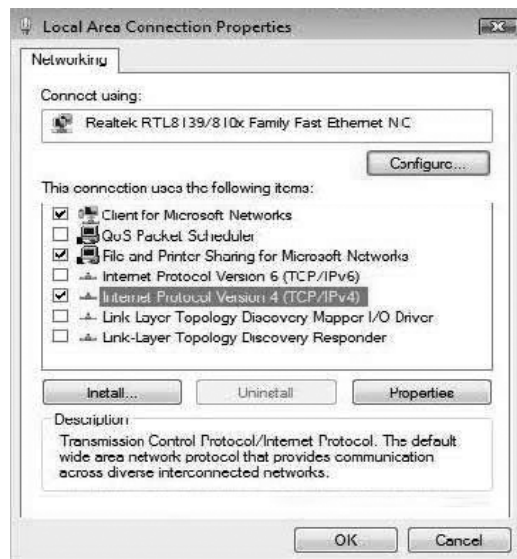
Click on Manage network connections



Select Local area Connection → properties (all possible situation of LaN card will be same as Xp)



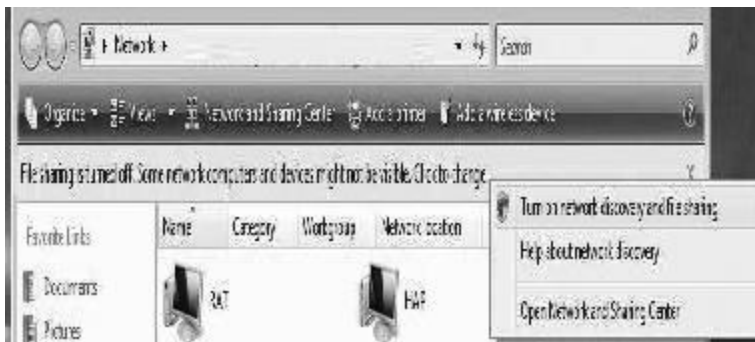
By Default vista will include More options used for Ipv6 (Just uncheck these options) select Internet protocol version 4 (TCP/IPv4) → properties



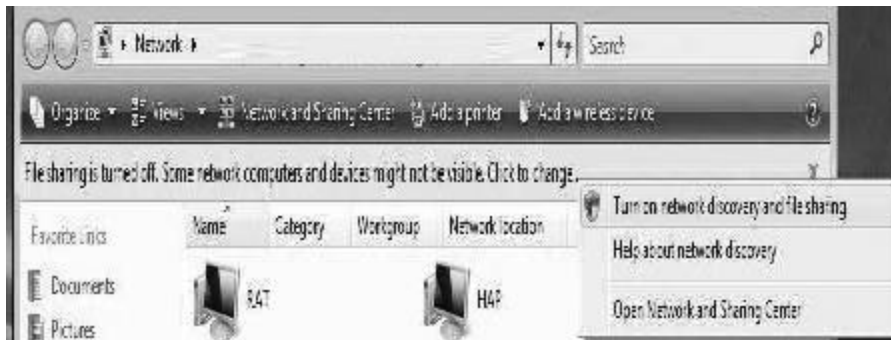
now give the Ip address → ok → ok



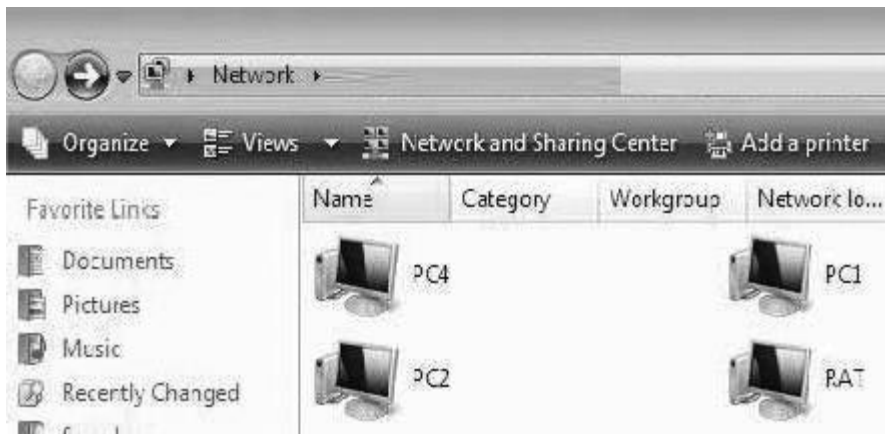
Now open My network place → Click to change



Select Turn on network discovery and file sharing



If you can see all your computer in my network place then its times to cheers you have successfully configured workgroup

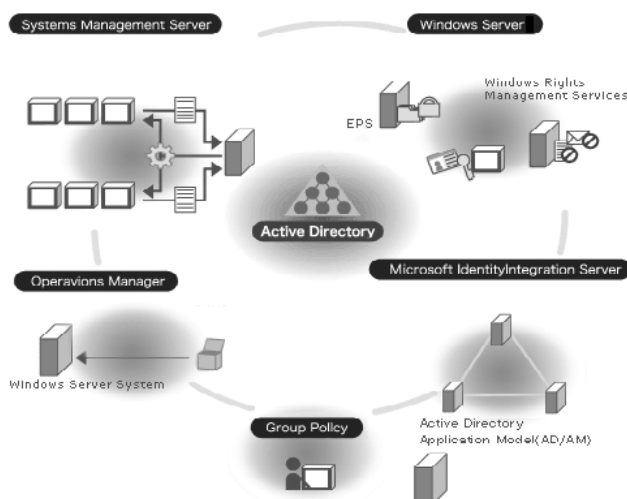


Chapter - 9

DNS, active Directory Services Configuration

Introduction:

An active directory is a directory structure used on Microsoft Windows computers and servers to store information about networks and domains. It is primarily used for online information and was originally created in 1996. It was first used with Windows 2000. An active directory (sometimes referred to as an AD) has many functions. It provides information on objects, organizes these objects for easy retrieval and access, allows users and administrators to access it, and allows the administrator to set security up for the directory. An active directory can be defined as a hierarchical structure. This structure is usually broken up into three main categories: the resources that might include hardware such as printers, services for users such as web email servers, and objects that are the domain and network's main functions.



Understanding active Directories

It is interesting to note the framework for the objects. An object can be a piece of hardware such as a printer, an end user, or security settings that the administrator set. These objects can hold other objects within their file structure. All objects have an ID, usually an object name (folder name). In addition to these objects being able to hold other objects, every object has its own attributes that allow it to be characterized by the information it contains. Most IT professionals call these settings or characterizations schemas.

The schema type created for a folder ultimately determines how these objects are used. For instance, some objects with certain schemas cannot be deleted, they can only be deactivated. Others types of schemas with certain attributes can be deleted entirely. For

instance, a user object can be deleted, but the administrator object cannot be deleted.

In order to understand active directories, it is important to know the framework in which objects can be viewed. In fact, an active directory can be viewed at either one of three levels. These levels are called forests, trees, or domains. The highest structure is called the forest because it shows all objects included in the active directory.

Within the Forest structure are trees, these structures usually hold one or more domains. Further down the active directory structure are single domains. To put the forest, trees, and domains into perspective, consider the following example.

A large organization has many dozens of users and processes. The forest might be the entire network of users and specific computers at a set location. Within this forest directory are now trees that hold information on specific objects such as domain controllers, program data and system, among others. Within these objects are even more objects that can be controlled and categorized.

how are active Directories Used?

A computer administrator for a large corporation or organization can easily update all users' computers with new software, patches, and files by simply updating one object in a forest or tree.

Because each object fits into a set schema and has specific attributes, a network administrator can easily clear a person on a set tree or instantly give or deny access to select users for certain applications. The Microsoft servers use trust to determine whether access should be allowed. Two types of trusts that Microsoft active directories incorporate are transitive trusts and one way non-transitive trust. A transitive trust is when there is a trust that goes further than two domains in a set tree, meaning two entities are able to access each other's domains and trees.

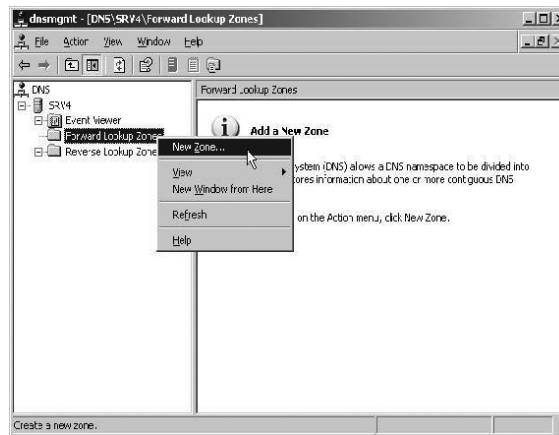
A one way transitive trust is when a user is allowed access to another tree or domain, but the other domain does not allow access to the further domains. This can be summed up as a network administrator and user. The network administrator can access most trees in the forest including a specific user's domain. However the end user, while able to access his or her own domain, cannot access other trees.

It is important to note that active directories are a great way to organize a large organization or corporation's computer data and network. Without an active directory, most users would have computers that need to be updated individually and would not have access to a larger network where data can be processed and reports can be created. While active directories can be technical to a good extent and require considerable expertise to navigate, they are essential to storing information and data on networks.

Configure the DNS Zones: (Not mandatory, can be done via the DCPROMO process)

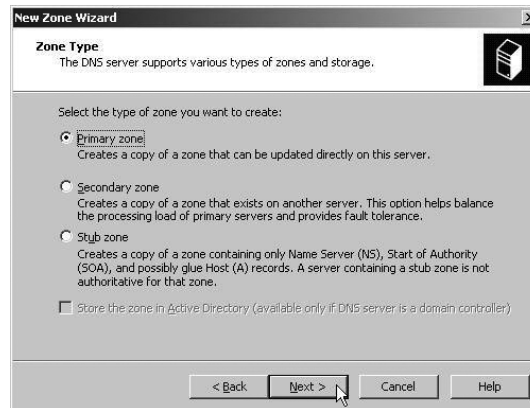
We assume that you already have the DNS service installed. If this is not the case, please read Create a New DNS Server for AD. Furthermore, it is assumed that the DC will also be its own DNS server. If that is not the case, you **MUST** configure another Windows

2000/2003 server as the DNS server, and if you try to run DCPROMO without doing so, you'll end up with errors and the process will fail.



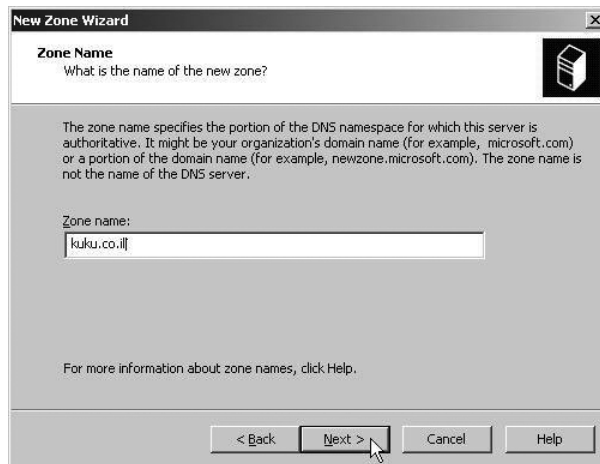
Creating a Standard primary Forward Lookup Zone

1. Click Start, point to All Programs, point to Administrative Tools, and then click DNS Manager. You see two zones under your computer name: Forward Lookup Zone and Reverse Lookup Zone.
2. Right click Forward Lookup Zones and choose to add a new zone.
3. Click Next. The new forward lookup zone must be a primary zone so that it can accept dynamic updates. Click Primary, and then click next.

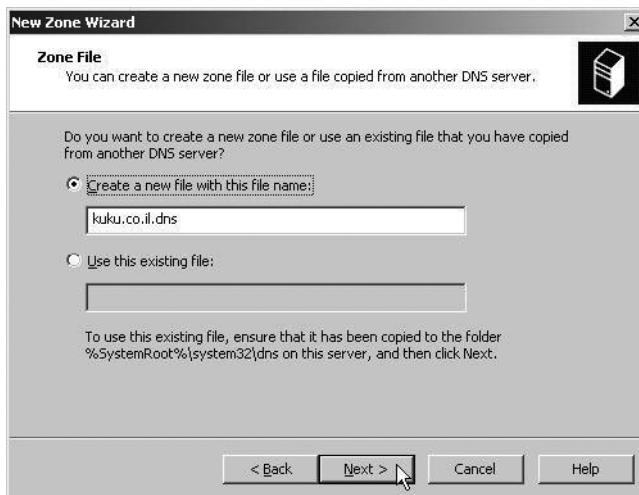


4. The name of the zone must be the same as the name of the Active Directory domain, or be a logical DNS container for that name. For example, if the Active Directory domain is named "lab.dpetri.net", legal zone names are "lab.dpetri.net", "dpetri.net", or "net".

Type the name of the zone, and then click next.



5. Accept the default name for the new zone file. Click Next.



6. To be able to accept dynamic updates to this new zone, click "Allow both no secure and Secure dynamic updates". Click Next.



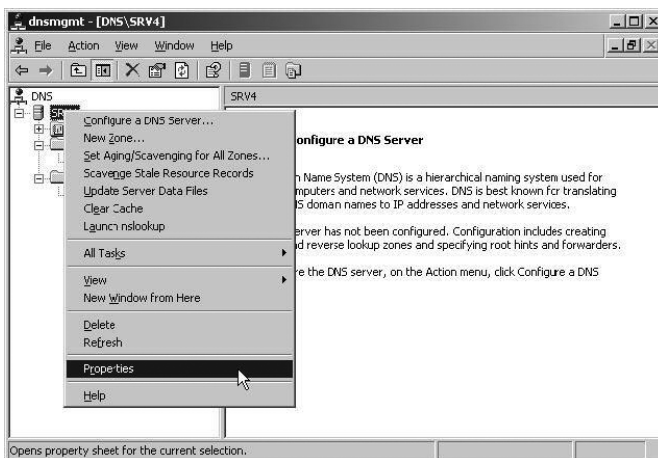
7. Click Finish.



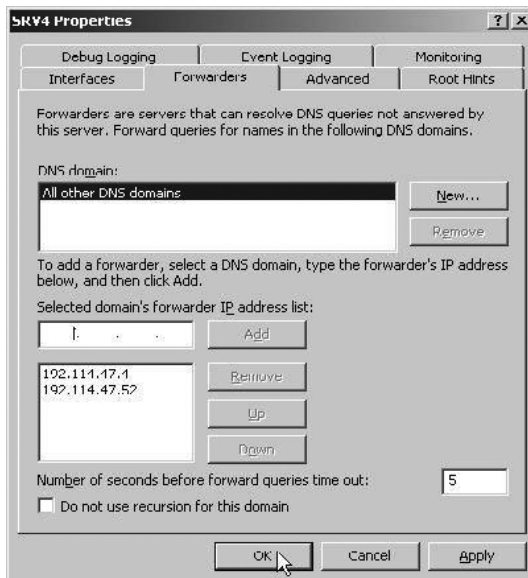
You should now make sure your computer can register itself in the new zone. Go to the Command Prompt (CMD) and run "ipconfig /registering" (no quotes, duh...). Go back to the DNS console, open the new zone and refresh it (F5). Notice that the computer should by now be listed as an A Record in the right pane. If it's not there try to reboot (although if it's not there a reboot won't do much good). Check the spelling on your zone and compare it to the suffix you created in step 1. Check your IP settings.

enable DNS Forwarding for Internet connections

1. Start the DNS Management Console.
2. Right click the DNS Server object for your server in the left pane of the console, and click Properties.

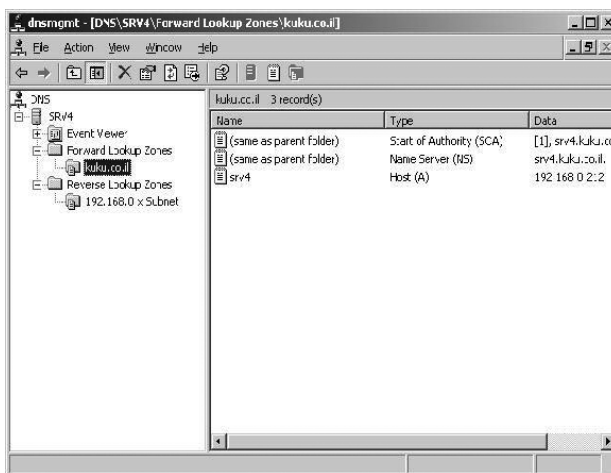


3. Click the Forwarders tab.
4. In the IP address box enter the IP address of the DNS servers you want to forward queries to – typically the DNS server of your ISP. You can also move them up or down. The one that is highest in the list gets the first try, and if it does not respond within a given time limit - the query will be forwarded to the next server in the list.



5. Click OK. Creating a Standard Primary Reverse Lookup Zone

You can (but you don't have to) also create a reverse lookup zone on your DNS server. The zone's name will be the same as your TCP/IP Network ID. For example, if your IP address is 192.168.0.200, then the zone's name will be 192.168.0 (DNS will append a long name to it, don't worry about it). You should also configure the new zone to accept dynamic updates.



Installing active Directory Services

Running DCPROMO - After completing all the previous steps (remember you didn't have to do them) and after double Checking your requirements you should now run Dcpromo.exe from the Run command.

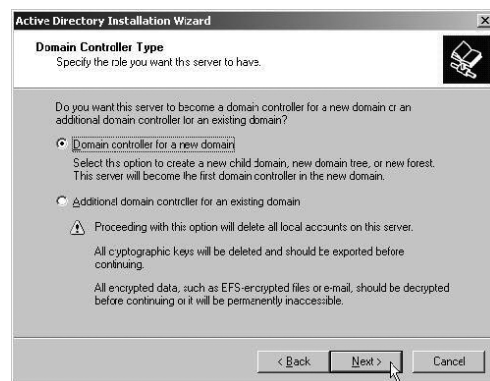
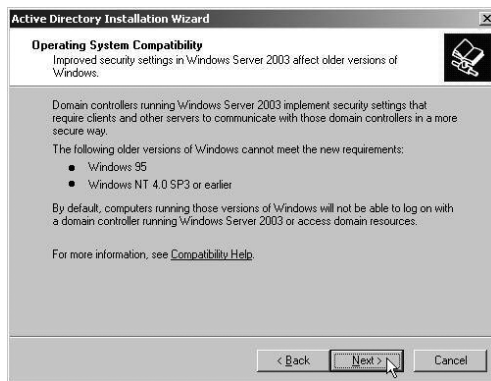
1. Click Start, point to Run and type "Dcpromo".



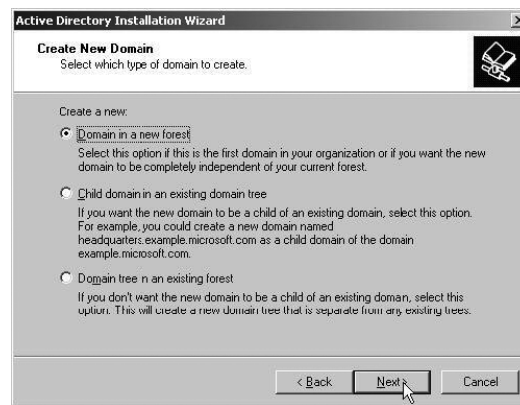
- The wizard windows will appear. Click Next.



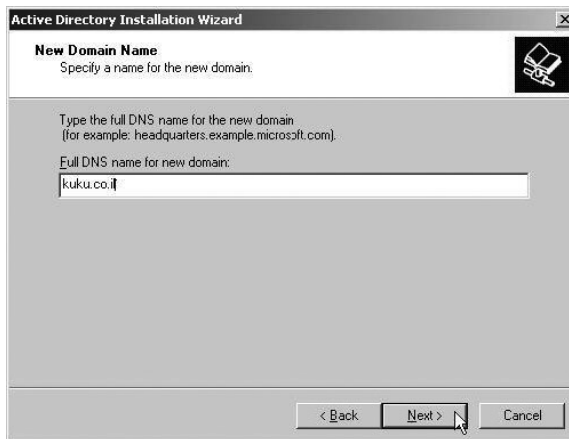
- In the Operating System Compatibility windows read the requirements for the domains Clients and if you like what you see - press Next.



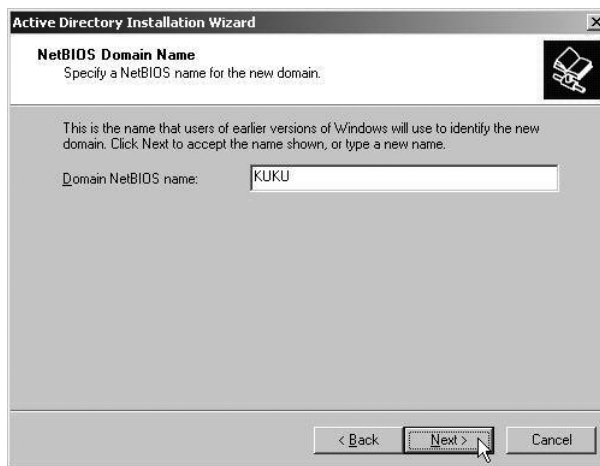
- Choose Domain Controller for a new domain and click next.



5. Choose create a new Domain in a new forest and click next.



6. Enter the full DNS name of the new domain, for example - kuku.co.il - this must be the same as the DNS zone you've created in step 3, and the same as the computer name suffix you've created in step 1. Click Next.

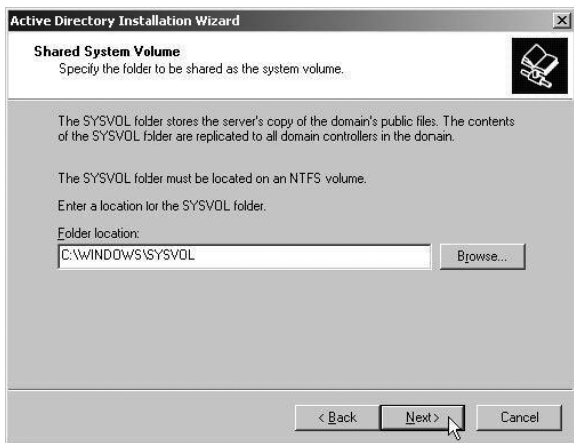


This step might take some time because the computer is searching for the DNS server and checking to see if any naming conflicts exist.

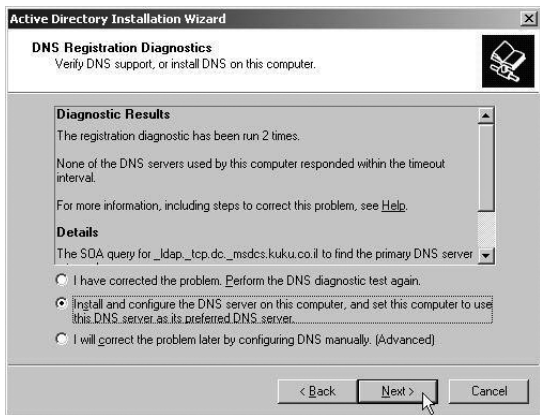
7. Accept the down-level NetBIOS domain name, in this case it's KUKU. Click Next



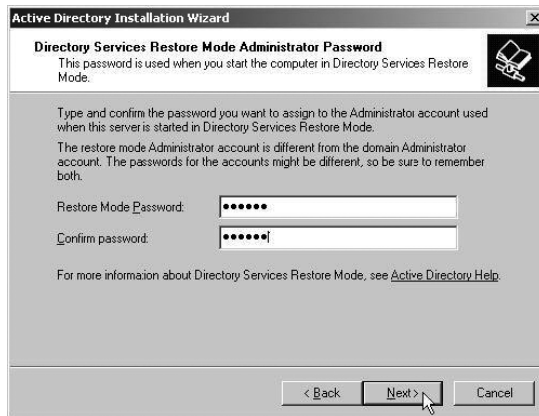
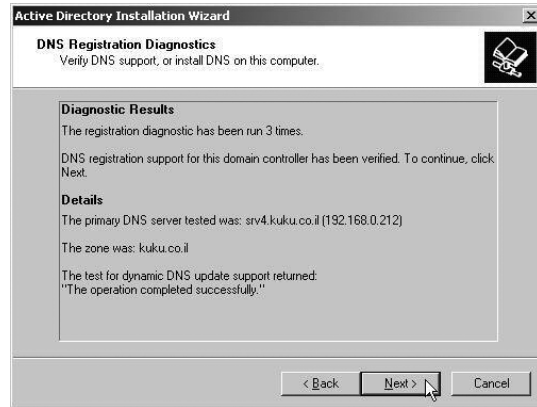
8. Accept the Database and Log file location dialog box (unless you want to change them of course). The location of the files is by default %system root%\NTDS, and you should not change it unless you have performance issues in mind. Click Next.



9. Accept the Sysvol folder location dialog box (unless you want to change it of course). The location of the files is by default %system root%\SYSVOL, and you should not change it unless you have performance issues in mind. This folder must be on an NTFS v5.0 partition. This folder will hold all the GPO and scripts you'll create, and will be replicated to all other Domain Controllers. Click Next.



10. If your DNS server, zone and/or computer name suffix were not configured correctly you will get the following warning:
11. This means the Dcpromo wizard could not contact the DNS server, or it did contact it but could not find a zone with the name of the future domain. You should check your settings. Go back to steps 1, 2 and 3. Click Ok. You have an option to let

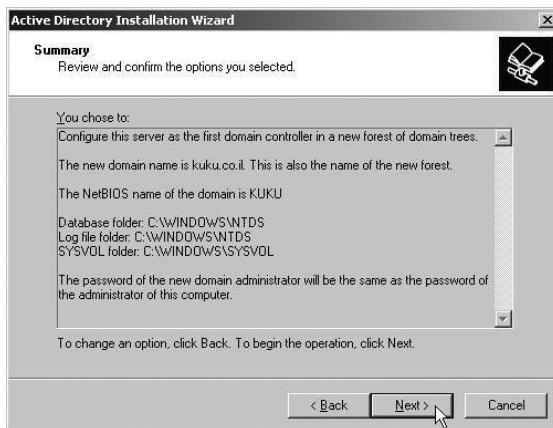


Dcpromo do the configuration for you. If you want, Dcpromo can install the DNS service, create the appropriate zone, configure it to accept dynamic updates, and configure the TCP/IP settings for the DNS server IP address. To let Dcpromo do the work for you, select "Install and configure the DNS server. Click Next. Otherwise, you can accept the default choice and then quit Dcpromo and check steps 1-3. If your DNS settings were right, you'll get a confirmation window.

12. Just click next. Accept the Permissions compatible only with Windows 2000 or Windows Server 2003 settings, unless you have legacy apps running on Pre-W2K servers.
13. Enter the Restore Mode administrator's password. In Windows Server 2003 this password can be later changed via NTDSUTIL. Click Next.



14. Review your settings and if you like what you see - Click Next.
15. See the wizard going through the various stages of installing AD. Whatever you do - NEVER click Cancel!!! You'll wreck your computer if you do. If you see you made a mistake and want to undo it, you'd better let the wizard finish and then run it again to undo the AD.



16. If all went well you'll see the final confirmation window. Click Finish.



17. You must reboot in order for the AD to function properly.

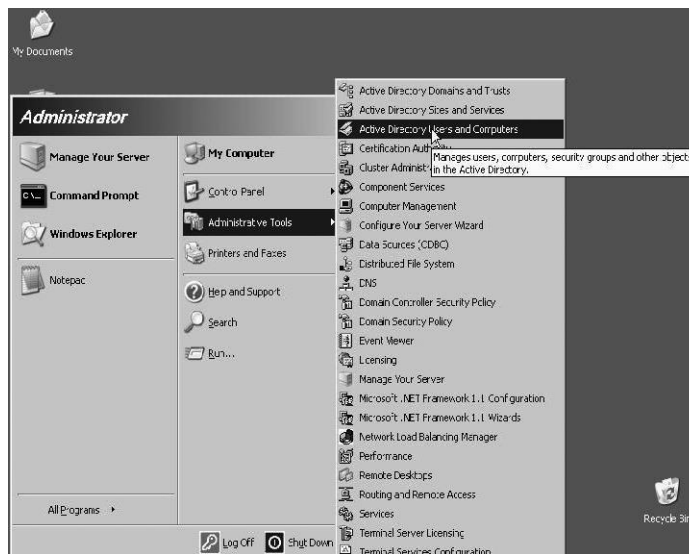


18. Click Restart now.

Checking the aD installation

You should now check to see if the AD installation went well.

1. First, see that the Administrative Tools folder has all the AD management tools installed.



2. Run Active Directory Users and Computers (or type "dsa.msc" from the Run command). See that all OUs and Containers are there.

adding Users and Computers to the active Directory Domain

After the new Active Directory domain is established, create a user account in that domain to use as an administrative account. When that user is added to the appropriate security groups, use that account to add computers to the domain.

to create a new user, follow these steps:

- a. Click **Start**, point to **administrative tools**, and then click **active Directory Users and Computers** to start the Active Directory Users and Computers console.
- b. Click the domain name that you created, and then expand the contents.
- c. Right-click **Users**, point to **New**, and then click **User**.
- d. Type the first name, last name, and user logon name of the new user, and then click **next**.
- e. Type a new password, confirm the password, and then click to select one of the following check boxes:
 - Users must change password at next logon (recommended for most users)
 - User cannot change password
 - Password never expires
 - Account is disabled - Click **Next**.
- f. Review the information that you provided, and if everything is correct, click **Finish**.

After you create the new user, give this user account membership in a group that permits that user to perform administrative tasks. Because this is a laboratory environment that you are in control of, you can give this user account full administrative access by making it a member of the Schema, Enterprise, and Domain administrators groups. To add the account to the Schema, Enterprise, and Domain administrators groups, follow these steps:
- g. On the Active Directory Users and Computers console, right-click the new account that you created, and then click **properties**.
- h. Click the **Member Of** tab, and then click **add**.
- i. In the **Select Groups** dialog box, specify a group, and then click **OK** to add the groups that you want to the list.
- j. Repeat the selection process for each group in which the user needs account membership.
- k. Click **OK** to finish.
- l. The final step in this process is to add a member server to the domain. This process also applies to workstations. To add a computer to the domain, follow these steps:

Log on to the computer that you want to add to the domain.

1. Right-click **My Computer** and then click **properties**.
2. Click the **Computer Name** tab, and then click **Change**.
3. In the **Computer Name Changes** dialog box, click **Domain** under **Member Of**, and then type the domain name. Click **OK**.
4. When you are prompted, type the user name and password of the account that you previously created, and then click **OK**.

5. A message that welcomes you to the domain is generated.
6. Click **OK** to return to the **Computer Name** tab, and then click **OK** to finish.
7. Restart the computer if you are prompted to do so.

to assign user rights for your local computer

Administrators can assign specific rights to group accounts or to individual user accounts. These rights authorize users to perform specific actions, such as logging on to a system interactively or backing up files and directories. User rights are different from permissions because user rights apply to user accounts, and permissions are attached to objects.

User rights define capabilities at the local level. Although user rights can apply to individual user accounts, user rights are best administered on a group account basis. This ensures that a user logging on as a member of a group automatically inherits the rights associated with that group. By assigning user rights to groups rather than individual users, you simplify the task of user account administration. When users in a group all require the same user rights, you can assign the set of user rights once to the group, rather than repeatedly assigning the same set of user rights to each individual user account.

User rights that are assigned to a group are applied to all members of the group while they remain members. If a user is a member of multiple groups, the user's rights are cumulative, which means that the user has more than one set of rights. The only time that rights assigned to one group might conflict with those assigned to another is in the case of certain logon rights. In general, however, user rights assigned to one group do not conflict with the rights assigned to another group. To remove rights from a user, the administrator simply removes the user from the group. In this case, the user no longer has the rights assigned to that group.

There are two types of user rights: privileges, such as the right to back up files and directories, and logon rights, such as the right to log on to a system locally.

Open Local Security Settings

1. In the console tree, click **User rights assignment**. >Security Settings > Local Policies > User Rights Assignments
2. In the details pane, double-click the user right you want to change.
3. In **User right properties**, click **add**.
4. Add the user or group and click **OK**.

To open Local Security Policy, click **Start**, click **Control panel**, click **performance and Maintenance**, click **administrative tools**, and then double-click **Local Security policy**.

Windows 2003 NTFS and Share permissions & Security

The concept of permissions in a Microsoft environment is one of the more confusing subjects that certification candidates face, but a very necessary topic to know as many of Microsoft's certification exams test on this. This guide aims to help you understand

the different the various types of permissions and how to use them in a Windows 2003 environment.

NTFS file permissions are used to control the access that a user, group, or application has to folders and files. They are referred to as NTFS permissions because a drive must be formatted with NTFS in order to utilize these permissions.

NtFS File permissions:

NTFS file permissions are used to control the access that a user, group, or application has to files. This first table displays the available permissions for files.

Full Control	Read, write, modify, execute, change attributes, permissions, and take ownership of the file.
Modify	Read, write, modify, execute, and change the file's attributes.
Read & Execute	Display the file's data, attributes, owner, and permissions, and run the file (if it's a program or has a program associated with it for which you have the necessary permissions).
Read	Display the file's data, attributes, owner, and permissions.
Write	Write to the file, append to the file, and read or change its attributes.

Windows 2000 & 2003 have the option of denying a user or users a particular permission. For example, if you wanted to make sure that Bob is unable to read any file, then simply deny him read permissions. Permissions are cumulative, except for Deny, which overrides everything. By cumulative, we mean that a user's effective permissions are the result of combining the user's assigned permissions and the permissions assigned to any groups that the user is a member of. For example, if Bob is assigned Read access to a file, and the "sales" group that Bob is a member of has Write permissions assigned, Bob's effective permissions is are Read and Write for that file.

NtFS Folder permissions

NTFS Folder permissions determine the access that is granted to a folder and the files and subfolders within that folder. These permissions can be assigned to a user or group. The following table displays the different permissions for folders.

Full Control	Read, write, modify, and execute files in the folder, change attributes, permissions, and take ownership of the folder or files within.
Modify	Read, write, modify, and execute files in the folder, and change attributes of the folder or files within.
Read & Execute	Display the folder's contents and display the data, attributes, owner, and permissions for files within the folder, and run files within the folder (if they're programs or have a program associated with them for which you have the necessary permissions).

List Folder Contents	Display the folder's contents and display the data, attributes, owner, and permissions for files within the folder, and run files within the folder (if they're programs or have a program associated with them for which you have the necessary permissions).
Read	Display the file's data, attributes, owner, and permissions.
Write	Write to the file, append to the file, and read or change its attributes.

The Read & Execute and List Folder Contents folder permissions appear to be exactly the same, however, they are inherited differently, thus are different permissions. Files can inherit the Read & Execute permissions but can't inherit the List Folder Contents permission. Folders can inherit both. File permissions override folder permissions. For example, let's say that Bob has read access to a file called file.txt which is located in a folder that he has no access to. In this case, the file will be invisible to the Bob and since he cannot list the folder contents, he would have to access the file using the UNC path or the logical file path.

Copying, Moving, and Inheritance

The next table shows what happens to files when they are copied or moved within or across NTFS partitions.

Moving within a partition	Does not create a new file - simply updates location in directory. File keeps its original permissions.
Moving across a partition	Creates a new file and deletes the old one. Inherits the target folders permissions.
Copying within a partition	Creates a new file which inherits permissions of target folder.

Files moved from an NTFS partition to a FAT partition do not retain their attributes or security descriptors, but will retain their long filenames

Special access File permissions

Windows 2000 & 2003 also support special access permissions which are made by combining other permissions. The following tables will show special access permissions and the recipes to make them.

File Special permissions	Full Control	Modify	read & execute	read	Write
Traverse Folder/Execute File	X	X	X		
List Folder/Read Data	X	X	X	X	
Read Attributes	X	X	X	X	
Read Extended Attributes	X	X	X	X	
Create Files/Write Data	X	X			X
Create Folders/Append Data	X	X			X
Write Attributes	X	X			X

Write Extended Attributes	X	X			X
Delete Subfolders and Files	X				
Delete	X	X			
Read Permissions	X	X	X	X	X
Change Permissions	X				
Take Ownership	X				
Synchronize	X	X	X	X	X

Special access Folder permissions

Below are the special access permissions for folders.

Folder Special permissions	Full Control	Modify	read & execute	List Folder Contents	read
Traverse Folder/Execute File	X	X	X	X	
List Folder/Read Data	X	X	X	X	X
Read Attributes	X	X	X	X	X
Read Extended Attributes	X	X	X	X	X
Create Files/Write Data	X	X			
Create Folders/Append Data	x	x			
Write Attributes	X	X			
Write Extended Attributes	X	X			
Delete Subfolders And Files	X				
Delete	X	X			
Read Permissions	X	X	X	X	X
Change Permissions	X				
Take Ownership	X				
Synchronize	X	X	X	X	X

Remember that file permissions override the permissions of its parent folder. Anytime a new file is created, the file will inherit permissions from the target folder.

Share permissions

Shares are administered through the MMC, My Computer or through Explorer and permissions can be set on a share in the "Share Permissions" tab. Share level permissions only apply when a file or folder is being accessed via the network and do not apply to a user logged into the machine locally. The following are the different share-level permissions.

read	View files and subdirectories. Execute applications. No changes can be made.
Change	Includes read permissions and the ability to add, delete or change files or subdirectories.
Full Control	Can perform any and all functions on all files and folders within the share.

The Deny permission can also be applied to shares. The Deny permission overrides all others. When folders on FAT and FAT32 volumes are shared, only the share level permissions apply as these systems do not support file and directory (NTFS) permissions. When folders on NTFS volumes are shared, the effective permission of the user will be the most restrictive of the NTFS and share permissions. This means that if Bob is trying to access a file called *mystuff* located on *myshare* and he has share permissions of read and file permissions of full control, his effective permissions would be read. Conversely, if his share permissions are full control and his file permissions are read, he will still only have read permissions to *mystuff*.

effective permissions tool in Windows 2003

Determining effective permissions can get confusing, especially on enterprise networks. In Windows 2003, Microsoft included a new feature that helps sort this mess out. If you go to the Advanced properties of the Security tab for NTFS resources, there is a tab titled "Effective Permissions" which allows you to calculate the permissions that apply to users or groups. This tool does not take share permissions into account.

Best practices

The way companies manage their permissions will vary based on their needs. In any event, a lot of planning should be done before implementing permissions systems in order to avoid a lot of headaches later. Below are some best practices for using permissions. When setting permissions, you want to minimize the amount of administration required. Imagine if you had to manage the permissions on every file on your network for every user. It would be an administrative nightmare. For this reason, unless absolutely necessary, assign permissions to groups and place users in the relevant group. The same should be done for share permissions as well.

Avoid using Deny permissions except in the following types of cases:

- Use Deny permissions to exclude a subset of a group which has allowed permissions.
- Use Deny to exclude one special permission when you have already granted full control to a user or group.

You definitely should not ever use Deny permissions for the everyone group because that includes administrators.

When possible, use security templates

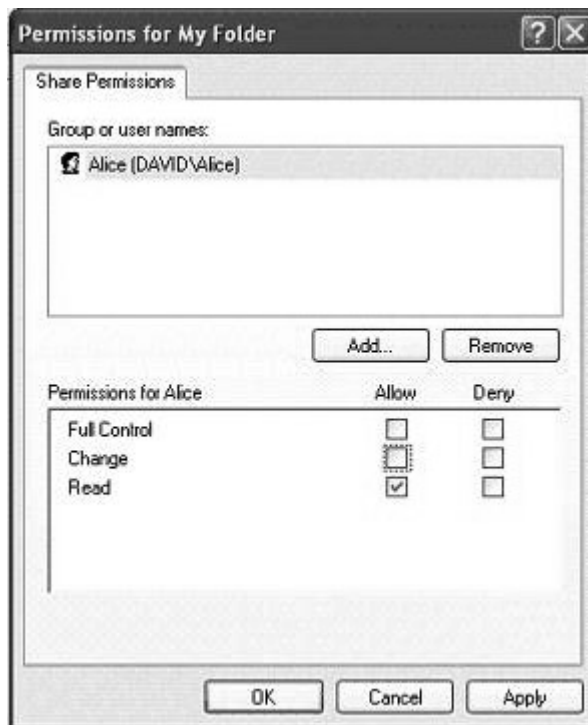
Keep in mind that privileges (rights) can sometimes override permissions.

Note: While the permissions systems in Windows 2000 and 2003 are nearly identical, there are a few differences. One of the biggest permissions differences between Windows 2000 and 2003 was the default security settings. Windows 2000 shipped with full control for the everyone group (NTFS and share permissions), guest account was enabled, etc. Windows 2003 was locked down better in its default state.

Understanding Windows Shared permissions vs NtFS Security

General Information:

- Windows 9x/ME workstations cannot access NTFS partitions
- Shared permissions only apply to shares connected to over the network
- NTFS Security applies to users both locally and across the network
- When there's a difference between the sharing permission and the NTFS security permission, **the most restrictive setting wins**
- There are two types of NTFS permissions, file and folder
- Deny will always take precedence over allow permissions.



First, let's cover the definitions of security levels and permissions. We'll start with Shared permissions, there are only 3.

1. **read:** View files and subdirectories. Execute applications. No changes can be made.
2. **Change:** Includes read permissions and the ability to add, delete or change files or subdirectories
3. **Full Control:** Abilities to perform any and all functions on all files and folders within the share.

Now, let's cover what the 5 NTFS **file** permissions are and what they allow, you should notice that each level of security builds upon the one before it.

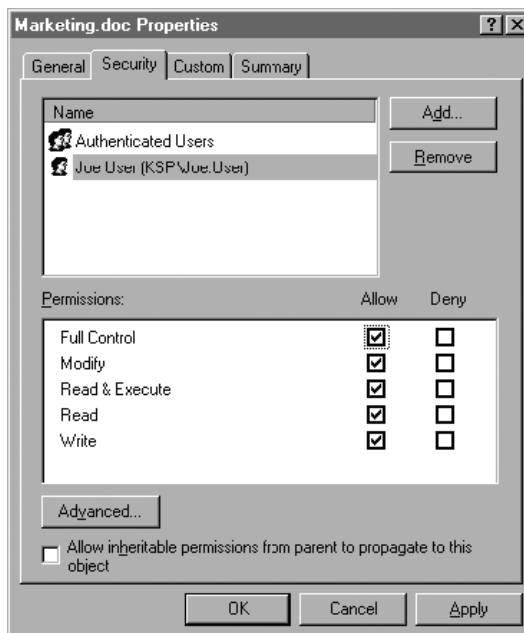
1. **read:** This allows the user or group to read the file and view its *attributes***, ownership, and permissions set.
2. **Write:** This allows the user or group to overwrite the file, change its attributes, view its ownership, and view the permissions set.
3. **read & execute:** This allows the user or group to run and execute the application. In addition, the user can perform all duties allowed by the Read permission.
4. **Modify:** This allows the user or group to modify and delete a file including perform

all of the actions permitted by the Read, Write, and Read and Execute NTFS file permissions.

5. **Full Control:** This allows the user or group to change the permission set on a file, take ownership of the file, and perform actions permitted by all of the other NTFS file permissions.

Next, are the the 6 NTFS **folder** permissions.

1. **read:** This allows the user or group to view the files, folders, and subfolders of the parent folder. It also allows the viewing of folder ownership, permissions, and attributes of that folder.
2. **Write:** This allows the user or group to create new files and folders within the parent folder as well as view folder ownership and permissions and change the folder attributes.
3. **Folder Contents:** This allows the user or group to view the files and subfolders contained within the folder.
4. **read & execute:** This allows the user or group to navigate through all files and subfolders including perform all actions allowed by the Read and List Folder Contents permissions.



5. **Modify:** This allows the user to delete the folder and perform all activities included in the Write and Read & Execute NTFS folder permissions.
6. **Full Control:** This allows the user or group to change permissions on the folder, take ownership of it, and perform all activities included in all other permissions.

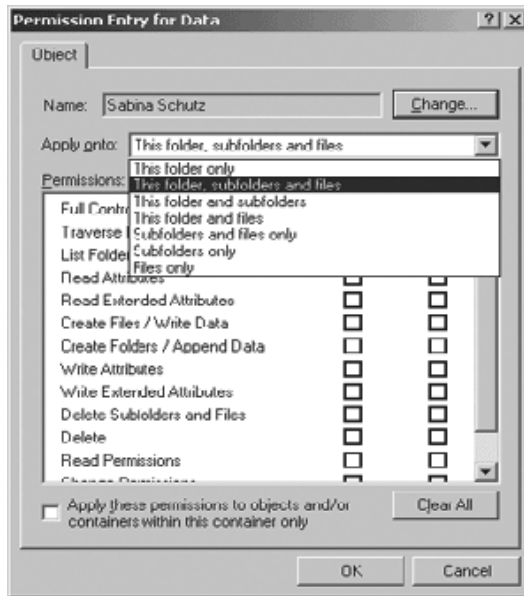
Earlier in the General Information list the last bullet mentioned deny takes precedence over allow. This is in reference to **NtFS special permission**, which is used when your file and folder permissions just aren't specific enough. Here are all 13 of them...

1. **traverse Folder/execute File:** This allows or denies a user to browse through a folder's subfolders and files where he would otherwise not have access. In addition, it allows or denies the user the ability to run programs within that folder.
2. **List Folder/read Data:** This allows or denies the user to view subfolders and file names in the parent folder. In addition, it allows or denies the user to view the data within the files in the parent folder or subfolders of that parent.
3. **read attributes:** This allows or denies a user to view the standard NTFS attributes of a file or folder.

4. **read extended attributes:** This allows or denies the user to view the extended attributes of a file or folder, which can vary due to the fact that they are defined by the programs themselves.

5. **Create Files/Write Data:** This allows or denies the user the right to create new files in the parent folder. In addition, it allows or denies the user to modify or overwrite existing data in a file.

6. **Create Folders/append Data:** This allows or denies the user to create new folders in the parent folder. In addition, it allows or denies the user the right to add data to the end of files. This does not include making changes to any existing data within a file.



7. **Write attributes:** This allows or denies the ability to change the attributes of a files or folder, such as Read-Only and Hidden.

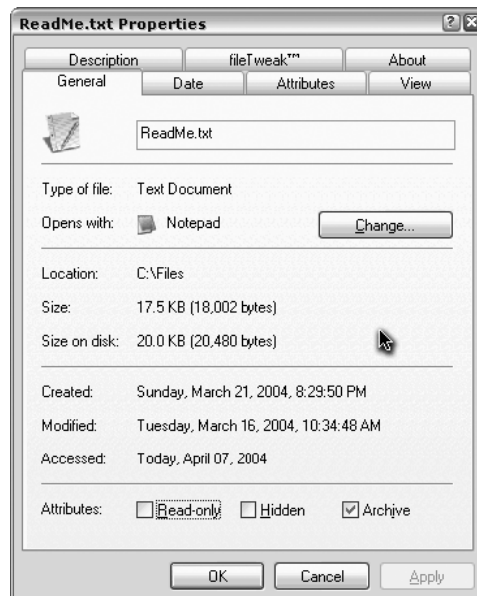
8. **Write extended attributes:** This allows or denies a user the ability to change the extended attributes of a file or folder. These attributes are defined by programs and may vary.

9. **Delete Subfolders and Files:** This allows or denies the deleting of files and subfolder within the parent folder. It also true that if this permission is assigned files and subfolders can be deleted even if the Delete special access permission has not been granted.

10. **Delete:** This allows or denies the deleting of files and folders. If the user does not have this permission assigned but does have the Delete Subfolders and Files permission, she can still delete.

Read Permissions This allows or denies the user the ability to read the standard NTFS permissions of a file or folder.

11. **Change permissions:** This allows or denies the user the ability to change the standard NTFS permissions of a files or folder.



12. **take Ownership:** This allows or denies a user the ability to take ownership of a file or folder. The owner of a file or folder can change the permissions on the files and folders she owns, regardless of any other permission that might be in place.
13. **Synchronize:** This allows or denies different threads to wait on the handle for the file or folder and synchronize with another thread that may signal it. This permission applies to only multithreaded, multiprocessing programs. So now that you have an idea of what defines these, what are the best practices, the best practice should be to keep access and administration to a minimum. Secure your windows shares with the minimum access needed. Utilize NTFS to further minimize access to your folders and files. Use groups for folders if appropriate as opposed to single user settings. Best of luck!

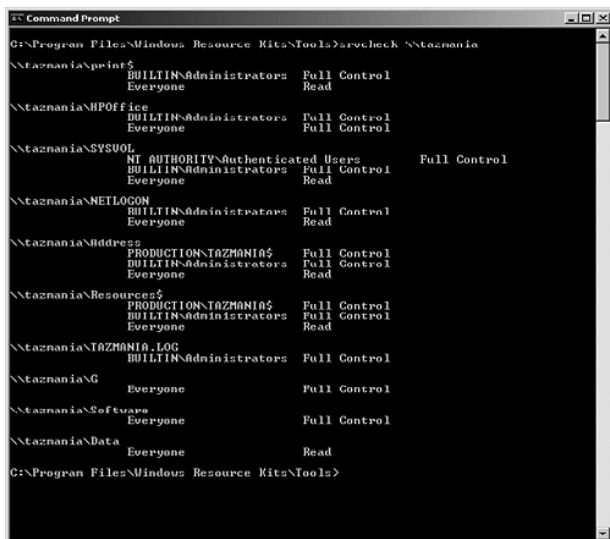
**Attributes are part of the file and include Read-Only, Hidden, Archive, and System

1. **read Only:** A file that is marked Read only cannot be altered. It can be read, but it cannot be changed or deleted.
2. **hidden:** By default, hidden files do not appear in a directory listing. (Normally power users uncheck “hide systems files in Folder Settings”).
3. **archive:** Every time the user or the software modifies a file, then the archive bit will be marked. This tells you when the file was last modified.
4. **System:** System files are files flagged for use by the operating system and is not usually displayed in a directory listing. System files should not be modified or deleted. You also want to be careful of contradictory permissions.

Summary

It recommends “assigning everyone full control at the share level and using NTFS permissions to secure the individual files or folders.” This is considered a security risk

to many, however, it may make it easier for you to keep track of what you’re sharing to whom. Also, if you want to play it safe and use permissions at both the NTFS and Share level, Server Check is a tool that is part of the Server 2003 Resource kit, and it works for Windows 2003, 2000, and XP. It is a command line interface that will let you know what permissions are defined for each shared resource. A screenshot of this application in progress from the article is shown.



Chapter – 10

remote Connectivity & Drive Mapping

How to configure Configuring NetMeeting

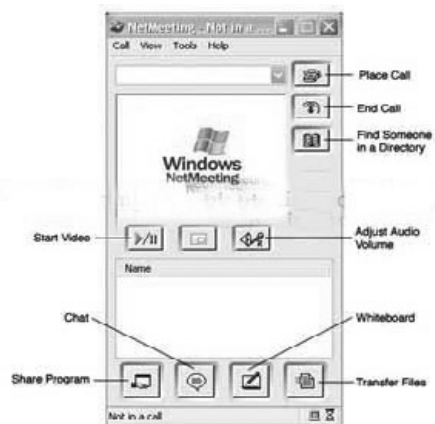
NetMeeting 3.0 is built in to all copies of Windows XP. However, it needs to be configured to use it.

To configure NetMeeting:

- Click Start and select Run:
- In Run box, type *conf.exe* and click OK
- In the NetMeeting window, click Next
- Fill in your name, email address, and location info, then click Next
- Click off “Log on to directory server when NetMeeting starts”, then click Next
- Select the network connection you are using, then click Next (On campus, select Local Area Network)
- Select “Put a shortcut to NetMeeting on my desktop”, and click next.
- In Audio Tuning Wizard window, click next.
- In Audio Tuning Wizard window, adjust the speaker or headphone volume and click next.
- When finished adjusting settings, click Finish.

NetMeeting setup is now complete. NetMeeting will then start, and an icon will be displayed on the desktop. (During startup, if Windows XP Firewall attempts to block NetMeeting, click Unblock.)

The NetMeeting main window will then appear



Finding Your IP Address

Connections in NetMeeting are done through IP addresses. You need to know your IP Address. To find out your IP Address:

- Click on Start button, select Run
- Type command and click OK
- In the window that appears, type ipconfig and press the Enter key
- Your IP Address will be displayed in the window (eg. 192.168.1.5) (Write down your IP Address)
- To close the window, type Exit and press the Enter key.

Alternatively, in the NetMeeting main window, click Help, and then select "About Windows NetMeeting". Your IP Address will be displayed in the window.

Starting NetMeeting

You can connect individually or to a group. To start NetMeeting:

- Click the NetMeeting shortcut icon on your desktop

The NetMeeting main window will appear.

Placing a Call

Click the Place Call button. Enter the IP Address of the person or meeting you want to connect to.



Receiving a call

When another person is calling you NetMeeting will display the following screen:

Click Accept to begin the call.



Hosting and Joining Meetings to host a meeting:

- In the Call menu, select Host Meeting.
- In Meeting Name, type the meeting name or leave it set to Personal Conference.
- To monitor who joins the meeting, click the “Only you can accept incoming calls” check box.
- To restrict participants from inviting other people, click the “Only you can place outgoing calls” check box. and Click OK

Using Chat

With chat you can communicate with an individual or a group by text messaging. These conversations can be saved as a rich text file for later reference. Options such as “Whisper” mode allow private messages between the host and an individual during a group session. To open a chat session:

Click the Chat button.



Using Whiteboard

With Whiteboard you can review, create and update graphic information. This option allows you to load saved Whiteboard pages into a conference by dragging and dropping the saved pages into the Whiteboard window. To open Whiteboard:

Click the Whiteboard button.



Sharing Programs

Shared Programs allows meeting participants to view and work on files together even if they do not have the program. Only one participant at a time can be in control of the shared program.

To share a program:

- Click the Share Program button.
- Select the program you wish to share.
- Choose who you want to share the program with.
- Click Share.



You can also share your computer desktop in order to share your entire computer with participants. To stop sharing, click Unshared in the Sharing dialog box.

Remote Desktop Sharing

Remote Desktop Sharing allows you to access a computer from another computer at another location. To use Remote Desktop Sharing, you activate it and then close NetMeeting.

To set up Remote Desktop Sharing:

- Under Tools on the menu bar, select Remote Desktop Sharing.
- In the Remote Desktop Sharing Wizard, click next.
- In the Remote Desktop Sharing Wizard, click yes, enable password-protected screen saver.
- Click Finish.

To activate Remote Desktop Sharing on the computer:

- Note the computer's IP Address.
- Under *Call* on the menu bar, select *Exit*.

To connect to the computer from a second location:

- Click the Call button in NetMeeting.
- In "To", type in the computer's IP Address.
- Type in your password. The remote desktop will appear on the second computer.

To end Remote Desktop Sharing:

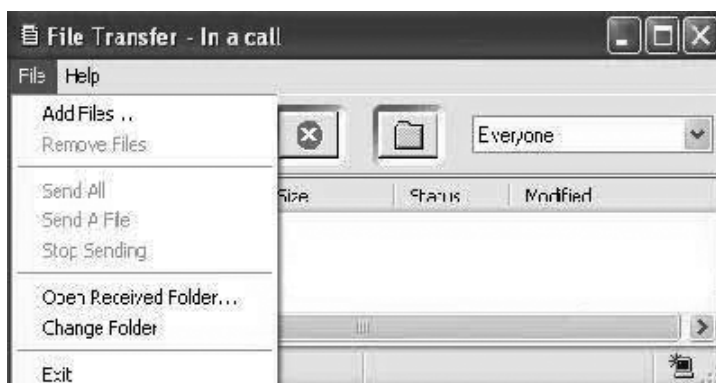
- On the computer being accessed, click **Start**.
- Select either **Log Off** or **Turn Off**.

Transferring Files

Files can also be transferred in the background while in a NetMeeting conference and can be sent either to an individual or a group.

To transfer a file:

- Click the Transfer Files button.
- Click the Add File button.
- Select the desired files.
- Choose the people you wish to send the file to (if you wish to send the file to everyone in the meeting, click all).
- Click Send All button to transfer the files.



Configuring Settings

To configure NetMeeting's video and audio options:

* Under the Tools menu, select Options. The Options dialog box will appear.

For video settings:

* Select the Video Tab

To configure audio options:

* Select the Audio tab

Getting help

For help using Windows NetMeeting, select Help Topics under Help on the menu bar.

How to configure Remote Desktop RDP Step By Step Guide

Remote Desktop is an optional Windows XP Professional service. To install it on a host system (to enable a computer to accept a remote connection request), Follow these steps:

Start → Control Panel → Select Add Or Remove Programs → Select Add/Remove Windows Components → Select Internet Information Services → Click the Details button → Select World Wide Web Service → Click the Details button → Check the Remote Desktop Web Connection checkbox → Click OK → Click Next → Click Finish to complete the wizard

To make this update in your system either restart the computer or follow these steps

- Click Start → Select Run → Enter **Net Stop w3svc** → click the OK button or press Enter.
- Click Start → Select All Programs → Select Microsoft Update → Select Scan For Updates → Install all critical updates on the host system.
- Click Start → Select Run → Enter **Net Start w3svc** → click the OK button.

Installing Remote Desktop connection on non-XP systems

Non-Windows XP systems can also access Windows systems running Windows Remote Desktop. The local system used to access the remote computer must have the remote connectivity client software installed. To install the required Terminal Services components:

- Insert a Windows XP Professional CD in the local system's CD or DVD drive.
- From the resulting Welcome to Microsoft Windows XP screen, click Perform Additional Tasks.
- Click Setup Remote Desktop Connection from the What Do You Want To Do Screen.
- The Install Shield Wizard will open; click Next on the Welcome To The Install Shield Wizard for Remote Desktop Connection.
- Read and accept the license agreement and click Next.
- Enter the customer name and organization, and specify whether the desktop connection is to be available to all users or only the logged in user and click Next.
- Click Install.
- Click Finish.

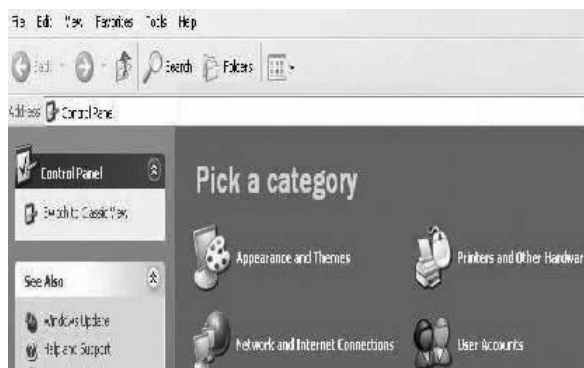
The older Windows system can now open the Remote Desktop Connection menu by clicking Start → Programs → Accessories → Communications → Remote Desktop Connection or by opening a command prompt and typing mstsc.

Firewall settings

Before attempting a Remote Desktop session, ensure the host system's Windows Firewall is set to enable the connection. Follow these steps to confirm the Windows Firewall is properly configured:

- Click **Start**.
- Click **Control Panel**.
- Access the Windows Firewall menu (by clicking Windows Firewall using Control Panel's Category View or by clicking Security Center and selecting Windows Firewall using the Classic View).
- Click the **Exceptions tab**.
- Confirm the **Remote Desktop checkbox is checked** and isn't overridden by a group policy.

When working with other firewalls, it's usually best that **port 3389 (and port 80)** be opened to enable Terminal Services traffic (and the connection to the Remote Desktop application). This is especially true when attempting to connect to Small Business Server 2003 desktops.

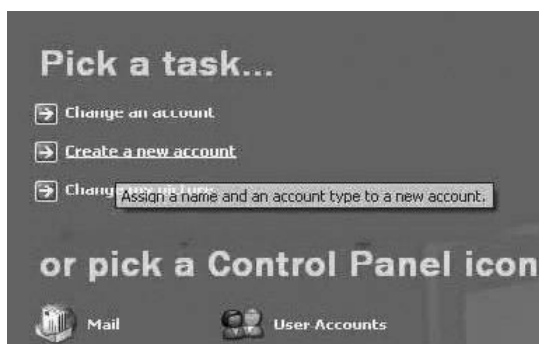


Enabling user access

Create a user account that has administrative privilege (How to create user account in XP)

- Click Start.
- Click Control Panel.
- Click User accounts

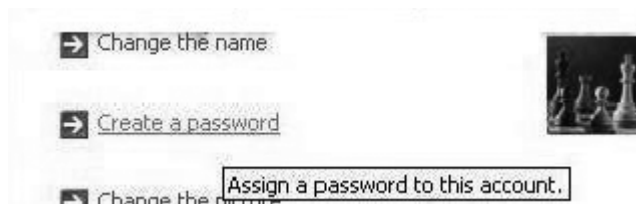
Click on Create a new account



Enter the name for new account



Now create password for this account



Next, you need to specify which users can access the system remotely. To do so:

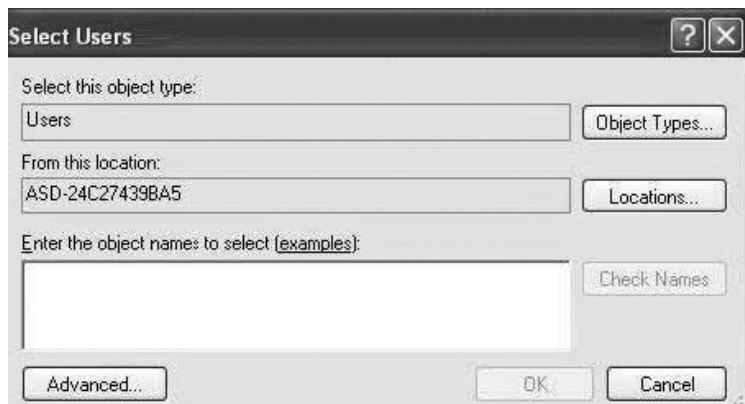
- Right click on My Computer and select properties
- Click the Remote tab.
- Checked the Allow Users To Connect Remotely To This Computer.
- Click the Select Remote Users button



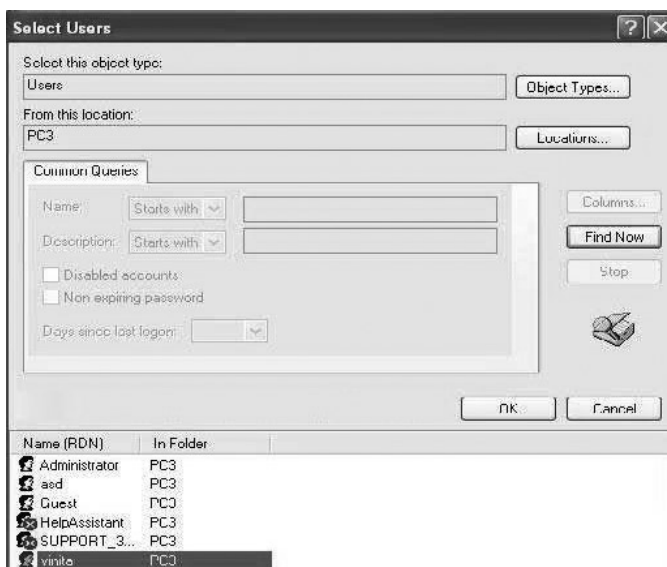
Click the Add button



Now click on advance



Specify those users that should receive permission to access the system remotely.



- Click OK to close the Select Users window.
- Click OK to close the Remote Desktop Users window

By default, any members of the Administrators group can connect to the system, even if they're not specifically authorized using the Remote Desktop Users window. Should you wish to remove a user's permission to log on remotely, highlight that user's name and click the Remove button?

Connecting with Remote Desktop from other computer

Once those conditions are met, users and administrators should be able to access systems using Remote Desktop by:

1. Clicking Start.
2. Selecting Run.
3. Typing *mstsc* and clicking OK. **Alternatively, one can:**

1. Click Start.
2. Click All Programs.
3. Click Accessories.
4. Click Communications.
5. Click Remote Desktop Connection.

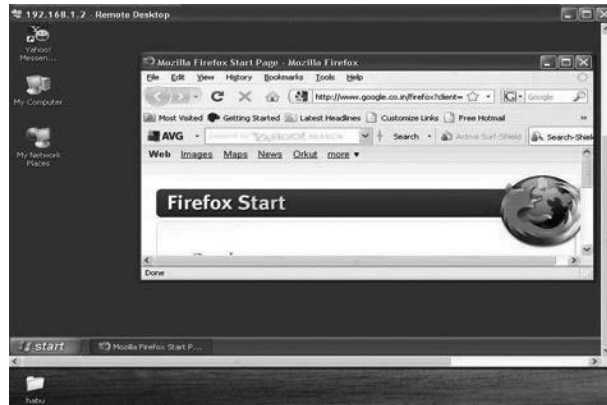
Type the ip address of the computer to which you want to connect



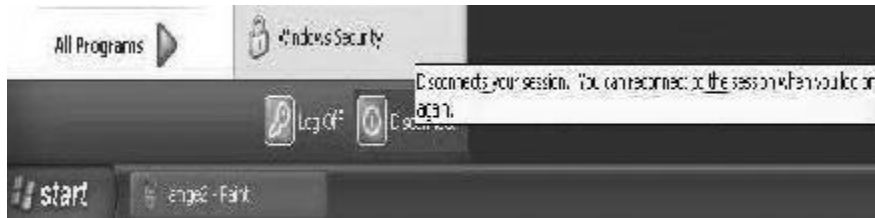
Give the user name and password



Now you can use other computer



When you have finished you can disconnects your session by start → Disconnects



How to configure Remote Assistance Step By Step Guide

The days of traveling to each client system to troubleshoot problems are over. Microsoft's native Windows XP assistance tool is all that is required. Follow these steps to configure and enable Windows XP's Remote Assistance.

Sending a remote assistance request

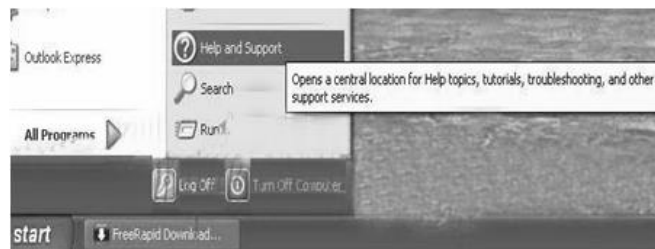
Windows XP's Remote Assistance feature enables users to call for help. The application proves particularly helpful when clients in remote locations require support.

Before an administrator can render assistance, the end user must send a Remote Assistance request to the administrator.

Clients should follow these steps to send a Remote Assistance request:

- Click **Start**.
- Click **Help and Support**.

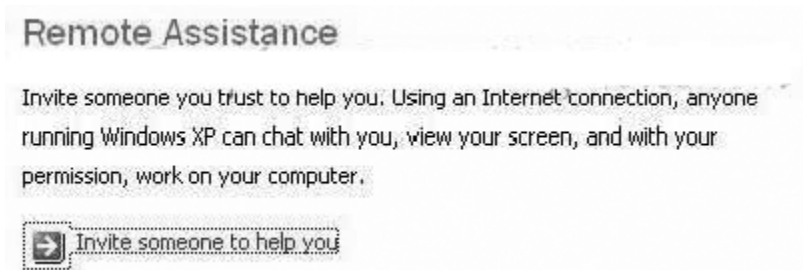
Select the Invite a Friend to Connect to Your Computer with Remote Assistance link (found beneath the Ask for



Assistance heading). The Remote Assistance menu appears.



Click the Invite Someone to Help you link.



Three options appear; users seeking help can either send an invitation through Windows Messenger or Microsoft Outlook or save invitation.

Click on save invitation as a file (Advance)



you should enter your name and set the invitation's expiration period and click Continue.

Remote Assistance - Save Invitation

Enter your name

From (the name you would like to appear on the invitation):

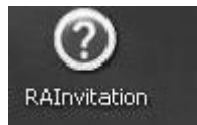
Set the invitation to expire

To lessen the chance that someone fraudulently gains access to your computer you can limit the time in which a recipient can accept a Remote Assistance invitation. Specify the duration that this invitation will remain open.

01 Hours

You should specify a location for the remote assistance file and click Save.

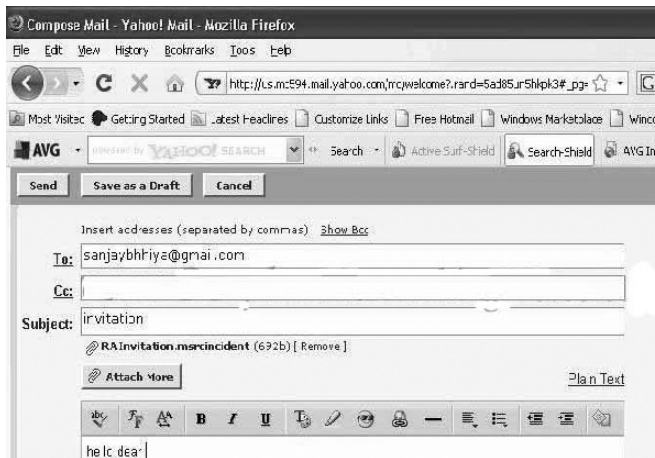
Windows will save the remote connection file (named **RAInvitation.msincident** by default) to the location the end user specifies; you will then have to forward it to the administrator or support technician.



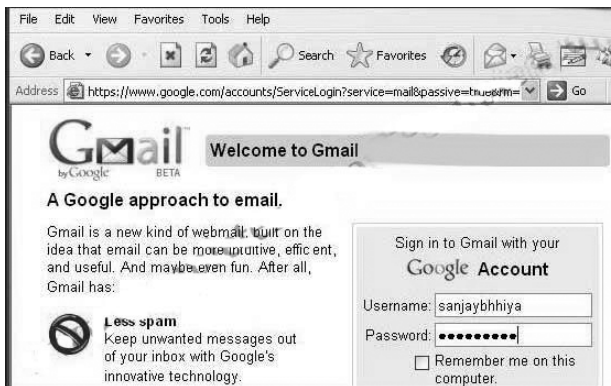
Login from your e-mail account



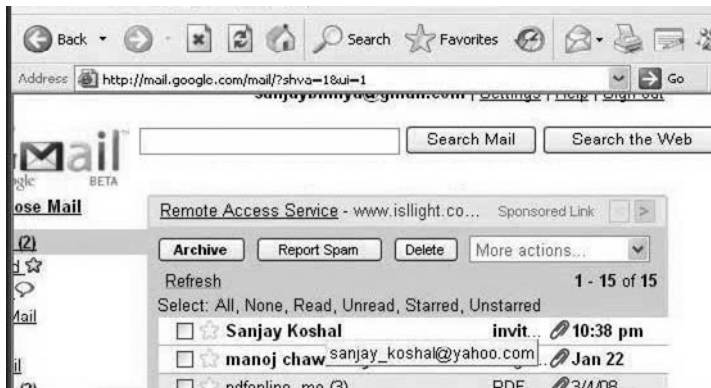
Attach invitation and send mail



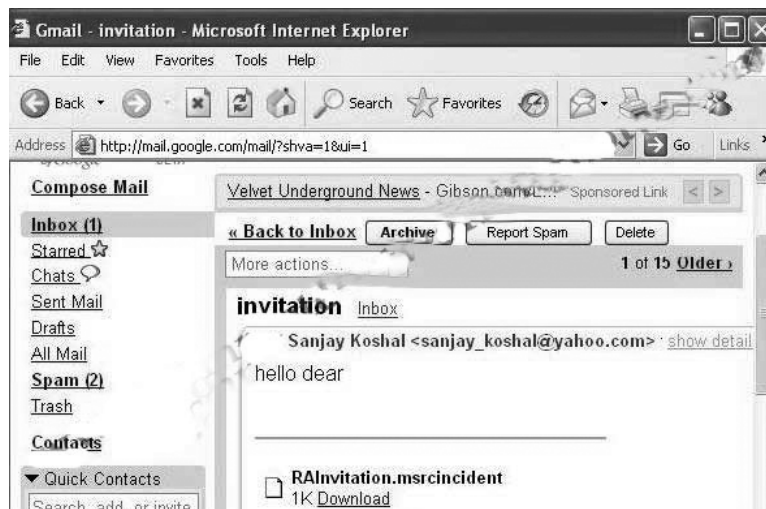
Administrator should login from his e-mail account



Open the mail containing invitation

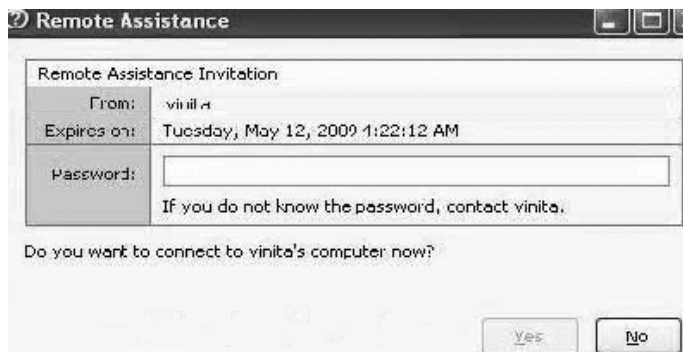


Now download the invitation



Once the remote assistance invitation is downloaded, administrators can follow these steps to render assistance:

- To accept the Remote Assistance invitation, the administrator should double-click the attachment. Before doing so, it's a good idea for the administrator to confirm the user, in fact, sent the request. When doing so, the administrator can learn the password the client entered for the remote assistance request.
- Upon double-clicking the attachment, the administrator will have to supply the password and click OK



The client will receive a dialog box stating that the administrator wishes to connect to the user's desktop. The client must click yes to enable the connection.



Now administrator can provide text base help



- If the administrator wishes to take control of the user's system, the administrator can click the **Take Control** icon that appears at the top of the Remote Assistance window.
- Once the administrator or support technician has clicked Take Control, the end user will see a dialog box stating that the user providing the assistance would like to share control of the computer to help solve the problem. The user must click Yes to permit the support tech with access. When the remote user clicks Yes, the staff member providing support will receive a confirmation message stating the helper is now in control of the user's desktop. To surrender desktop control, the administrator need only press the Esc key; the end user can terminate the administrator's control at any time by **Pressing the Esc key** (or disconnecting the session using the Disconnect button from the Remote Assistance menu).

Having the ability to view or actually control a remote user's desktop drastically simplifies troubleshooting and repair operations. All the end user must do is send the Remote Assistance request to an administrator. The administrator or support tech needs only to connect to the remote system and perform diagnostic actions and repairs. The user and support tech can exchange chat messages with one another using the provided window.

Confirming proper firewall configuration

Occasionally Remote Assistance connections fail to connect. A typical culprit, ironically, is Windows own firewall. Note that the Windows Firewall (installed by default with Windows XP Service Pack 2) must be properly configured to enable connectivity. Follow these steps to confirm Windows Firewall isn't blocking Remote Assistance connections:

- Click **Start**.
- Click **Control Panel**.
- Click **Windows Firewall**.
- Select the **Exceptions tab**.
- Ensure the **Remote Assistance box is checked**.

Chapter - 11

print Management

Introduction

A printer is an output device that produces text and graphics on paper.

Major types of printer:

Printers can be divided into two main groups, impact printer and non-impact printer. Impact printer produces text and images when tiny wire pins on print head strike the ink ribbon by physically contacting the paper. Non-impact printer produces text and graphics on paper without actually striking the paper.

Printers can also be categorized based on the print method or print technology. The most popular ones are inkjet printer, laser printer, dot-matrix printer and thermal printer. Among these, only dot-matrix printer is impact printer and the others are non-impact printers. Some printers are named because they are designed for specific functions, such as photo printers, portable printers and all-in-one / multifunction printers. Photo printers and portable printers usually use inkjet print method whereas multifunction printers may use inkjet or laser print method. Inkjet printers and laser printers are the most popular printer types for home and business use. Dot matrix printer was popular in 70's and 80's but has been gradually replaced by inkjet printers for home use. However, they are still being used to print multi-part forms and carbon copies for some businesses. The use of thermal printers is limited to ATM, cash registers and point-of-sales terminals. Some label printers and portable printers also use thermal printing. Due to the popularity of digital camera, laptop and SoHo office (small office / home office), the demand for photo printers, portable printers and multifunction printers has also increased substantially in recent years.

Inkjet printers:

Inkjet printers are non-impact printers which print text and images by spraying tiny droplets of liquid ink onto paper. They are the most popular printers for home use.

Currently, most inkjet printers use either thermal inkjet or piezoelectric inkjet technology. Thermal inkjet printer uses heating element to heat liquid ink to form vapor bubble, which forces the ink droplets onto the paper through the nozzle. Most inkjet manufacturers use this technology in consumer inkjet printers. Piezoelectric inkjet technology is used on all Epson printers and industrial inkjet printers. Instead of using heating element, these printers use a piezoelectric crystal in each nozzle. The piezoelectric crystal changes shape and size based on the electric current received, and forces tiny droplets of ink onto the paper from the nozzle. Thermal inkjet printers use aqueous ink which is a mixture of water, glycol and dyes. These inks are inexpensive but they can only be used on paper or specially coated materials. Piezoelectric inkjet printers allow the use of a wider range of inks, such as solvent inks, UV-curable inks, dye sublimation inks, and can print text

and graphics on different uncoated materials. The inkjet head design is also divided into two main groups: fixed-head and disposable head. Fixed-head is built into the printer and should last for the whole life of the printer. It produces more accurate output than cheap disposable head. The ink cartridges for fixed head printers are also cheaper as the print head does not need to be replaced. However, if the head is damaged, the entire printer has to be replaced. Disposable head is included in replacement ink cartridge. It is replaced each time an ink cartridge runs out of ink. This increases the cost of ink cartridges and also limits the use of high quality print head in these cartridges. However, a damaged print head is not a problem as one can easily replace it with a new ink cartridge. Some printer manufacturers use disposable ink and disposable print head separately. The print head can last much longer than cheap disposable head and is suitable for high volume printing. However, it can also be replaced easily if the head is clogged or damaged. Although inkjet printers are generally used in home and small businesses, some manufacturers, such as Hewlett Packard, have produced high end inkjet printers for industrial use. These professional inkjet printers are usually used to print advertising graphics or technical drawings.

advantages of inkjet printers:

- 1) Low cost
- 2) High quality of output, capable of printing fine and smooth details
- 3) Capable of printing in vivid color, good for printing pictures
- 4) Easy to use
- 5) Reasonably fast
- 6) Quieter than dot matrix printer
- 7) No warm up time

Disadvantages of inkjet printers:

- 1) Print head is less durable, prone to clogging and damage
- 2) Expensive replacement ink cartridges
- 3) Not good for high volume printing
- 4) Printing speed is not as fast as laser printers
- 5) Ink bleeding, ink carried sideways causing blurred effects on some papers
- 6) Aqueous ink is sensitive to water; even a small drop of water can cause blurring
- 7) Cannot use highlighter marker on inkjet printouts.

Laser printers:

Laser printers are non-impact printers which can print text and images in high speed and high quality resolution, ranging from 600 to 1200 dpi. Unlike inkjet printers, laser printer use toner (black or colored powder) instead of liquid inks. A laser printer consists of these

major components: drum cartridge, rotating mirror, toner cartridge and roller. The drum cartridge rotates as the paper is fed through. The mirror deflects laser beam across the surface of the drum. Laser beam creates charge that causes the toner to stick to the drum. As the drum rotates and presses on paper, toner is transferred from the drum to paper, creating images. Rollers then use heat and pressure to fuse toner to paper. Colored laser printers add colored toner in three additional passes.

advantages of laser printers:

- 1) High resolution
- 2) High print speed
- 3) No smearing
- 4) Low cost per page (compared to inkjet printers)
- 5) Printout is not sensitive to water
- 6) Good for high volume printing

Disadvantages of laser printers:

- 1) More expensive than inkjet printers
- 2) Except for high end machines, laser printers are less capable of printing vivid colors and high quality images such as photos.
- 3) The cost of toner replacement and drum replacement is high
- 4) Bulkier than inkjet printers
- 5) Warm up time needed

Dot-matrix printer

Dot-matrix printer is an impact printer that produces text and graphics when tiny wire pins on the print head strike the ink ribbon. The print head runs back and forth on the paper like a typewriter. When the ink ribbon presses on the paper, it creates dots that form text and images. Higher number of pins means that the printer prints more dots per character, thus resulting in higher print quality. Dot-matrix printers were very popular and the most common type of printer for personal computer in 70's to 80's. However, their use was gradually replaced by inkjet printers in 90's. As of today, dot matrix printers are only used in some point-of-sales terminals, or businesses where printing of carbon copy multi-part forms or data logging are needed.

advantages of dot matrix printer:

- 1) Can print on multi-part forms or carbon copies
- 2) Low printing cost per page
- 3) Can be used on continuous form paper, useful for data logging
- 4) Reliable, durable

Disadvantages of dot matrix printer:

- 1) Noisy
- 2) Limited print quality
- 3) Low printing speed
- 4) Limited color printing

Thermal printers

Thermal printers use two types of printing technologies: **direct thermal** and **thermal transfer** printing. Traditional thermal printers use direct thermal method by pushing electrically heated pins against heat-sensitive paper (thermal paper). The coating on the thermal paper turns black in the areas where it is heated, producing characters or images. Direct thermal printers have no ink, toner or ribbon. These printers are durable, easy to use and cost less to print than other printers. However, the thermal paper is sensitive to heat, light, water, and abrasion and the text and images may fade over time. In thermal transfer printing, a thermal print head applies heat to a heat-sensitive ribbon, which melts ink onto paper and a wide range of materials to form text and images. The printouts can be extremely durable and can be stored over long period of time. Thermal printers are often used in cash registers, ATM and point-of-sales terminals. Direct thermal printing was used in some older fax machines before the 21st century. However, these old models are now replaced by new machines which use laser and inkjet printing. Thermal printing is still considered as the best technology for bar code printing because it produces accurate, high quality images with exact bar widths. Some portable printers and most label printers still use thermal printing method. Thermal printer is not the same as thermal inkjet printer. The latter uses inkjet print technology by heating liquid ink to form vapor bubble, which forces the ink droplet onto the paper from the nozzle.

Specialty printers**photo printer**

Photo printers are color printers that produce photo lab quality pictures on photo paper. They can also be used to print documents. These printers have a very high number of nozzles and can print very fine droplets for improved image quality. Some photo printers also have media card readers. They can print 4" x 6" photos directly from the media card of digital cameras without a computer in between. Theoretically, most inkjet printers and high end laser printers are capable of printing high quality pictures. Sometimes, these printers are marketed as "photo printers". However, a dedicated photo printer is designed to print photos effectively and economically. Apart from a higher number of nozzles and very fine droplets, these printers also use additional cartridges, such as photo cyan, light magenta and light black. These additional color cartridges allow the printing of more vivid and realistic photos and the result is better than ordinary inkjet and laser printers.

portable printer

Portable printers are small, lightweight inkjet or thermal printers that allow computer users to print from laptop computers when traveling. They are easy to carry, convenient to use but generally more expensive than normal inkjet printers due to the compact design. Their printing speed is also lower than normal printers. Some portable printers are designed to print photos immediately from digital cameras and are known as portable photo printers.

Multi Function / all-in-One printers

Multifunction printer (MFP) is also known as all-in-one printer or multifunction device (MFD). It is a machine that includes several functionalities including printer, scanner, copier and fax. Multifunction printer is very popular in SoHo (Small office / Home office) offices. It can use either inkjet or laser print method. Some multifunction printers also have media card readers, allowing printing of pictures directly from digital cameras without using a computer.

advantages of multi function printers:

- 1) Low cost – it is often cheaper to buy a multifunction printer than individual components (fax machine, scanner, printer, and copier) separately
- 2) Take up less room

Disadvantages of multi function printers:

- 1) If one component is broken, the entire machine has to be replaced
- 2) Failure in any component will affect other functions
- 3) The print quality and speed may be lower than some stand alone components

Installing and Configuring Printers:

Two types of print devices are used on a network:

- **Local print device** A print device that is physically attached to the user's computer and employed only by the user who's logged on to that computer.
- **Network print device** A print device that is set up for remote access over the network. This can be a print device attached directly to a print server or a network-attached print device.

To install or configure a new printer, you must be a member of one of the privileged groups shown in Table, on the following page. On Windows NT servers, as you can see, Administrators, Printer Operators, and Server Operators can configure printers. On Windows NT workstations, Administrators and Power Users can configure printers.

table: Groups that Can Configure printers, according to System type

Group	Windows Nt Workstation	Windows Nt Server
Administrators	X	X
Power Users	X	
Print Operators		X
Server Operators		X

To connect to and print documents to the printer, you must have the appropriate access permissions. The sections that follow describe procedures for installing and configuring printers. You install new network printers on print servers. You connect to network printers on remote systems, such as a user’s workstation.

Installing Network print Devices

Print devices can connect directly to the network or to an actual system on the network by way of a parallel or serial port. Regardless of which is used, print servers are used to manage network printing. Any Windows NT workstation or server can be configured as a print server. The primary job of the print server is to share the print device out to the network and to handle print spooling.

You install new network printing as follows:

1. Log on locally to the print server.
2. Follow the print device manufacturer’s instructions for installing printer services and protocols on the print server as necessary. For example, to use a network print device that is physically attached to the network rather than to a computer printer port, you may need to install the DLC (Data Link Control) protocol. To do this, follow these steps:
 - Double-click on the Network icon in the Control Panel.
 - In the Network dialog box, select the Protocols tab and then click on the Add button.
 - In the Select Network Protocol dialog box, select DLC Protocol from the Network Protocol list.
 - Choose OK.
 - When prompted, insert the appropriate disk or disks and specify the location of the protocol drivers.
 - Close the Network dialog box and reboot the print server when prompted.
3. Double-click on the Printers icon in the Control Panel or select Settings in the Start menu and then choose the Printers option. This opens the Printers folder shown in Figure 1. You should see the Add Printer icon and an icon for each additional printer configured for the system.

4. Double-click on the Add Printer icon to open the Add Printer Wizard shown in Figure 2.



Figure 1: The Printers folder allows you to add printers, update currently configured printers, and manage print server properties.

5. Select the My Computer radio button, and then click on the Next button.
6. Next, you need to configure the port or ports used by the printer (see Figure 3, on the following page).
- For a print device physically connected to the print server, select the appropriate LPT or COM port. If you select more than one port, Windows NT prints to the first available port. You can also print to a file. If you do, Windows NT prompts users for a file name each time they print.
 - For a print device physically connected to the network, click on the Add Port button. This opens the Printer Ports dialog box. You can now select the appropriate port type for the printer you're configuring, such as Digital Network Port, Lexmark DLC Network Port, or Lexmark TCP/IP Port. If necessary, click on the New Monitor button to specify a new print monitor. Then complete the process by clicking on the New Port button to create the new port. Once the port is defined, you can select it from the Available Ports list.



Figure 2: The Add Printer Wizard lets you configure local print devices and remote access to network printer servers.



Figure 3: In the Add Printer Wizard window, select a printer port for a local printer or click on the Add Port button for a network-attached printer.

Note: The appropriate port type should be specified in the print device's documentation. Digital Network Port is used with DECNet and DEC printers. LPR port is used to create a print gateway to a UNIX system. DLC Network Port is used with Lexmark and HP print devices (and you may see Lexmark DLC Network Port or Hewlett-Packard DLC Network Port).

- When you're finished configuring ports, click on the Next button to display the window shown in Figure 13-4. You must now specify the print device manufacturer and model. This allows Windows NT to assign a printer driver to the print device. After you choose a print device manufacturer, choose a printer model. If the print device manufacturer and model you're using isn't displayed in the list, choose Have Disk to install a new driver.



Figure 4: Select a print device manufacturer and model with the Add Printer Wizard.



Figure 5: Name the printer in the Add Printer Wizard.

Note: If a driver for the specific printer model you're using isn't available, you can usually select a generic driver or a driver for a similar print device. Consult the print device documentation for specific pointers.

8. Click on the Next button to assign a name to the printer, as shown in Figure 5. This is the name you'll see in the Printers folder of Control Panel. You can also specify whether the printer is the default used by the local system. Choose Yes or No and click on the Next button.
9. You can now specify whether the printer is available to remote users (see Figure 6, on the following page). To create a network printer that is accessible to remote users, click on the Shared radio button and enter a name for the shared resource. In a large organization, you'll want the share name to be logical and helpful in locating the printer. For example, you may want to name the printer that points to the print device in the northeast corner of the twelfth floor Twelve.

Note: If Microsoft Windows 3.1 or MS-DOS systems will access the printer, be sure the printer name conforms to the standard MS-DOS naming rule. For example, use the name NORTH12.PRT rather than NORTH_PRINTER_FLOOR12.

10. In the same window, select the type of computers that will use the printer. The selections you make here are used to install printer drivers for other operating systems. When users from these systems access the printer, the driver can be downloaded to their systems. Normally, this is done if the driver on the print server is newer than the driver on the user's computer.

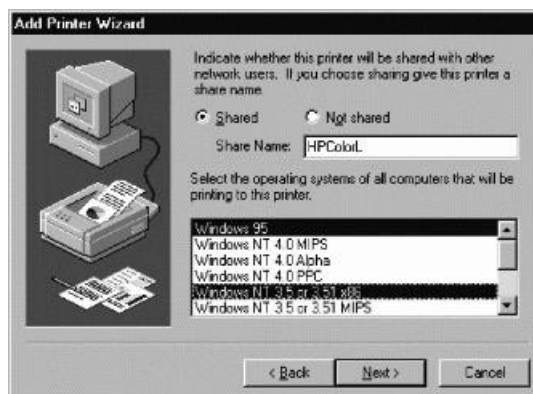


Figure 6: Share the network printer and assign it a name in the Add Printer Wizard. Afterward, select the operating systems of computers that will use the printer.

Note: If you make selections in this step, you'll need the Windows NT CD-ROM or the manufacturer's distribution disks.

11. The final window lets you test the installation by printing a test page to the print device. If you want to do this, select yes. Otherwise, select no. When you're ready to install the printer, click on the Finish button.

When the Add Printer Wizard finishes installing the new printer, the Printers folder in the Control Panel will have an additional icon with the name set the way you previously specified. You can change the printer properties and status at any time. For more information, see the section of this chapter titled "Configuring Printer Properties."

tip If you repeat this process, you can create additional printers for the same print device. All you need to do is change the printer name and share name. Having additional printers for a single print device allows you to set different properties to serve different needs. For example, you could have a high priority printer for print jobs that need to be printed immediately and a low priority printer for print jobs that aren't as urgent.

Installing Local print Devices

A local print device is physically connected to a user's computer and accessible only on that computer. Installing printing on a local system is much like installing network printing. The key difference is that the printer isn't shared. Accordingly, follow the steps for creating a printer as specified in the section of this chapter titled "Installing Network Print Devices." Then in step 9, specify that the printer is not shared.

Note: A local printer can easily become a network printer. To learn how to do this, see the section of this chapter titled "Starting and Stopping Printer Sharing."

Connecting to printers Created on the Network

Once you create a network printer, remote users can connect to it and use it much like any other printer. You'll need to set up a connection on a user-by-user basis or have users do

this themselves. To create the connection to the printer on a Windows NT system, follow these steps:

1. With the user logged on, double-click on the Printers icon in the Control Panel or select Settings in the Start menu and then choose the Printers option. This opens the Printers folder shown in Figure 1.
2. Double-click on the Add Printer icon to open the Add Printer Wizard shown in Figure 2.
3. Select the Network Printer Server radio button, and then click on the Next button.
4. Using the Connect to Printer dialog box shown in Figure 7, select the shared printer. Click on the items in the Shared Printers list to work your way down to the shared printer to which you want to connect. When the printer is selected, click OK.
5. Determine whether the printer is the default used by Windows applications. Choose Yes or No and then click on the Next button.
6. Choose Finish to complete the operation.

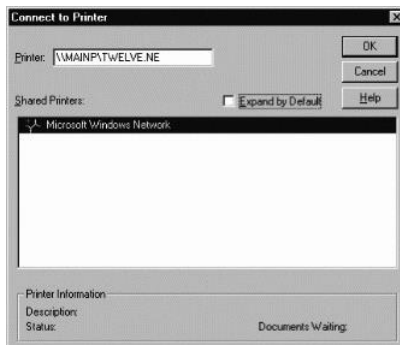


Figure 7: In the *Connect to Printer* dialog box, work your way down from *Microsoft Windows Network* to the shared printer.

The user can now print to the network printer by selecting the printer in an application. The Printers tab on the user's computer shows the new network printer. You can configure local property settings using this icon.

tip As you might expect, Windows NT provides several different ways to connect to a network printer. You can also set up a printer by browsing to the print server in Network Neighborhood and then accessing the server's Printers folder by double-clicking on it. Next, double-click on the icon of the printer to which you want to connect. This opens a management window for the printer. Finally, select Install from the Printer menu.

Solving Spooling problems

Windows NT uses a service to control the spooling of print jobs. If this service isn't running, print jobs can't be spooled. You can check the status of the Spooler using the Services utility in Control Panel. Follow these steps to check and restart the Spooler service:

1. Click Settings from the Start menu and then select Control Panel.
2. Double-click on Services.
3. Select the Spooler service as shown in Figure 8. The service status should read "Started." If it doesn't, click on the Startup button to restart the service. The Startup option should read Automatic. If it doesn't, click on the Startup button and change the startup type to Automatic.

tip Spoolers can become corrupted. Symptoms include a frozen printer or one that doesn't send jobs to the print device. Sometimes the print device may print pages of garbled data. In most of these cases, stopping and starting the Spooler service will resolve the problem.

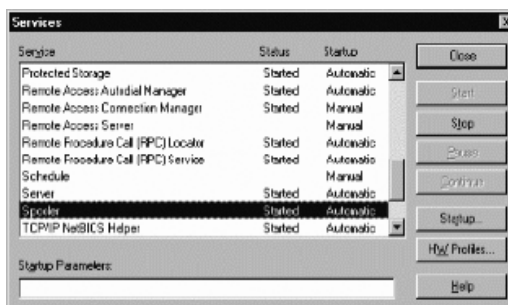


Figure 8: The Spooler service handles print spooling.

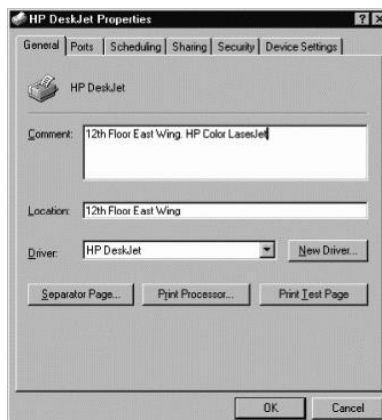


Figure 9: Set printer properties with the dialog box for the printer you want to configure.

Configuring a Printer in Windows 7

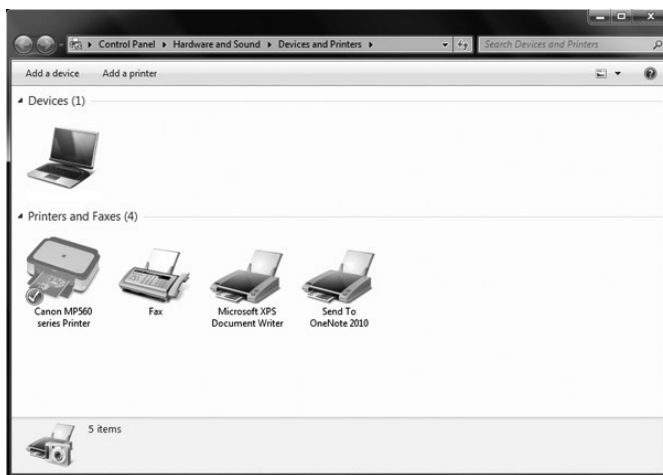
In most cases, setting up and configuring a printer in Windows 7 or Vista is straightforward. Follow the instructions that came with your printer's software on an installation CD, or download that information from the printer manufacturer's Website. If you can't find the information there, follow this guide to set up a printer manually on your PC. We show

the steps to add a local and network printer in Windows 7. The process is very similar in Windows Vista.

Step by Step: Configuring a Printer in Windows 7

Step 1 Click *Start, Devices and Printers*.

Step 2 In the window that pops up, click the *Add a Printer* button on the toolbar near the top.



Step 3 In the next window, select how you will connect to your printer. If you are trying to connect your printer directly to your PC with a cord, click *Add a local printer*. If you are trying to connect your printer wirelessly (over a network or over Bluetooth) or you wish to connect to a printer wired to your network, click *Add a network, wireless or Bluetooth printer*.

For Local printers

Step 4 Be sure that *Use an existing port* is selected, and click *Next*.

Choose a printer port

A printer port is a type of connection that allows your computer to exchange information with a printer.

Use an existing port:

Create a new port:

Type of port:

Step 5 Choose your printer manufacturer from the left list, followed by the model in the right list, and then click *next*. You may need to click the *Windows Update* button to have

Windows search an expanded list. Or, if you have the disk that was packaged with your printer, clicks have *Disk*.

Step 6 Windows will lead you through some additional steps to complete the installation.

For Network and Wireless printers

Step 4 Windows will attempt to locate your printer.

Step 5 Select your printer from the list and click *next*. Follow the additional prompts to complete the installation.

Step 6 If your printer is not set as the default printer and you want it to be, click *Start, Devices and Printers*. Right-click the printer you wish to make the default, and select *Set as default printer* from the context menu. You can also delete the printer by clicking *Remove device* from this context menu.

Chapter - 12

Backup & restore

A network backup means one person can do the work, but users must put their important files on the server, the network traffic is more intensive though and the registry cannot be backed up over the network. A local backup uses less network resources but the users are responsible for carrying out their own backup to tape. If a file is in use, NT backs up the last saved version. The registry on a domain controller contains all the user accounts and must be backed up. It can only be backed up to a tape within the same computer so make sure that the tape drive is in the domain controller. Files have an archive attribute which is a backup marker. If it is set then the marker indicates that the file has been backed up.

there are the following backup types:

- **Normal** - Selected files, marking their archive attributes a normal backup copies all selected files and marks each file as having been backed up (in other words, the archive attribute is cleared). With normal backups, you need only the most recent copy of the backup file or tape to restore all of the files. You usually perform a normal backup the first time you create a backup set.
- **Copy** - selected files without marking their archive attributes. This is good for making tape copies that do not interfere with archive backups, since it does not set the archive attribute.

A copy backup copies all selected files but does not mark each file as having been backed up (in other words, the archive attribute is not cleared). Copying is useful if you want to back up files between normal and incremental backups because copying does not affect these other backup operations.

- **Incremental** - selected files, marking their archive attributes, but only backs up the ones that have changed since the last backup. An incremental backup backs up only those files created or changed since the last normal or incremental backup. It marks files as having been backed up (in other words, the archive attribute is cleared). If you use a combination of normal and incremental backups, you will need to have the last normal backup set as well as all incremental backup sets in order to restore your data.
- **Differential** - Selected files, NOT marking their archive attributes, but only backs up the ones that have changed since the last backup. Differential backup copies files created or changed since the last normal or incremental backup. It does not mark files as having been backed up (in other words, the archive attribute is not cleared). If you are performing a combination of normal and differential backups, restoring files and folders requires that you have the last normal as well as the last differential backup.
- **Daily** - Only backs up files that have changed that day, does not mark their archive attributes. A daily backup copies all selected files that have been modified the day

the daily backup is performed. The backed-up files are not marked as having been backed up (in other words, the archive attribute is not cleared).

A Backup Set is one backup operation for files and folders from a single volume. A Catalog is a picture of the backup and this is placed on the backup tape. The tape catalog shows the backup sets on a tape whilst the backup set catalog shows the files and folders. A Backup Log is a text file that records the backup operations. This log can contain the date, the user, and the type of backup, the files, the computer, the tape drive location and the tape-set number. The Backup program is run from the Administrative Tools menu (erasing a tape is achieved by selecting Erase Tape). In the drives window, check the files and folders that you need to back up. When you click Backup you can input a tape name and select the following options:

- **append** - add a new backup set to existing backup sets.
- **replace**
- **Verify after Backup**
- **Backup registry**
- **restrict access to Owner or administrator**
- **hardware Compression** - The tape drive needs to support this
- **pick the backup type.**
- **Log Information** - Decide a name of the log file to be stored in

The first two lines connect the server on to computers called marry and john and the volumes x: and y: are mapped to the public folders on these computers. The next line uses the **ntbackup backup source paths destination path** command and it has the following syntax:

- /a - appends
- /b - backs up the local registry
- /d "text" - description
- /e - summary log instead of default full detail log.
- /l "filename" - the log filename
- /r - limits access to the administrators, owner or backup operators.
- /t Normal | Copy | Incremental | Differential | Daily
- /v - verify
- /hc:on | off - hardware compression

take the following steps to perform a scheduled backup:

- In Administrative Tools click on Server Manager
- Under **Computer**, select the computer name and click **Services** on the Computer menu.

- Under Service, select **Schedule** and click **Startup**.
- Under **Startup type** select **automatic**
- Under Service, select **Schedule** and click **Start**
- Use the **at** command with the following syntax **at \\computer_name id /delete time interactive /every: date next: date "command"** , where command would be ntbackup.

Delete means that the scheduled command is cancelled. Interactive means that the job will be visible on the desktop of the user.

restoring data needs the following steps:

- When restoring a backup the tape catalog must be loaded first. This is achieved by starting the Backup program and clicking **Catalog** on the **Operation** menu.
- Next, load the backup set catalog by clicking on the appropriate backup set folder. (Question marks turn to + signs when the catalogs are loaded and a red x indicates a corrupted file).
- Check the entire backup sets that you wish to restore, or even individual files and folders within a backup set.
- Click **restore**.
- Select the drive to restore to, this can be different from the original. You can restore the local registry, the file permissions and you can choose to verify after restore has occurred.
- You can create a log using **Select Log Options**

Other Backup software's:

- 1) VERITAS backup
- 2) Nero Backup tool
- 3) R- Drive Image tool
- 4) ABC Backup software

Chapter – 13

transmission Media (Cable)

The means through which data is transferred from one place to another is called transmission or communication media. There are two categories of transmission media used in computer communications.

- **Bounded/Guided Media**
- **Unbounded/Unguided Media**

BoUnded Media:

Bounded media are the physical links through which signals are confined to narrow path. These are also called guided media. Bounded media are made up of an external conductor (Usually copper) bounded by jacket material. Bounded media are great for LABS because they offer high speed, good security and low cost. However, some time they cannot be used for distance communication. Three common types of bounded media are used of the data transmission. These are:

- Coaxial Cable
- Twisted Pairs Cable
- Fiber Optics Cable

Coaxial CaBle:

Coaxial cable is very common & widely used commutation media. For example TV wire is usually coaxial. Coaxial cable gets its name because it contains two conductors that are parallel to each other. The center conductor in the cable is usually copper. The copper can be either a solid wire or stranded martial. Outside this central Conductor is a non-conductive material. It is usually white, plastic material used to separate the inner Conductor from the outer Conductor. The other Conductor is a fine mesh made from Copper. It is used to help shield the cable form EMI. Outside the copper mesh is the final protective cover. The actual data travels through the center conductor in the cable. EMI interference is caught by outer copper mesh. There are different types of coaxial cable vary by gauge & impedance. Gauge is the measure of the cable thickness. It is measured by the Radio Grade measurement, or RG number. The high the RG number, the thinner the central conductor core, the lower the number the thicker the core.

here the most common coaxial standards.

- 50-Ohm RG-7 or RG-11: used with thick Ethernet.
- 50-Ohm RG-58 : used with thin Ethernet
- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62: used with ARCNET.

CharaCteriStiCs of Coaxial CaBlE

- Low cost
- Easy to install
- Up to 10Mbps capacity
- Medium immunity from EMI
- Medium of attenuation

advantaGes Coaxial CaBlE

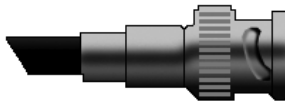
- Inexpensive
- Easy to wire
- Easy to expand
- Moderate level of EMI immunity

disadvantage Coaxial Cable

- Single cable failure can take down an entire network.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector. Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather



Coaxial CaBel



BnC Connector

twisted Pair CaBlE:

The most popular network cabling is twisted pair. It is light weight, easy to install, inexpensive and support many different types of network. It also supports the speed of 100 mbps. Twisted pair cabling is made of pairs of solid or stranded copper twisted along each other. The twists are done to reduce vulnerability to EMI and cross talk. The number of pairs in the cable depends on the type. The copper core is usually 22-AWG or 24-AWG, as measured on the American wire gauge standard. There are two types of twisted pairs cabling

1. Unshielded twisted pair (UTP)
2. Shielded twisted pair (STP)

Unshielded twisted Pair (Utp) Cable

UTP is more common. It can be either voice grade or data grade depending on the condition. UTP cable normally has an impedance of 100 ohm. UTP cost less than STP and easily available due to its many use. There are five levels of data cabling.

Category 1: These are used in telephone lines and low speed data cable.

Category 2: These cables can support up to 4 mps implementation.

Category 3: These cable supports up to 16 mps and are mostly used in 10 mps.

Category 4: These are used for large distance and high speed. It can support 20mps.

Category 5: This is the highest rating for UTP cable and can support up to 100mps.

UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use RJ-11 connector and 4 pair cable use RJ-45 connector.

CharaCteriCstiCs of Utp CaBle:

- Low cost
- Easy to install
- High speed capacity
- High attenuation
- Effective to EMI
- 100 meter limit

advantaGes of Utp CaBle:

- Easy installation
- Capable of high speed for LAN
- Low cost

disadvantaGes of Utp CaBle:

- Short distance due to attenuation.

shielded twisted Pair (stP)

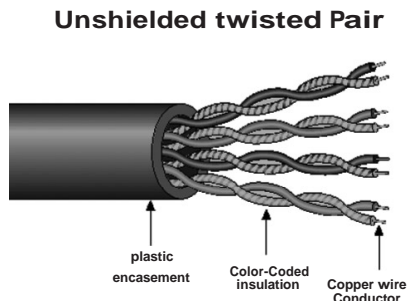
It is similar to UTP but has a mesh shielding that's protects it from EMI which allows for higher transmission rate. IBM has defined category for STP cable.

type 1: STP features two pairs of 22-AWG

type 2: This type include type 1 with 4 telephone pairs

type 6: This type feature two pairs of standard shielded 26-AWG

type 7: This type of STP consists of 1 pair of standard shielded 26-AWG



type 9: This type consist of shielded 26-AWG wire

CharaCteriCstiCs of stP

- Medium cost
- Easy to install
- Higher capacity than UTP
- Higher attenuation, but same as UTP
- Medium immunity from EMI
- 100 meter limit

advantaGes of stP:

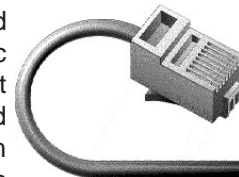
- Shielded
- Faster than UTP and coaxial

disadvantaGes of stP:

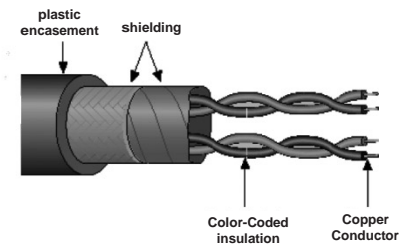
- More expensive than UTP and coaxial
- More difficult installation
- High attenuation rate

UtP & stP ConneCtor:

The standard connector for unshielded twisted pair cabling and shielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector. A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.



shielded twisted Pair CaBle



fiber optics:

Fiber optic cable uses electrical signals to transmit data. It uses light. In fiber optic cable light only moves in one direction for two way communication to take place a second connection must be made between the two devices. It is actually two stands of cable. Each stand is responsible for one direction of communication. A laser at one device sends pulse of light through this cable to other device. These pulses translated into "1's" and "0's" at the other end. In the center of fiber cable is a glass stand or core. The light from the laser moves through this glass to the other device around the internal core is a reflective material known as CLADDING. No light escapes the glass core because of this reflective cladding. Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting

networks between Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is .The center core of fiber cables is made from glass or plastic fibers. A plastic coating then cushions the fiber center, and kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of teflon or PVC.



There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive. Fiber optic cable has bandwidth more than 2 gbps (Gigabytes per Second)

Characteristics of fiber optic Cable:

- Expensive
- Very hard to install
- Capable of extremely high speed
- Extremely low attenuation
- No EMI interference

advantages of fiber optic Cable:

- Fast
- Low attenuation
- No EMI interference

disadvantages fiber optics:

- Very costly
- Hard to install

ethernet Cable summary

specification	Cable type
10BaseT	Unshielded Twisted Pair
10Base2	Thin Coaxial
10Base5	Thick Coaxial

specification	Cable type
100BaseT	Unshielded Twisted Pair
100BaseFX	Fiber Optic
100BaseBX	Single mode Fiber
100BaseSX	Multimode Fiber
1000BaseT	Unshielded Twisted Pair
1000BaseFX	Fiber Optic
1000BaseBX	Single mode Fiber
1000BaseSX	Multimode Fiber

some Guidelines regarding Caballing:

When running cable, it is best to follow a few simple rules:

1. Always use more cable than you need. Leave plenty of slack.
2. Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
3. Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
4. If it is necessary to run cable across the floor, cover the cable with cable protectors.
5. Label both ends of each cable.
6. Use cable ties (not tape) to keep cables in the same location together.

Unbounded Media:

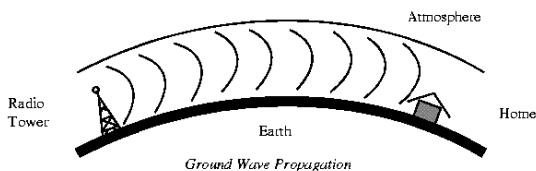
Unguided transmission media is data signals that flow through the air. They are not guided or bound to a channel to follow. They are classified by the type of wave propagation.

rf Propagation

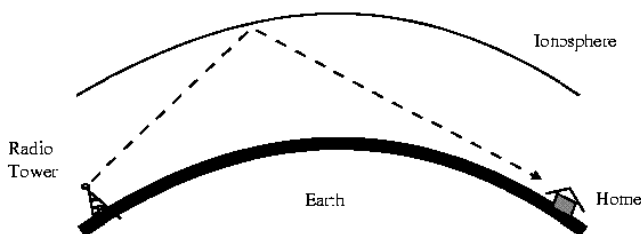
There are three types of RF (radio frequency) propagation:

- Ground Wave
- Ionospheric
- Line of Sight (LOS)

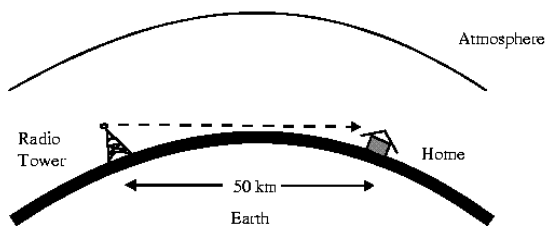
Ground wave propagation follows the curvature of the Earth. Ground waves have carrier frequencies up to 2 MHz AM radio is an example of ground wave propagation.



- ionospheric propagation** bounces off of the Earth's ionospheric layer in the upper atmosphere. It is sometimes called double hop propagation. It operates in the frequency range of 30 - 85 MHz. Because it depends on the Earth's ionosphere, it changes with the weather and time of day. The signal bounces off of the ionosphere and back to earth. Ham radios operate in this range.



- line of sight propagation** transmits exactly in the line of sight. The receive station must be in the view of the transmit station. It is sometimes called space waves or tropospheric propagation. It is limited by the curvature of the Earth for ground-based stations (100 km, from horizon to horizon). Reflected waves can cause problems. Examples of line of sight propagation are: FM radio, microwave and satellite.



radio frequencies

The frequency spectrum operates from 0 Hz (DC) to gamma rays (10¹⁹ Hz).

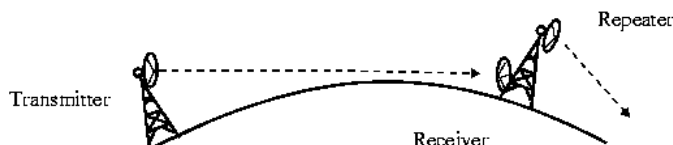
name	frequency (hertz)	examples
Gamma Rays	10 ¹⁹ +	Atomic Energy
X-Rays	10 ¹⁷	Body Scan
Ultra-Violet Light	7.5 x 10 ¹⁵	Writing special Coding
Visible Light	4.3 x 10 ¹⁴	Regular Lights

name	frequency (hertz)	examples
Infrared Light	3×10^{11}	Remote Sensing (TV, Mobile)
EHF - Extremely High Frequencies	30 GHz (Giga = 10^9)	Radar
SHF - Super High Frequencies	3 GHz	Satellite & Microwaves
UHF - Ultra High Frequencies	300 MHz (Mega = 10^6)	UHF TV (Ch. 14-83)
VHF - Very High Frequencies	30 MHz	FM & TV (Ch2 - 13)
HF - High Frequencies	3 MHz	Short Wave Radio
MF - Medium Frequencies	300 kHz (kilo = 10^3)	AM Radio
LF - Low Frequencies	30 kHz	Navigation
VLF - Very Low Frequencies	3 kHz	Submarine Communications
VF - Voice Frequencies	300 Hz	Audio
ELF - Extremely Low Frequencies	30 Hz	Power Transmission

Radio frequencies are in the range of 300 kHz to 10 GHz. We are seeing an emerging technology called wireless LANs. Some use radio frequencies to connect the workstations together, some use infrared technology.

- **Microwave**

Microwave transmission is line of sight transmission. The transmit station must be in visible contact with the receive station. This sets a limit on the distance between stations depending on the local geography. Typically the line of sight due to the Earth's curvature is only 50 km to the horizon! Repeater stations must be placed so the data signal can hop, skip and jump across the country.



Microwaves operate at high operating frequencies of 3 to 10 GHz. This allows them to carry large quantities of data due to their large bandwidth.

advantages:

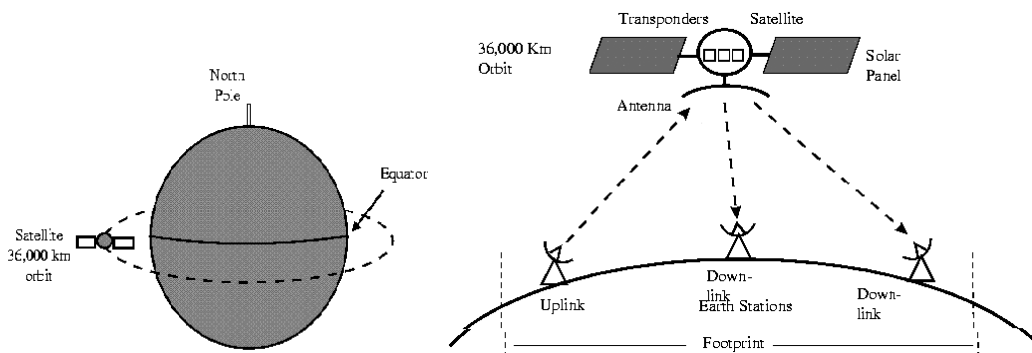
1. They require no right of way acquisition between towers.
2. They can carry high quantities of information due to their high operating frequencies.
3. Low cost land purchase: each tower occupies only a small area.
4. High frequency/short wavelength signals require small antennae.

disadvantages:

1. Attenuation by solid objects: birds, rain, snow and fog.
2. Reflected from flat surfaces like water and metal.
3. Diffracted (split) around solid objects.
4. Refracted by atmosphere, thus causing beam to be projected away from receiver.

• **satellite**

Satellites are transponders (units that receive on one frequency and retransmit on another) that are set in geostationary orbits directly over the equator. These geostationary orbits are 36,000 km from the Earth's surface. At this point, the gravitational pull of the Earth and the centrifugal force of Earth's rotation are balanced and cancel each other out. Centrifugal force is the rotational force placed on the satellite that wants to fling it out into space.

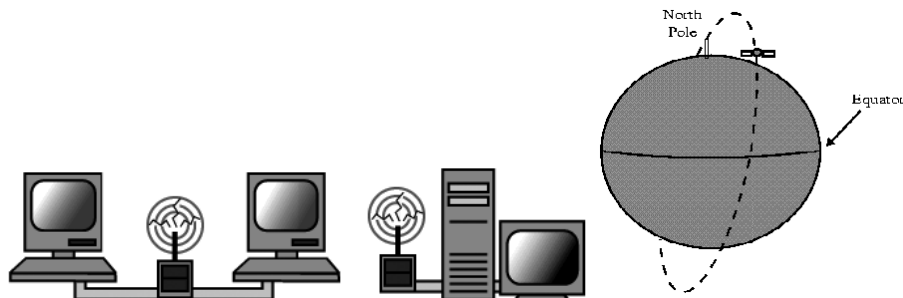


The uplink is the transmitter of data to the satellite. The downlink is the receiver of data. Uplinks and downlinks are also called Earth stations because they are located on the Earth. The footprint is the "shadow" that the satellite can transmit to, the shadow being the area that can receive the satellite's transmitted signal.

• **iridium telecom system**

The Iridium Telecom System is a new satellite system that will be the largest private aerospace project. It is a mobile telecom system intended to compete with cellular phones. It relies on satellites in lower Earth orbit (LEO). The satellites will orbit at an altitude of 900 - 10,000 km in a polar, non-stationary orbit. Sixty-six satellites are planned. The user's handset will require less power and will be cheaper than cellular phones. There will be 100% coverage of the Earth.

wireless lans



More and more networks are operating without cables, in the wireless mode. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite. Wireless networks are great for allowing laptop computers or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables. The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network. Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

wireless standards and speeds

The Wi-Fi Alliance is a global, non-profit organization that helps to ensure standards and interoperability for wireless networks, and wireless networks are often referred to as Wi-Fi (Wireless Fidelity). The original Wi-Fi standard (IEEE 802.11) was adopted in 1997. Since then many variations have emerged (and will continue to emerge). Wi-Fi networks use the Ethernet protocol.

standard	Max speed	typical range
802.11a	54 Mbps	150 feet
802.11b	11 Mbps	300 feet
802.11g	54 Mbps	300 feet

advantages of wireless networks:

- **Mobility** - With a laptop computer or mobile device, access can be available throughout a school, at the mall, on an airplane, etc. More and more businesses are also offering free Wi-Fi access.
- **fast setup** - If your computer has a wireless adapter, locating a wireless network can be as simple as clicking "Connect to a Network" -- in some cases, you will connect automatically to networks within range.
- **Cost** - Setting up a wireless network can be much more cost effective than buying and installing cables.
- **expandability** - Adding new computers to a wireless network is as easy as turning the computer on (as long as you do not exceed the maximum number of devices).

disadvantages of wireless networks:

- **security** - Wireless networks are much more susceptible to unauthorized use. If you set up a wireless network, be sure to include maximum security. You should always enable WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access), which will improve security and help to prevent virtual intruders and freeloaders.
- **interference** - Because wireless networks use radio signals and similar techniques for transmission, they are susceptible to interference from lights and electronic devices.
- **inconsistent connections** - how many times you have hears "Wait a minute, I just lost my connection?" Because of the interference caused by electrical devices and/or items blocking the path of transmission, wireless connections are not nearly as stable as those through a dedicated cable.
- **Power consumption** - The wireless transmitter in a laptop requires a significant amount of power; therefore, the battery life of laptops can be adversely impacted. If you are planning a laptop project in your classroom, be sure to have power plugs and/or additional batteries available.
- **speed** - The transmission speed of wireless networks is improving; however, faster options (such as gigabit Ethernet) are available via cables. In addition, if set up a wireless network at home, and you are connecting to the Internet via a DSL modem (at perhaps 3 Mbps), your wireless access to the Internet will have a maximum of 3 Mbps connection speed.

Chapter - 14

Networking topologies

Introduction

Topologies the first thing to consider about a network is its physical shape, or the design layout, which will be extremely important when you select a wiring scheme and design the wiring for a new installation.

Network really has two shapes, or two types of topology; one is physical and the other is logical. The physical topology is the shape you can see, and the logical topology is the shape that the data travels in.

physical topologies

Physical topology is further divided in two sections

- **point-to-point connections**
- **Multipoint connections**

point-to-point connections

Only two devices are involved in a point-to-point connection, with one wire (or air, in the case of wireless) sitting between them. A point-to-point link is typified by two devices monopolizing the media-similar to two teenagers talking on the telephone with one another, not allowing anyone else to use the phone on either side.

Multipoint connections

In a multipoint connection, multiple machines share the cabling. Multipoint connections might be a group of computers strung together in a long line on an old-fashioned ThinNet (10Base2) cable, or it could be a party line of telephones, all sharing a common phone connection. In fact, even your local cable TV provider uses a multipoint system to get every person in the neighborhood hooked up. In every multipoint connection, each device must be able to identify itself. This is where addressing at the hardware level starts. The device's address must be unique on the channel that it shares with those other devices, or else confusion reigns. Just ask any network administrator who has accidentally assigned the same logical address to two computers. It's not fun dealing with any type of addressing conflict.

Logical topology

A logical topology describes how components communicate across the physical topology. The physical and logical topologies are independent of each other. For example, any variety of Ethernet uses a logical bus topology when components communicate, regardless of the physical layout of the cabling. This means that in Ethernet, you might be using 10BaseT with a physical star topology to connect components together; however, these components are using a logical bus topology to communicate.

Media Type	Physical Topology	Logical Topology
Ethernet	Bus, star, or point-to-point	Bus
FDDI	Ring	Ring
Token Ring	Star	Ring

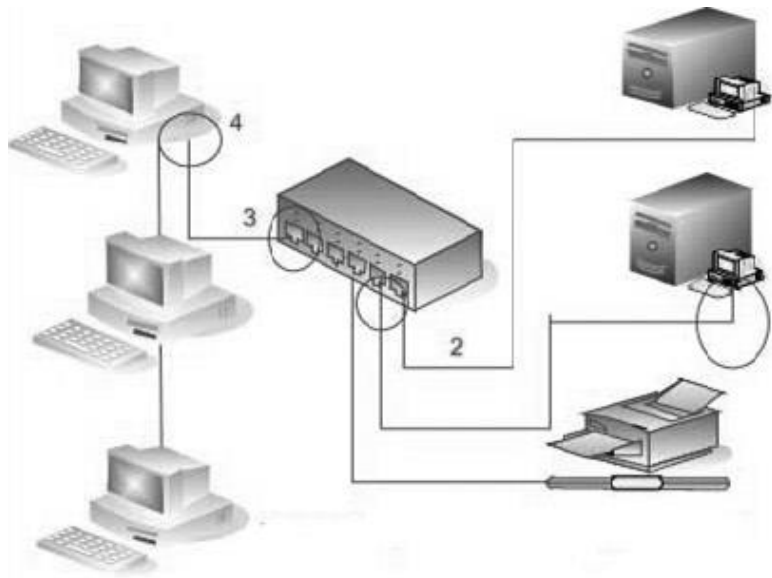
Token Ring is another good example of a communication protocol that has a different physical topology from its logical one. Physically, Token Ring uses a star topology, similar to 10BaseT Ethernet. Logically, however, Token Ring components use a ring topology to communicate between devices. This can create confusion when you are trying to determine how components are connected together and how they communicate. FDDI, on the other hand, is straightforward. FDDI's physical and logical topologies are the same: a ring.

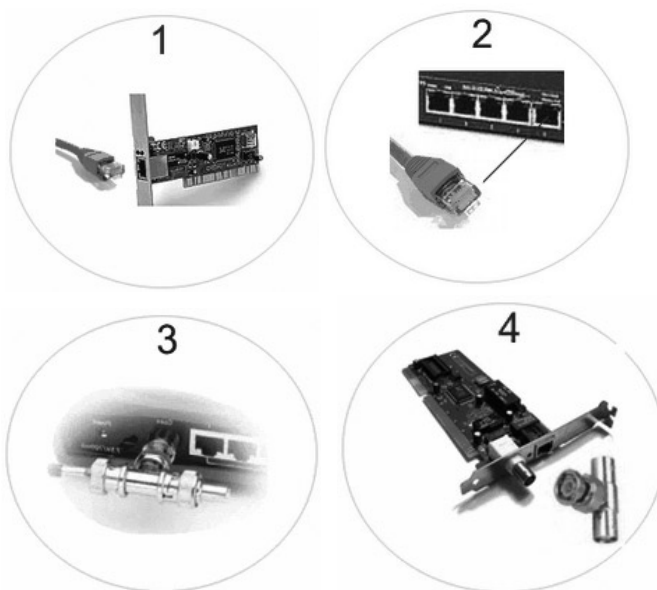
ethernet Networks

In late 1978, the first experimental network system was created to interconnect the Xerox Altos PCs to one another and to servers and laser printers. This first experimental network was called the Alto Aloha Network.

In 1979 the name was changed to Ethernet, to make it clear that the system could support any computer not just Altos and to point out that the new network mechanisms had evolved well beyond the Aloha system.

The base word ether was chosen as a way of describing an essential feature of the system; the physical medium (a cable) carries bits to all stations

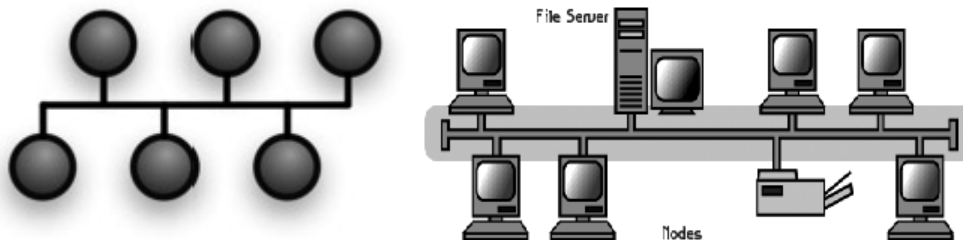




In the diagram you can see two Ethernet configurations. On the left the computers are connected together with a single cable coming from the router/switch, this is called a bus or thin Ethernet configuration. On the right side of the diagram each computer connects directly to the router/switch. This is how most Ethernets are configured today. In this topology management of the network is made much easier (such as adding and removing devices), because of the central point. If computers are connected in a row, along a single cable this is called a bus topology, if they branch out from a single junction or hub this is known as a star topology. When computers are connected to a cable that forms a continuous loop this is called a ring topology. We will go through all of these topologies in coming section.

Different types of logical topologies:

1. Bus topology:



In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds

the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data does match the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable breaks, the entire network will be down.

- **Linear bus**

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Note: The two endpoints of the common transmission medium are normally terminated with a device called a terminator that exhibits the characteristic impedance of the transmission medium and which dissipates or absorbs the energy that remains in the signal to prevent the signal from being reflected or propagated back onto the transmission medium in the opposite direction, which would cause interference with and degradation of the signals on the transmission medium.

- **Distributed bus**

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

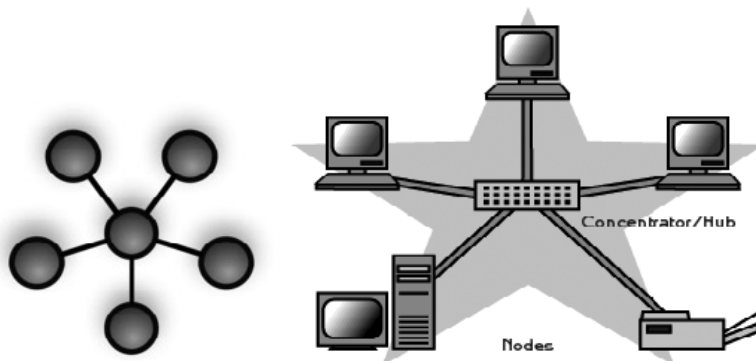
Notes: All of the endpoints of the common transmission medium are normally terminated. The linear bus topology is sometimes considered to be a special case of the distributed bus topology – i.e., a distributed bus with no branching segments. The physical distributed bus topology is sometimes incorrectly referred to as a physical tree topology – however, although the physical distributed bus topology resembles the physical tree topology, it differs from the physical tree topology in that there is no central node to which any other nodes are connected, since this hierarchical functionality is replaced by the common bus.

- **Advantages of a Linear Bus Topology**

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

- **Disadvantages of a Linear Bus Topology**
 - Entire network shuts down if there is a break in the main cable.
 - Terminators are required at both ends of the backbone cable.
 - Difficult to identify the problem if the entire network shuts down.
 - Not meant to be used as a stand-alone solution in a large building.

2. Star topology:



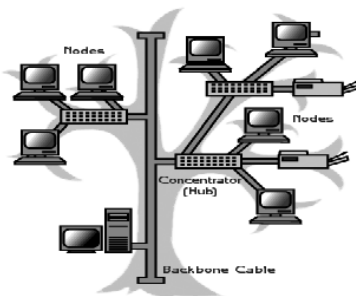
In local area networks with a star topology, each network host is connected to a central hub with a point-to-point connection. All traffic that traverses the network passes through the central hub. The hub acts as a signal repeater. The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the hub represents a single point of failure.

Notes: A point-to-point link (described above) is sometimes categorized as a special instance of the physical star topology – therefore, the simplest type of network that is based upon the physical star topology would consist of one node with a single point-to-point link to a second node, the choice of which node is the 'hub' and which node is the 'spoke' being arbitrary. After the special case of the point-to-point link, the next simplest type of network that is based upon the physical star topology would consist of one central node – the 'hub' – with two separate point-to-point links to two peripheral nodes – the 'spokes'. Although most networks that are based upon the physical star topology are commonly implemented using a special device such as a hub or switch as the central node (i.e., the 'hub' of the star), it is also possible to implement a network that is based upon the physical star topology using a computer or even a simple common connection point as the 'hub' or central node. Star networks may also be described as either broadcast multi-access or non broadcast multi-access (NBMA), depending on whether the technology of the network either automatically propagates a signal at the hub to all spokes, or only addresses individual spokes with each communication.

- **Advantages of a Star Topology**
 - Easy to install and wire.
 - No disruptions to the network when connecting or removing devices.
 - Easy to detect faults and to remove parts.
- **Disadvantages of a Star Topology**
 - Requires more cable length than a linear topology.
 - If the hub, switch, or concentrator fails, nodes attached are disabled.
 - More expensive than linear bus topologies because of the cost of the hubs, etc.

extended star

A type of network topology in which a network that is based upon the physical star topology has one or more repeaters between the central node (the 'hub' of the star) and the peripheral or 'spoke' nodes, the repeaters being used to extend the maximum transmission distance of the point-to-point links between the central node and the peripheral nodes beyond that which is supported by the transmitter power of the central node or beyond that which is supported by the standard upon which the physical layer of the physical star network is based. If the repeaters in a network that is based upon the physical extended star topology are replaced with hubs or switches, then a hybrid network topology is created that is referred to as a physical hierarchical star topology, although some texts make no distinction between the two topologies.



- **Advantages of a Star Topology**
 - Point-to-point wiring for individual segments.
 - Supported by several hardware and software vendors.
- **Disadvantages of a Star Topology**
 - Overall length of each segment is limited by the type of cabling used.
 - If the backbone line breaks, the entire segment goes down.
 - More difficult to configure and wire than other topologies.

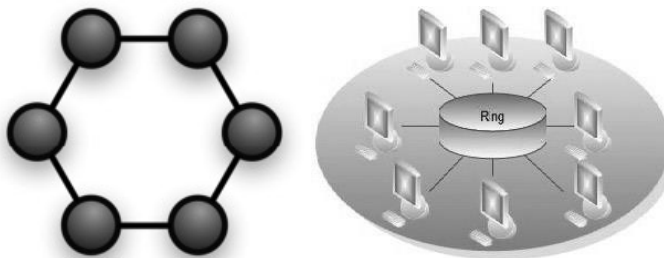
5-4-3 rule

A consideration in setting up a tree topology using Ethernet protocol is the 5-4-3 rule. One aspect of the Ethernet protocol requires that a signal sent out on the network cable reach every part of the network within a specified length of time. Each concentrator or repeater that a signal goes through adds a small amount of time. This leads to the rule that between any two nodes on the network there can only be a maximum of 5 segments, connected through 4 repeaters/concentrators. In addition, only 3 of the segments may be populated (trunk) segments if they are made of coaxial cable. A populated segment is one that has one or more nodes attached to it. This rule does not apply to other network protocols or Ethernet networks where all fiber optic cabling or a combination of a fiber backbone with UTP cabling is used. If there is a combination of fiber optic backbone and UTP cabling, the rule is simply translated to a 7-6-5 rule.

- **Distributed Star**

A type of network topology that is composed of individual networks that are based upon the physical star topology connected together in a linear fashion – i.e., 'daisy-chained' – with no central or top level connection point (e.g., two or more 'stacked' hubs, along with their associated star connected nodes or 'spokes').

3. ring topology:



A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring. The network is dependent on the ability of the signal to travel around the ring.

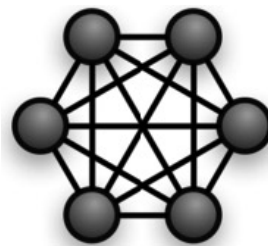
- **Advantages:**

- Very orderly network where every device has access to the token and the opportunity to transmit
- Performs better than a bus topology under heavy network load
- Does not require network server to manage the connectivity between the computers

- **Disadvantages:**
 - One malfunctioning workstation or bad port in the MAU can create problems for the entire network
 - Moves, adds and changes of devices can affect the network
 - Network adapter cards and MAU's are much more expensive than Ethernet cards and hubs
 - Much slower than an Ethernet network under normal load

4. Mesh topology:

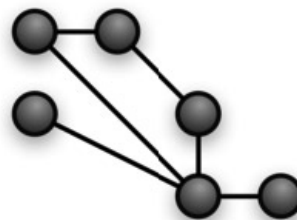
The value of fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.



- **Fully connected**

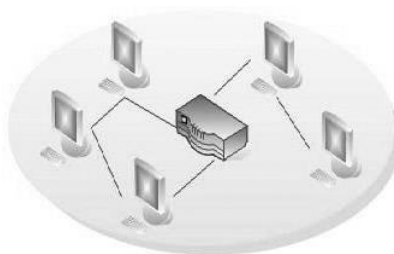
The number of connections in a full mesh = $n(n - 1) / 2$.

Note: The physical fully connected mesh topology is generally too costly and complex for practical networks, although the topology is used when there are only a small number of nodes to be interconnected.



- **partially connected**

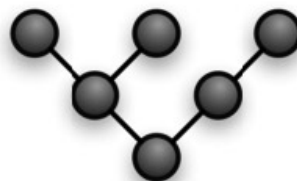
The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.



Note: In most practical networks that are based upon the partially connected mesh topology, all of the data that is transmitted between nodes in the network takes the shortest path between nodes, except in the case of a failure or break in one of the links, in which case the data takes an alternative path to the destination. This requires that the nodes of the network possess some type of logical 'routing' algorithm to determine the correct path to use at any particular time.

5. tree topology:

The type of network topology in which a central 'root' node (the top level of the hierarchy) is connected to one or more other nodes that are one level lower in the hierarchy (i.e., the second level) with a point-to-point link between each of the second level nodes and the top level central 'root' node, while each of the second level nodes that are connected to the top level



central 'root' node will also have one or more other nodes that are one level lower in the hierarchy (i.e., the third level) connected to it, also with a point-to-point link, the top level central 'root' node being the only node that has no other node above it in the hierarchy (The hierarchy of the tree is symmetrical.) Each node in the network having a specific fixed number, of nodes connected to it at the next lower level in the hierarchy, the number, being referred to as the 'branching factor' of the hierarchical tree. This tree has individual peripheral nodes. A network that is based upon the physical hierarchical topology must have at least three levels in the hierarchy of the tree, since a network with a central 'root' node and only one hierarchical level below it would exhibit the physical topology of a star. A network that is based upon the physical hierarchical topology and with a branching factor of 1 would be classified as a physical linear topology. The branching factor, f , is independent of the total number of nodes in the network and, therefore, if the nodes in the network require ports for connection to other nodes the total number of ports per node may be kept low even though the total number of nodes is large – this makes the effect of the cost of adding ports to each node totally dependent upon the branching factor and may therefore be kept as low as required without any effect upon the total number of nodes that are possible. The total number of point-to-point links in a network that is based upon the physical hierarchical topology will be one less than the total number of nodes in the network. If the nodes in a network that is based upon the physical hierarchical topology are required to perform any processing upon the data that is transmitted between nodes in the network, the nodes that are at higher levels in the hierarchy will be required to perform more processing operations on behalf of other nodes than the nodes that are lower in the hierarchy. Such a type of network topology is very useful and highly recommended.

6. hybrid

Hybrid networks use a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.). For example, a tree network connected to a tree network is still a tree network topology. A hybrid topology is always produced when two different basic network topologies are connected. Two common examples for Hybrid network are: *star ring network and star bus network*

- A Star ring network consists of two or more star topologies connected using a multi station access unit (MAU) as a centralized hub.

- A Star Bus network consists of two or more star topologies connected using a bus trunk (the bus trunk serves as the network's backbone).

While grid networks have found popularity in high-performance computing applications, some systems have used genetic algorithms to design custom networks that have the fewest possible hops in between different nodes. Some of the resulting layouts are nearly incomprehensible, although they function quite well. A Snowflake topology is really a "Star of Stars" network, so it exhibits characteristics of a hybrid network topology but is not composed of two different basic network topologies being connected together.

7. Daisy chain

Except for star-based networks, the easiest way to add more computers into a network is by daisy-chaining, or connecting each computer in series to the next. If a message is intended for a computer partway down the line, each system bounces it along in sequence until it reaches the destination. A daisy-chained network can take two basic forms: linear and ring.

- **a linear topology** puts a two-way link between one computer and the next. However, this was expensive in the early days of computing, since each computer (except for the ones at each end) required two receivers and two transmitters.
- By connecting the computers at each end, a **ring topology** can be formed. An advantage of the ring is that the number of transmitters and receivers can be cut in half, since a message will eventually loop all of the way around. When a node sends a message, the message is processed by each computer in the ring. If a computer is not the destination node, it will pass the message to the next node, until the message arrives at its destination. If the message is not accepted by any node on the network, it will travel around the entire ring and return to the sender. This potentially results in a doubling of travel time for data.

Centralization

The **star topology** reduces the probability of a network failure by connecting all of the peripheral nodes (computers, etc.) to a central node. When the physical star topology is applied to a logical bus network such as Ethernet, this central node (traditionally a hub) rebroadcasts all transmissions received from any peripheral node to all peripheral nodes on the network, sometimes including the originating node. All peripheral nodes may thus communicate with all others by transmitting to, and receiving from, the central node only. The failure of a transmission line linking any peripheral node to the central node will result in the isolation of that peripheral node from all others, but the remaining peripheral nodes will be unaffected. However, the disadvantage is that the failure of the central node will cause the failure of all of the peripheral nodes also, if the central node is *passive*, the originating node must be able to tolerate the reception of an echo of its own transmission, delayed by the two-way round trip transmission time (i.e. to and from the central node) plus any delay generated in the central node. An *active* star network has

an active central node that usually has the means to prevent echo-related problems. A tree topology (a.k.a. hierarchical topology) can be viewed as a collection of star networks arranged in a hierarchy. This tree has individual peripheral nodes (e.g. leaves) which are required to transmit to and receive from one other node only and are not required to act as repeaters or regenerators. Unlike the star network, the functionality of the central node may be distributed. As in the conventional star network, individual nodes may thus still be isolated from the network by a single-point failure of a transmission path to the node. If a link connecting a leaf fails, that leaf is isolated; if a connection to a non-leaf node fails, an entire section of the network becomes isolated from the rest. In order to alleviate the amount of network traffic that comes from broadcasting all signals to all nodes, more advanced central nodes were developed that are able to keep track of the identities of the nodes that are connected to the network. These network switches will "learn" the layout of the network by "listening" on each port during normal data transmission, examining the data packets and recording the address/identifier of each connected node and which port it's connected to in a lookup table held in memory. This lookup table then allows future transmissions to be forwarded to the intended destination only.

Decentralization

In a mesh topology (i.e., a partially connected mesh topology), there are at least two nodes with two or more paths between them to provide redundant paths to be used in case the link providing one of the paths fails. This decentralization is often used to advantage to compensate for the single-point-failure disadvantage that is present when using a single device as a central node (e.g., in star and tree networks). A special kind of mesh, limiting the number of hops between two nodes, is a hypercube. The number of arbitrary forks in mesh networks makes them more difficult to design and implement, but their decentralized nature makes them very useful. This is similar in some ways to a **grid network**, where a linear or ring topology is used to connect systems in multiple directions. A multi-dimensional ring has a toroidal topology, for instance. A fully connected network, complete topology or full mesh topology is a network topology in which there is a direct link between all pairs of nodes. In a fully connected network with n nodes, there are $n(n-1)/2$ direct links. Networks designed with this topology are usually very expensive to set up, but provide a high degree of reliability due to the multiple paths for data that are provided by the large number of redundant links between nodes. This topology is mostly seen in military applications.

Considerations When Choosing a topology

- **Money.** A linear bus network may be the least expensive way to install a network; you do not have to purchase concentrators.
- **Length of cable needed.** The linear bus network uses shorter lengths of cable.
- **Future growth.** With a star topology, expanding a network is easily done by adding another concentrator.
- **Cable type.** The most common cable in schools is unshielded twisted pair, which is most often used with star topologies.

Summary Chart:

physical topology	Common Cable	Common protocol
Linear Bus	Twisted Pair Coaxial Fiber	Ethernet
Star	Twisted Pair Fiber	Ethernet
tree	Twisted Pair Coaxial Fiber	Ethernet

Chapter - 15

Networking Devices

Introduction

All but the most basic of networks require devices to provide connectivity and functionality. Understanding how these networking devices operate and identifying the functions they perform are essential skills for any network administrator.

Networking Devices

1. Hub
2. Switch
3. Router
4. Repeater
5. Modem
6. Bridges
7. Brouters
8. Gateways
9. CSU/DSU Unit

Networks using a Star topology require a central point for the devices to connect. Originally this device was called a concentrator since it consolidated the cable runs from all network devices. The basic form of concentrator is the hub.

As shown in Figure; the hub is a hardware device that contains multiple; independent ports that match the cable type of the network. Most common hubs interconnect Category 3 or 5 twisted-pair cable with RJ-45 ends, although Coax BNC and Fiber Optic BNC hubs also exist. The hub is considered the least common denominator in device concentrators. Hubs offer an inexpensive option for transporting data between devices, but hubs don't offer any form of intelligence. Hubs can be active or passive.

ethernet hubs

An Ethernet hub is also called a multiport repeater. A repeater is a device that amplifies a signal as it passes through it, to counteract the effects of attenuation. If, for example, you have a thin Ethernet



8 Port Ethernet Hub

network with a cable segment longer than the prescribed maximum of 185 meters, you can install a repeater at some point in the segment to strengthen the signals and increase the maximum segment length. This type of repeater only has two BNC connectors, and is rarely seen these days.

The hubs used on UTP Ethernet networks are repeaters as well, but they can have many RJ45 ports instead of just two BNC connectors. When data enters the hub through any of its ports, the hub amplifies the signal and transmits it out through all of the other ports. This enables a star network to have a shared medium, even though each computer has its own separate cable. The hub relays every packet transmitted by any computer on the network to all of the other computers, and also amplifies the signals.

The maximum segment length for a UTP cable on an Ethernet network is 100 meters. A segment is defined as the distance between two communicating computers. However, because the hub also functions as a repeater, each of the cables connecting a computer to a hub port can be up to 100 meters long, allowing a segment length of up to 200 meters when one hub is inserted in the network.

I. **passive hub**

II. **active hub**

III. **Switch/ Intelligent hub**

passive hub

It provides no signal regeneration. They are simply cables connected together so that the signal is broken out to other nodes without regeneration. These are not used often today because of loss of cable length that is allowed.

active hub

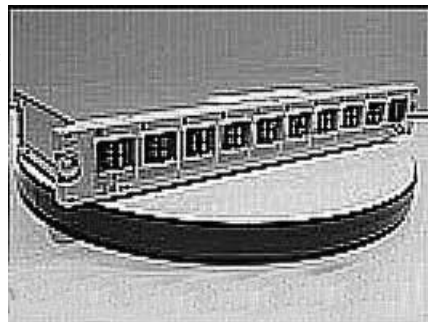
It acts as repeaters and regenerates the data signals to all ports. They have no real intelligence to tell whether the signal needs to go to all ports that is blindly repeated.

Switch hub

Switches are multi ports bridges. They filter traffic between the ports on the switch by using the address of computers transmitting to them. Switches can be used when data performance is needed or when collision need to be reduce.

advantages of hub

- Hubs need almost no configuration.
- Active hub can extend maximum network media distance.
- No processing is done at the hub to slow down performance

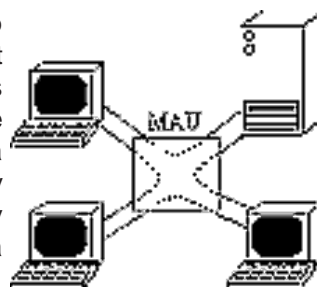


Disadvantages of hub

- Passive hubs can greatly limit maximum media distance.
- Hubs have no intelligence to filter traffic so all data is sent out on all ports whether it is needed or not. Since hubs can act as repeaters the network using them must follow the same rules as repeaters.

Multistation access Unit (MAU)

A Multistation Access Unit (MAU) is a special type of hub used for token ring networks. The word “hub” is used most often in relation to Ethernet networks, and MAU only refers to token ring networks. On the outside, the MAU looks like a hub. It connects to multiple network devices, each with a separate cable. Unlike a hub that uses a logical bus topology over a physical star; the MAU uses a logical ring topology over a physical star. When the MAU detects a problem with a connection, the ring will beacon. Because it uses a physical star topology, the MAU can easily detect which port the problem exists on and close the port, or “wrap” it. The MAU does actively regenerate signals as it transmits data around the ring.



Switches

Switches are a special type of hub that offers an additional layer of intelligence to basic, physical-layer repeater hubs. A switch must be able to read the MAC address of each frame it receives. This information allows switches to repeat incoming data frames only to the computer or computers to which a frame is addressed. This speeds up the network and reduces congestion.



Switches operate at both the physical layer and the data link layer of the OSI Model.

Bridges

A bridge is used to join two network segments together; it allows computers on either segment to access resources on the other. They can also be used to divide large networks into smaller segments. Bridges have all the features of repeaters, but can have more nodes, and since the network is divided, there is fewer computers competing for resources on each segment thus improving network performance. Bridges are used to connect similar network segments.

A bridge does not pass or signals it receives. When a bridge receives a signal, it determines its destination by looking at its destination and it sends the signals towards it. For example in an above figure a bridge has been used to join two network segments A AND B.



When the bridge receives the signals it read address of both sender and receiver. If the sender is a computer in segment A and the receiver is also segment A, it would not pass the signals to the segments B. It will however pass signals if the sender is in one segment and the receiver in other segment. Bridge works at the data link layer of O.S.I model.

advantages of Bridges

- Bridge extends network segments by connecting them together to make one logical network.
- They can affect the segment traffic between networks by filtering data if it does not need to pass.
- Like repeaters they can connect similar network types with different cabling.

Disadvantages of Bridges

- Bridge possess information about the data they receive with can slow performance.

routers

Routers are devices which connect two or more networks that use similar protocol. A router consists of hard ware and software. Hard ware can be a computer is specific device. Software consists of special management program that controls flow of data between networks. Routers operate at a network layer of O.S.I model.



Routers use logical and physical address to connect two or more logically separate network. They make this connection by organizing the large network into logical network segment (some times small sub network or sub nets). Each of these sub nets is given a logical address. Data is grouped into packets or block of data.



Each packet in addition to having a physical device address has a logical address. The network address allows routers to calculate more accurately and efficiently the path of the computer.

advantages of router

- They use high level of intelligence to route data
- Routers can also act as a bridge to handle non rout able protocols such as NetBEUI (Network Bios Extended User Interface)

Disadvantages of router:

- High level of intelligence take more processing time which can effect performance
- Routers are very complicated which installation and maintenance difficult.

repeater

Repeaters are used within network to extend the length of communication. Data process through transmission media in the farm of waves or signals. The transmission media weaken signals that move through it. The weakening of signal is called attenuation. If the data is to be transmitted beyond the maximum length of a communication media, signals have amplified. The devices that are used to amplify the signals are called repeaters. Repeaters work at the physical layer of OSI model.Repeaters is normally two ports boxes that connect two segments. As a signal comes in one port, it is regenerated and sends out to the other port. The signal is read as 1s and 0s. As 1s and 0s are transmitted, the noise can be cleaned out.

advantages of repeater

- Repeaters easily extend the length of network.
- They require no processing over head, so very little if any performance degradation occurs.
- It can connect signals from the same network type that use different types of cables.

Disadvantages of repeaters

- Repeaters cannot be used to connect segments of different network types.
- They cannot be used to segment traffic on a network to reduce congestion.
- Many types of network have a limit on the number of network s that can be used at once.

MODEM

The device that converts digital signals into analog signals and analog signals to digital signals is called Modem. The word modem stands for modulation and demodulation. The process of converting digital signals to analog signals is called modulation. The process of converting analog signals to digital signals is called demodulation. Modems are used with computers to transfer data from one computer to another computer through telephone lines. Modems have two connections these are.

- Analog connection
- Digital connection

analog connection.

The connection between the modem and the telephone line is called analog connection.

Types of Modem- THERE ARE TWO TYPES OF MODEMS

- **Internal modem**
- **External modem**

Digital connection.

The connection of modem to computer is called digital connection

INterNaL MODeM

It fits into expansion slots inside the computer. It is directly linked to the telephone lines through the telephone jack. It is normally less inexpensive than external modem. Its transmission speed is also less external modem.

eXterNaL MODeM

It is the external unit of computer and is connected to the computer through serial port. It is also linked to the telephone line through a telephone jack. External modems are expensive and have more operation features and high transmission speed.

Advantages of Modem

- I. Inexpensive hardware and telephone lines.
- II. Easy to setup and maintain.

Disadvantages of Modem

- I. Very slow performance.

Routers

Routers are a combination of router and bridge. This is a special type of equipment used for networks that can be either bridged or routed, based on the protocols being forwarded. Routers are complex, fairly expensive pieces of equipment and as such are rarely used. A Routers transmits two types of traffic at the exact same time:

bridged traffic and routed traffic. For bridged traffic, the Routers handles the traffic the same way a bridge or switch would, forwarding data based on the physical address of the packet. This makes the bridged traffic fairly fast, but slower than if it were sent directly through a bridge because the Routers has to determine whether the data packet should be bridged or routed.



Gateways

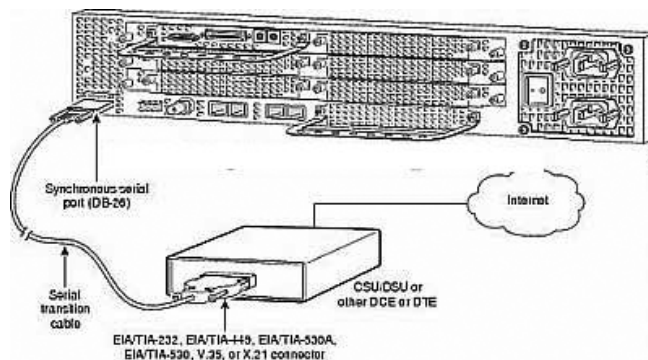
A gateway is a device used to connect networks using different protocols. Gateways operate at the network layer of the OSI model. In order to communicate with a host on another network, an IP host must be configured with a route to the destination network. If a configuration route is not found, the host uses the gateway (default IP router) to transmit the traffic to the destination host. The default gateway is where the IP sends packets that are destined for remote networks. If no default gateway is specified, communication is limited to the local network. Gateways receive data from a network using one type of protocol stack, remove that protocol stack and repackage it with the protocol stack that the other network can use.

Examples

- E-mail gateways-for example, a gateway that receives Simple Mail Transfer Protocol (SMTP) e-mail, translates it into a standard X.400 format, and forwards it to its destination
- Gateway Service for NetWare (GSNW), which enables a machine running Microsoft Windows NT Server or Windows Server to be a gateway for Windows clients so that they can access file and print resources on a NetWare server
- Gateways between a Systems Network Architecture (SNA) host and computers on a TCP/IP network, such as the one provided by Microsoft SNA Server
- A packet assembler/disassemble (PAD) that provides connectivity between a local area network (LAN) and an X.25 packet-switching network

CSU / DSU (Channel Service Unit / Data Service Unit)

A CSU/DSU is a device that combines the functionality of a channel service unit (CSU) and a data service unit (DSU). These devices are used to connect a LAN to a WAN, and they take care of all the translation required to convert a data stream between these two methods of communication.



A DSU provides all the handshaking and error correction required to maintain a connection across a wide area link, similar to a modem. The DSU will accept a serial data stream from a device on the LAN and translate this into a useable data stream for the digital WAN network. It will also take care of converting any inbound data streams from the WAN back

to a serial communication. A CSU is similar to a DSU except it does not have the ability to provide handshaking or error correction. It is strictly an interface between the LAN and the WAN and relies on some other device to provide handshaking and error correction.

NICs (Network Interface Card)

Network Interface Card or NIC is a hardware card installed in a computer so it can communicate on a network. The network adapter provides one or more ports for the network cable to connect to, and it transmits and receives data onto the network cable.



Wireless LaN card

every networked computer must also have a network adapter driver, which controls the network adapter. Each network adapter driver is configured to run with a certain type of network adapter.

Network card

Network Interface adapter Functions

Network interface adapters perform a variety of functions that are crucial to getting data to and from the computer over the network.



these functions are as follows:

Data encapsulation

The network interface adapter and its driver are responsible for building the frame around the data generated by the network layer protocol, in preparation for transmission. The network interface adapter also reads the contents of incoming frames and passes the data to the appropriate network layer protocol.

Signal encoding and decoding

The network interface adapter implements the physical layer encoding scheme that converts the binary data generated by the network layer-now encapsulated in the frame-into electrical voltages, light pulses, or whatever other signal type the network medium uses, and converts received signals to binary data for use by the network layer.

Transmission and reception

The primary function of the network interface adapter is to generate and transmit signals of the appropriate type over the network and to receive incoming signals. The nature of the signals depends on the network medium and the data-link layer protocol. On a typical LAN, every computer receives all of the packets transmitted over the network, and the network interface adapter examines the destination address in each packet, to see if it is intended for that computer. If so, the network interface adapter passes the packet to the computer for processing by the next layer in the protocol stack; if not, the network interface adapter discards the packet.

Data buffering

Network interface adapters transmit and receive data one frame at a time, so they have built-in buffers that enable them to store data arriving either from the computer or from the network until a frame is complete and ready for processing.

Serial/parallel conversion

The communication between the computer and the network interface adapter runs in parallel, that is, either 16 or 32 bits at a time, depending on the bus the adapter uses. Network communications, however, are serial (running one bit at a time), so the network interface adapter is responsible for performing the conversion between the two types of transmissions.

Media access control

The network interface adapter also implements the MAC mechanism that the data-link layer protocol uses to regulate access to the network medium. The nature of the MAC mechanism depends on the protocol used.

Table 3.4 Network Devices Summary

Device	Function/Purpose	Key Points
Hub	Connects devices on a twisted-pair network.	A hub does not perform any tasks besides signal regeneration.
Switch	Connects devices on a twisted-pair network.	A switch forwards data to its destination by using the MAC address embedded in each packet.
Bridge	Divides networks to reduce overall network traffic.	A bridge allows or prevents data from passing through it by reading the MAC address.
Router	Connects networks together.	A router uses the software-configured network address to make forwarding decisions.
Gateway	Translates from one data format to another.	Gateways can be hardware or software based. Any device that translates data formats is called a gateway.
CSU/DSU	Translates digital signals used on a LAN to those used on a WAN.	CSU/DSU functionality is sometimes incorporated into other devices, such as a router with a WAN connection.

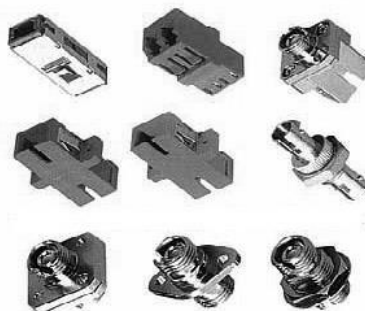
Network card	Enables systems to connect to the network.	Network interfaces can be add-in expansion cards, PCMCIA cards, or built-in interfaces.
ISDN terminal adapter	Connects devices to ISDN lines.	ISDN is a digital WAN technology often used in place of slower modem links. ISDN terminal adapters are required to reformat the data format for transmission on ISDN links.
WAP	Provides network capabilities to wireless network devices.	A WAP is often used to connect to a wired network, thereby acting as a link between wired and wireless portions of the network.

Table 3.4 Network Devices Summary (continued)

Device	Function/Purpose	Key Points
Modem	Provides serial communication capabilities across phone lines.	Modems modulate the digital signal into analog at the sending end and perform the reverse function at the receiving end.
Transceiver	Converts one media type to another, such as UTP to fiber.	A device that functions as a transmitter and a receiver of signals such as analog or digital.
Firewall	Provides controlled data access between networks.	Firewalls can be hardware or software based and are an essential part of a networks security strategy.

Transceivers (media converters)

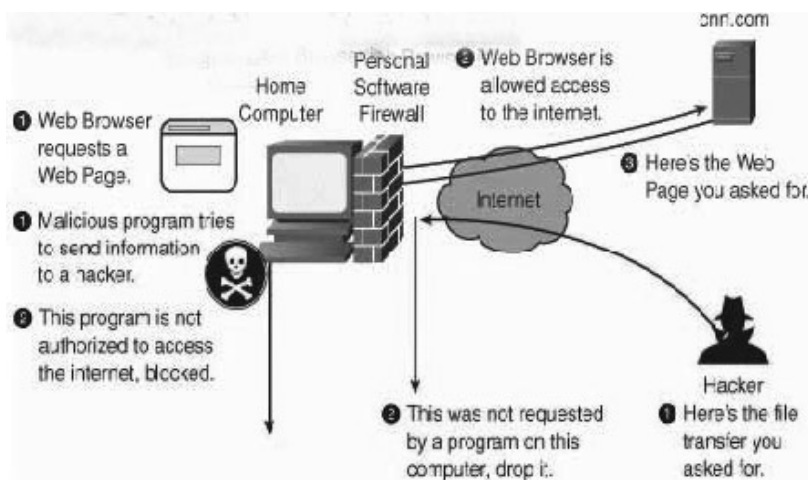
Transceiver short for transmitter-receiver, a device that both transmits and receives analog or digital signals. The term is used most frequently to describe the component in local-area networks (LANs) that actually applies signals onto the network wire and detects signals passing through the wire. For many LANs, the transceiver is built into the network interface card (NIC). Some types of networks, however, require an external transceiver.



In Ethernet networks, a transceiver is also called a Medium Access Unit (MAU). Media converters interconnect different cable types twisted pair, fiber, and Thin or thick coax, within an existing network. They are often used to connect newer 100-Mbps, Gigabit Ethernet, or ATM equipment to existing networks, which are generally 10BASE-T, 100BASE-T, or a mixture of both. They can also be used in pairs to insert a fiber segment into copper networks to increase cabling distances and enhance immunity to electromagnetic interference (EMI).

Firewalls

In computing, a firewall is a piece of hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy, analogous to the function of firewalls in building construction.



A firewall has the basic task of controlling traffic between different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with high trust). The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.

There are three basic types of firewalls depending on:

- whether the communication is being done between a single node and the network, or between two or more networks
- whether the communication is intercepted at the network layer, or at the application layer
- whether the communication state is being tracked at the firewall or not

With regard to the scope of filtered communication these firewalls are exist:

- Personal firewalls, a software application which normally filters traffic entering or leaving a single computer through the Internet.

- Network firewalls, normally running on a dedicated network device or computer positioned on the boundary of two or more networks or DMZs (demilitarized zones). Such a firewall filters all traffic entering or leaving the connected networks.

In reference to the layers where the traffic can be intercepted, three main categories of firewalls exist:

- Network layer firewalls An example would be iptables.
- Application layer firewalls An example would be TCP Wrapper.
- application firewalls An example would be restricting ftp services through /etc/ftpaccess file

These network-layer and application-layer types of firewall may overlap, even though the personal firewall does not serve a network; indeed, single systems have implemented both together.

There's also the notion of application firewalls which are sometimes used during wide area network (WAN) networking on the world-wide web and govern the system software. An extended description would place them lower than application layer firewalls, indeed at the Operating System layer, and could alternately be called operating system firewalls.

Lastly, depending on whether the firewalls track packet states, two additional categories of firewalls exist:

- Stateful firewalls
- Stateless firewalls

Network layer firewalls

Network layer firewalls operate at a (relatively low) level of the TCP/IP protocol stack as IP-packet filters, not allowing packets to pass through the firewall unless they match the rules. The firewall administrator may define the rules; or default built-in rules may apply (as in some inflexible firewall systems).

A more permissive setup could allow any packet to pass the filter as long as it does not match one or more "negative-rules", or "deny rules". Today network firewalls are built into most computer operating system and network appliances.

Modern firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or port, destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, domain name of the source, and many other attributes.

application-layer firewalls

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgement to the sender). In principle, application firewalls can prevent all unwanted outside traffic from reaching protected machines.

By inspecting all packets for improper content, firewalls can even prevent the spread of the likes of viruses. In practice, however, this becomes so complex and so difficult to attempt (given the variety of applications and the diversity of content each may allow in its packet traffic) that comprehensive firewall design does not generally attempt this approach.

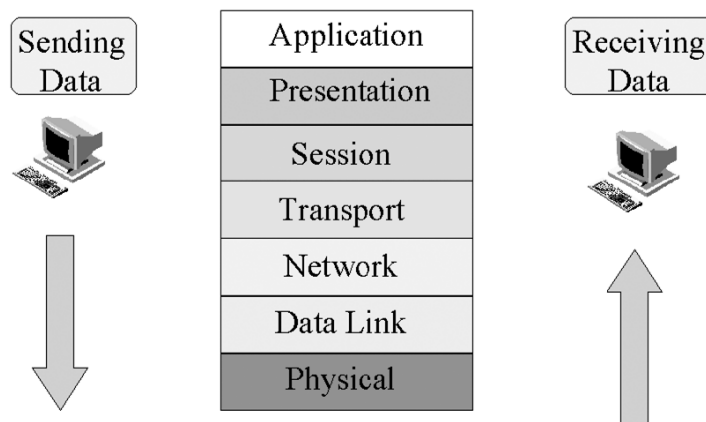
Chapter - 16

OSI reference Model

Introduction

As the concept of network models grew, the need for one universal model was apparent. In the late 1970s, an international standards organization, the International Organization for Standardization (ISO), commissioned a committee to establish such a model. The Open Systems Interconnection (OSI) Reference Model was created. It has become the most widely accepted network model. The OSI model contains seven layers.

Introduction to the OSI Model



The OSI model was developed in 1977 and contains seven layers. Each layer is responsible for performing certain tasks. The OSI model is a pattern; it performs no specific functions. Each of the following layers will be covered in detail.

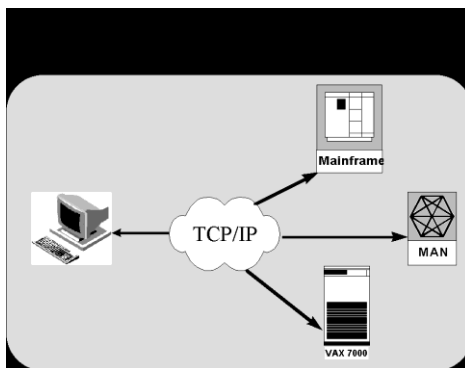
- Physical
- Data Link
- Network
- Transport
- Session
- Presentation
- Application

The first layer is the physical layer, even though workstation processing starts with the application layer. Data from the application layer are passed to the presentation layer. The presentation layer data are passed to the session layer, and so on.

Consider using the following mnemonics for learning the OSI model. Please Do Not Throw Sausage Pizza Away. The reverse mnemonic is All People Seem to Need Data Processing.

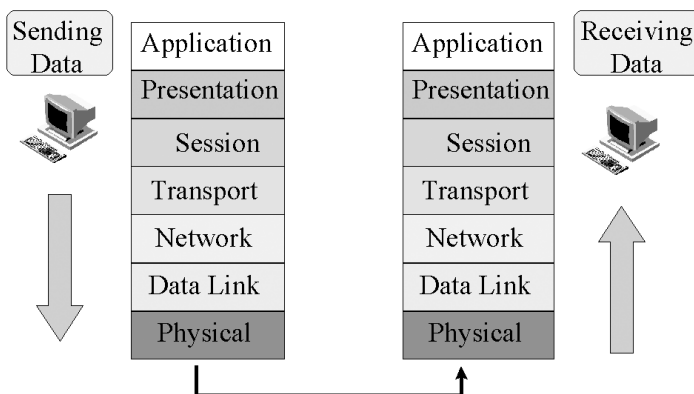
What Is a Network Implementation?

As previously discussed, protocols are established to enable interoperability of devices produced by different manufacturers. The specific uses of a protocol(s) are called the protocol or network implementation. Products may look and operate differently but, if the protocol is implemented correctly, the devices will function the same. An example of a network implementation is TCP/IP. These protocols can run on systems ranging from Apple MACs to IBM mainframe computers and enable users on small personal computers to log in and access resources on supercomputers. The implementation of network protocols has led to widespread interoperability between computers and networks from different manufacturers. The responsibility of a network administrator is to understand the functions and procedures of the protocols and to implement these protocols on an organization's systems.



Data passing through the OSI Model

Data Passing Through the OSI Model

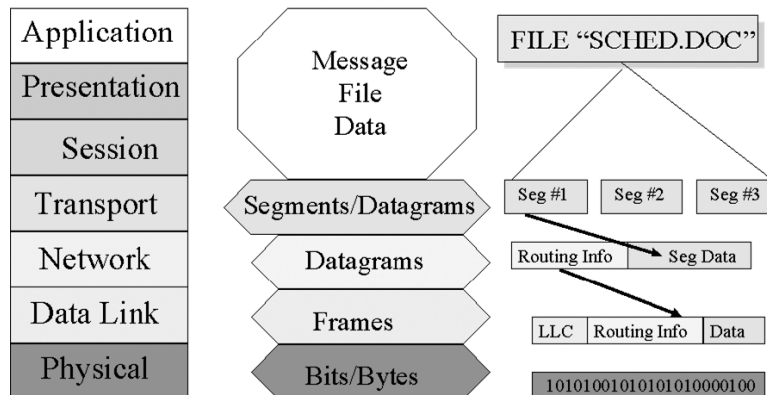


Workstation processing starts with the application layer. Data from the application layer are passed to the presentation layer. The presentation layer data are passed to the session layer, and so on. Each layer adds a header to the front of the data. The header contains information pertaining to that layer. When data are transmitted, the last layer it goes

through is the OSI layer. At the receiving station, the first layer to receive the information is the physical layer. This data layer strips off the physical layer header information and passes the rest of data to the data link layer. The data link layer strips off the data link layer header and passes the rest of the data to the network layer. The process continues all the way up to the application layer.

Data Layer Units

Data Layer Units

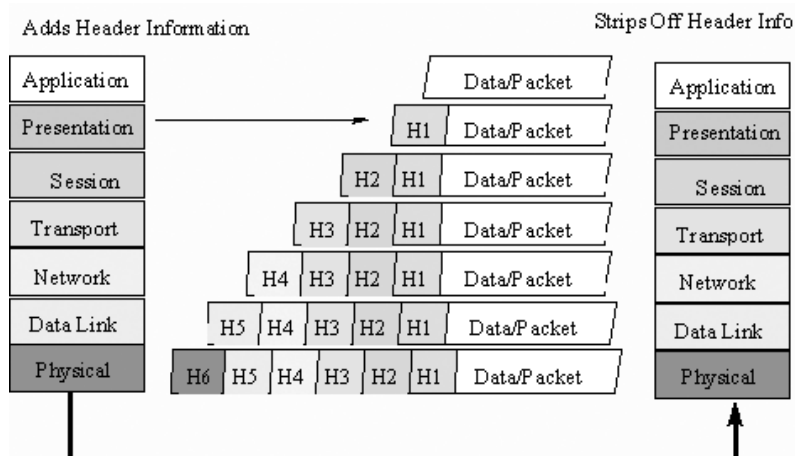


As data are passed up and down through the different layers of the OSI model, data will be referred to in different terms based on the OSI layer where the data are located.

1. **physical Layer** - at the physical layer, the data units are called **bits or bytes**. A bit stands for binary digit. The binary number system consists of 1's and 0's or "ON/OFF," or "TRUE/FALSE." When data are transmitted along the wire and into the network card, they are represented by bits. Bits are the smallest unit of information. A byte is a group of eight bits.
2. **Data Link** - at the data link layer, bits and bytes are organized into units with specific information called **data frames**. A frame is a block of bits. Frames can be different sizes, depending on the protocols used.
3. **Network Layers** - at the network layer, routing information is added to the frame. This data unit is then referred to as a **datagram**.
4. **transport Layer** - Data at the transport layer consist of files that are divided into smaller layers called segments.
5. **application, presentation, Session Layer** - Data from the session to the application layer are called a message, file, or data. Remember, each layer adds its own header to the data. Data passed from one layer to another are called a service data unit. Thus, data passed from layer 3 (the network layer) to layer 2 (the data link layer) are called a data link layer service data unit.

The term, packet, can describe data at any layer of the OSI model.

Data header Information



Data Control Information

As data are passed up and down through the different layers of the OSI model, control information is added to the data. This control information is added at each layer and enables the data to be interpreted by the corresponding layer on the receiving station. This information can also be used between adjacent layers. The information added at each layer is organized into fields or headers before the data information.

As the packet is passed down the OSI model, it becomes long and stores more control information. As the data are received by each layer at the receiving station, the headers are stripped off the packet until the data remains.

easy Way to Understand OSI Model

aLL peOpLe SeeM tO NeED Data prOCeSSING			
LaYer	What the LaYer IS reSpONSIBLE FOR/ SerVICeS eTC.	COrrEspONDING DeVICeS	COrrEspONDING prOtOCOLS
7. application	<ol style="list-style-type: none"> Interface between the user & the computer (applications & Gateways). Provides services that directly support user applications, such as the USER INterFace, e-Mail, FILE traNSFer, terMINAL eMULatION, DataBase aCCeSS, etc. API incorporated in this layer Allows applications to use the network. Handles Network access, flow control & error recovery. Messages are sent between layers. 	Gateways (can work at all layers)	<ul style="list-style-type: none"> • SNMP • FTP • TELNET • WWW • HTTP • SMB • NCP • TCP • TFTP • NFS • SMTP

aLL peOpLe SeeM tO NeED Data prOCeSSING			
LaYer	What the LaYer IS reSpONSIBLe FOrr/ SerVICes etc.	COrrerSpONding DeVICes	COrrerSpONding prOtOCOLs
6. presentation	<ol style="list-style-type: none"> 1. Translation of data into understandable format for transmission (into a form usable by the application layer i.e. translates data between the formats the network requires and the computer expects). 2. Handles character encoding, bit order and byte order issues. Encodes and decodes data. 3. Data compression and encryption takes place at this layer. 4. Generally determines the structure of data 5. The redirector works at this layer. 6. Responsible for protocol conversion 7. Messages are sent between layers 8. Communicates through GATEWAYS and APPLICATION INTERFACES 9. SERVICES: Telnet, FTP use TCP, TFTP, NFS, SNMP, SMTP use TCP 	Gateways	<ul style="list-style-type: none"> • JPEG • MIDI • MPEG • All kinds of music, pictures & movie formats • NCP

aLL peOpLe SeeM tO NeED Data prOCeSSING			
LaYer	What the LaYer IS reSpONSIBLE FOR/ SerVICeS etC.	COrrESpONDIg DeVICeS	COrrESpONDIg prOtOCOLs
5. Session	<ol style="list-style-type: none"> 1. Responsible for opening, using and closing session. That is. It allows applications or connecting systems to establish a session (Establishes and maintains a connection). 2. Provides synchronization between communicating computers (nodes), messages are sent between layers (i.e. Manages upper layer errors). 3. Also places checkpoints in the data flow, so that if transmission fails, only the data after the last checkpoint needs to be retransmitted. 4. Handles remote procedure calls. 5. Communicates through Gateways & application interfaces. 6. SERVICES: Telnet, FTP use TCP, TFTP, NFS, SNMP, SMTP use TCP 	Gateways	<ul style="list-style-type: none"> • Network File System (NFS) • SQL • RPC

aLL peOpLe SeeM tO NeEd Data prOCeSSING			
LaYer	What the LaYer IS reSpONSIBLE FOrr/ SerVICes etc.	COrrEspONDING DeVICes	COrrEspONDING prOtOCOLS
4. transport	<ol style="list-style-type: none"> 1. Responsible for PACK-ET HANDLING. Ensures error free delivery. Repackages messages, divides messages into smaller packets (Fragments and reassembles data), and handles error handling 2. Ensures proper sequencing and without loss and duplication. 3. Takes action to correct faulty transmissions 4. Controls flow of data 5. Acknowledges successful receipt of data 6. Sliding window is at this Layer -segments of message fragments are sent between layers 7. TCP/SPX - connection oriented communication for applications to ensure error free delivery. 8. UDP - connectionless communications and does not guarantee packet delivery between transfer points 9. Communicates through Gateway Services, routers & brouters. 	Gateways	<ul style="list-style-type: none"> • TCP • UDP • SPX • NetBEUI

aLL peOpLe SeeM tO NeEd Data prOCeSSING			
LaYer	What the LaYer IS reSpONSIBLE FOrr/ SerVICeS eTc.	COrrEspONDING DeVICeS	COrrEspONDING prOtOCOLs
3. Network	<ol style="list-style-type: none"> 1. Logical addressing - software addresses to hardware addresses are resolved (ARP, RARP). 2. Routing of message (Packets) between hosts & networks (IP, IPX). 3. Determining the best route (Makes routing decisions & forwards packets (a.k.a. DATA-GRAMS) for devices that could be farther away than a single link. 4. Moves information to the correct address. 5. Sends messages and reports errors regarding packet delivery (ICMP) 6. Reports host group membership to local multicast routers (IGMP) 7. Communicates through GATEWAY SERVICES, ROUTERS & BROUTERS 	<ul style="list-style-type: none"> • Routers • Brouters 	<ul style="list-style-type: none"> • IP • IPX • RIP • ICMP • ARP • RARP • OSPF • EGP • IGMP • NetBEUI • DLC • DecNET

aLL peOpLe SeeM tO NeEd Data prOCeSSING			
LaYer	What the LaYer IS reSPONSIBLe FOrr/ SerVICeS etC.	COrrerSpONDIING DeVICeS	COrrerSpONDIING prOtOCOLs
2. Data Link	<ol style="list-style-type: none"> 1. Provides for flow of data over a single link from one device to another 2. Controls access to communication channel 3. Controls flow of data 4. Packets placed into frames at this layer (i.e. Organizes data into logical frames - logical units of information). 5. Identifies the specific computer on the network 6. CRC is added at this Layer (Error detection). 7. If CRC fails at the receiving computer, this layer will request retransmission. 8. MAC addresses are resolved at this Layer (switches, Routers and bridges function on this layer using the MAC sub layer) 9. Sends data from network layer to physical layer. 10. Manages physical layer communications between connecting systems. 11. Data frames are sent between layers. 	<ul style="list-style-type: none"> • Brouters • Bridges • Switches 	<ul style="list-style-type: none"> • HDLC (High-Level Data Link Control) - Supports asynchronous & synchronous transmissions. • Uses LLC flow control. • SLIP • PPP

aLL peOpLe SeeM tO NeED Data prOCeSSING			
LaYer	What the LaYer IS reSpONSIBLE FOrr/ SerVICes etC.	COrrerSpONDING DeVICes	COrrerSpONDING prOtOCOLS
	<p>12. Ethernet, Token Ring & other communications occur here via frames. LLC -(802.2) manages link control & defines SAP'S (Service Access Points). MAC- (802.3, 802.4, 802.5, and 802.12) communicates with adapter card.</p> <p>13. Communicates through SWITCHES, BRIDGES & INTELLIGENT HUBS</p> <p>NOTE: the Data Link Layer contains two SUB-LaYers</p> <p>LLC (Logical Link Control) - The upper sub-layer, which establishes and maintains links between communicating devices. Also responsible for frame error correction and hardware addresses</p> <p>MAC (Media Access Control) - The lower sub-layer, which controls how devices share a media channel. Either through CONTENTION or TOKEN PASSING</p>		

aLL peOpLe SeeM tO NeED Data prOCeSSING			
LaYer	What the LaYer IS reSpONSIBLe FOrr/ SerVICeS etC.	COrrerSpONding DeVICeS	COrrerSpONding prOtOCOLs
1. physical	<ol style="list-style-type: none"> 1. Data (BITS) is sent across physical media like wires and hubs. 2. Responsible for encoding scheme (like Manchester encoding) 3. Defines cables, cards and physical aspects. 4. Provides electrical and mechanical interfaces for a network. 5. Specifies how signals are transmitted on network 6. Communicates through REPEATERS, HUBS, SWITCHES, CABLES, CONNECTORS, TRANSMITTERS, RECEIVERS, MULTIPLEXERS 	<ul style="list-style-type: none"> • Hubs • Repeaters • Amplifiers • Transceivers • Multiplexers • Receivers • Transmitters • Connectors • Cables • Switches 	None

Chapter - 17

Network protocols

Introduction

The word protocol is derived from the Greek word “protocollon” which means a leaf of paper glued to manuscript volume. In computer protocols means a set of rules, a communication language or set of standards between two or more computing devices. Protocols exist at the several levels of the OSI (open system interconnectivity) layers model. In the telecommunication system, there are one more protocols at each layer of the telephone exchange. On the internet, there is a suite of the protocols known as TCP/IP protocols that are consisting of transmission control protocol, internet protocol, file transfer protocol, dynamic host configuration protocol, Border gateway protocol and a number of other protocols. In the telecommunication, a protocol is set of rules for data representation, authentication, and error detection. The communication protocols in the computer networking are intended for the secure, fast and error free data delivery between two communication devices. Communication protocols follow certain rules for the transmission of the data.

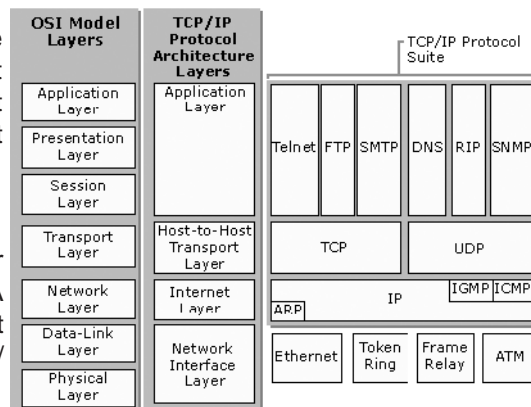
protocols properties:

Different protocols perform different functions so it is difficult to generalize the properties of the protocols. There are some basic properties of most of the protocols. • Detection of the physical (wired or wireless connection) • Handshaking • How to format a message. • How to send and receive a message. • Negotiation of the various connections • Correction of the corrupted or improperly formatted messages. • Termination of the session.

The widespread use of the communication protocols is a prerequisite to the internet. The term TCP/IP refers to the protocols suite and a pair of the TCP and IP protocols are the most important internet communication protocols. Most protocols in communication are layered together where the various tasks listed above are divided. Protocols stacks refer to the combination of the different protocols. The OSI reference model is the conceptual model that is used to represent the protocols stacks. There are different network protocols that perform different functions.

tCp/Ip protocol architecture

TCP/IP protocols map to a four-layer conceptual model known as the DARPA model, named after the U.S. government agency that initially developed TCP/IP. The four layers of the DARPA model are: Application, Transport, Internet, and



tCp/Ip protocol architecture

Network Interface. Each layer in the DARPA model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) model. Figure shows the TCP/IP protocol architecture.

Network Interface Layer

The *Network Interface layer* (also called the Network Access layer) is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. In this way, TCP/IP can be used to connect differing network types. These include LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM). The Network Interface layer encompasses the Data Link and Physical layers of the OSI model. Note that the Internet layer does not take advantage of sequencing and acknowledgment services that might be present in the Data-Link layer. An unreliable Network Interface layer is assumed, and reliable communications through session establishment and the sequencing and acknowledgment of packets is the responsibility of the Transport layer.

Internet Layer:

The Internet layer is responsible for addressing, packaging, and routing functions. The core protocols of the Internet layer are IP, ARP, ICMP, and IGMP.

- The **Internet protocol (Ip)** is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets.
- The Address Resolution Protocol (ARP) is responsible for the resolution of the Internet layer address to the Network Interface layer address such as a hardware address.
- The **Internet Control Message protocol (ICMp)** is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.
- The **Internet Group Management protocol (IGMp)** is responsible for the management of IP multicast groups.

The Internet layer is analogous to the Network layer of the OSI model.

transport Layer:

The *Transport layer* (also known as the Host-to-Host Transport layer) is responsible for providing the Application layer with session and datagram communication services. The core protocols of the Transport layer are *Transmission Control Protocol* (TCP) and the *User Datagram Protocol* (UDP).

- TCP provides a one-to-one, connection-oriented, reliable communications service. TCP is responsible for the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.

- UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when the overhead of establishing a TCP connection is not desired or when the applications or upper layer protocols provide reliable delivery.

The Transport layer encompasses the responsibilities of the OSI Transport layer and some of the responsibilities of the OSI Session layer.

application Layer:

The *Application layer* provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data. There are many Application layer protocols and new protocols are always being developed.

The most widely-known Application layer protocols are those used for the exchange of user information:

- The Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the Web pages of the World Wide Web.
- The File Transfer Protocol (FTP) is used for interactive file transfer.
- The Simple Mail Transfer Protocol (SMTP) is used for the transfer of mail messages and attachments.
- Telnet, a terminal emulation protocol, is used for logging on remotely to network hosts.

Additionally, the following Application layer protocols help facilitate the use and management of TCP/IP networks:

- The Domain Name System (DNS) is used to resolve a host name to an IP address.
- The Routing Information Protocol (RIP) is a routing protocol that routers use to exchange routing information on an IP internetwork.
- The Simple Network Management Protocol (SNMP) is used between a network management console and network devices (routers, bridges, intelligent hubs) to collect and exchange network management information.

Examples of Application layer interfaces for TCP/IP applications are Windows Sockets and NetBIOS. Windows Sockets provides a standard application programming interface (API) under Windows 2000. NetBIOS is an industry standard interface for accessing protocol services such as sessions, datagrams, and name resolution.

Following is the description of the some of the most commonly used protocols:

http (hyper text transfer protocol)

Hypertext transfer protocol is a method of transmitting the information on the web. HTTP basically publishes and retrieves the HTTP pages on the World Wide Web. HTTP is a language that is used to communicate between the browser and web server. The information that is transferred using HTTP can be plain text, audio, video, images, and hypertext. HTTP is a request/response protocol between the client and server. Many proxies, tunnels, and gateways can be existing between the web browser (client) and server (web server). An HTTP client initializes a request by establishing a TCP connection to a particular port on the remote host (typically 80 or 8080). An HTTP server listens to that port and receives a request message from the client. Upon receiving the request, server sends back 200 OK messages, its own message, an error message or other message.

pOp3 (post Office protocol)

In computing, e-mail clients such as (MS outlook, outlook express and thunderbird) use Post office Protocol to retrieve emails from the remote server over the TCP/IP connection. Nearly all the users of the Internet service providers use POP 3 in the email clients to retrieve the emails from the email servers. Most email applications use POP protocol.

SMtp (Simple Mail transfer protocol)

Simple Mail Transfer Protocol is a protocol that is used to send the email messages between the servers. Most email systems and email clients use the SMTP protocol to send messages to one server to another. In configuring an email application, you need to configure POP, SMTP and IMAP protocols in your email software. SMTP is a simple, text based protocol and one or more recipient of the message is specified and then the message is transferred. SMTP connection is easily tested by the Telnet utility. SMTP uses the by default TCP port number 25

Ftp (File transfer protocol)

FTP or file transfer protocol is used to transfer (upload/download) data from one computer to another over the internet or through or computer network. FTP is a most commonly communication protocol for transferring the files over the internet. Typically, there are two computers are involved in the transferring the files a server and a client. The client computer that is running FTP client software such as Cuteftp and AceFTP etc initiates a connection with the remote computer (server). After successfully connected with the server, the client computer can perform a number of the operations like downloading the files, uploading, renaming and deleting the files, creating the new folders etc. Virtually operating system supports FTP protocols.

Ip (Internet protocol)

An Internet protocol (IP) is a unique address or identifier of each computer or communication devices on the network and internet. Any participating computer networking device such as routers, computers, printers, internet fax machines and switches may have their own unique IP address. Personal information about someone can be found by the IP address.

Every domain on the internet must have a unique or shared IP address.

DhCp (Dynamic host Configuration protocol)

The DHCP or Dynamic Host Configuration Protocol is a set of rules used by a communication device such as router, computer or network adapter to allow the device to request and obtain an IP address from a server which has a list of the larger number of addresses. DHCP is a protocol that is used by the network computers to obtain the IP addresses and other settings such as gateway, DNS, subnet mask from the DHCP server. DHCP ensures that all the IP addresses are unique and the IP address management is done by the server and not by the human. The assignment of the IP addresses expires after the predetermined period of time. DHCP works in four phases known as DORA such as Discover, Offer, Request and Acknowledge.

IMap (Internet Message access protocol)

The Internet Message Access Protocol known as IMAP is an application layer protocol that is used to access the emails on the remote servers. POP3 and IMAP are the two most commonly used email retrieval protocols. Most of the email clients such as outlook express, thunderbird and MS outlooks support POP3 and IMAP. The email messages are generally stored on the email server and the users generally retrieve these messages whether by the web browser or email clients. IMAP is generally used in the large networks. IMAP allows users to access their messages instantly on their systems.

arCNet

ARCNET is a local area network technology that uses token bus scheme for managing line sharing among the workstations. When a device on a network wants to send a message, it inserts a token that is set to 1 and when a destination device reads the message it resets the token to 0 so that the frame can be used by another device.

FDDI

Fiber distributed data interface (FDDI) provides a standard for data transmission in a local area network that can extend a range of 200 kilometers. The FDDI uses token ring protocol as its basis. FDDI local area network can support a large number of users and can cover a large geographical area. FDDI uses fiber optic as a standard communication medium. FDDI uses dual attached token ring topology. A FDDI network contains two token rings and the primary ring offers the capacity of 100 Mbits/s. FDDI is an ANSI standard network and it can support 500 stations in 2 kilometers.

UDp

The user datagram protocol is a most important protocol of the TCP/IP suite and is used to send the short messages known as datagram. Common network applications that use UDP are DNS, online games, IPTV, TFTP and VOIP. UDP is very fast and light weight. UDP is an unreliable connectionless protocol that operates on the transport layer and it is sometimes called Universal Datagram Protocol.

X.25

X.25 is a standard protocol suite for wide area networks using a phone line or ISDN system. The X.25 standard was approved by CCITT now ITU in 1976.

tFtp

Trivial File Transfer Protocol (TFTP) is a very simple file transfer protocol with the very basic features of the FTP. TFTP can be implemented in a very small amount of memory. TFTP is useful for booting computers such as routers. TFTP is also used to transfer the files over the network. TFTP uses UDP and provides no security features.

SNMP

The simple network management protocol (SNMP) forms the TCP/IP suite. SNMP is used to manage the network attached devices of the complex network.

pptp

The point to point tunneling protocol is used in the virtual private networks. PPP works by sending regular PPP session. PPTP is a method of implementing VPN networks.

ethernet

The Ethernet protocol is by far the most widely used. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant. When this happens a collision occurs. Each computer then backs off and waits a random amount of time before attempting to retransmit. With this access method, it is normal to have collisions. However, the delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network. The Ethernet protocol allows for linear bus, star, or tree topologies. Data can be transmitted over twisted pair, coaxial, or fiber optic cable at a speed of 10 Mbps.

Fast ethernet

To allow for an increased speed of transmission, the Ethernet protocol has developed a new standard that supports 100 Mbps. This is commonly called Fast Ethernet. Fast Ethernet requires the use of different, more expensive network concentrators/hubs and network interface cards. In addition, category 5 twisted pair or fiber optic cable is necessary.

LocalTalk

LocalTalk is a network protocol that was developed by Apple Computer, Inc. for Macintosh computers. The method used by LocalTalk is called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). It is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. LocalTalk adapters and special twisted pair cable can be used to connect a series of computers through the serial port. The

Macintosh operating system allows the establishment of a peer-to-peer network without the need for additional software. With the addition of the server version of AppleShare software, a client/server network can be established. The Local Talk protocol allows for linear bus, star, or tree topologies using twisted pair cable. A primary disadvantage of LocalTalk is speed. Its speed of transmission is only 230 Kbps.

token ring

The Token Ring protocol was developed by IBM in the mid-1980s. The access method used involves token-passing. In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next. If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the data is captured by the receiving computer. The Token Ring protocol requires a star-wired ring using twisted pair or fiber optic cable. It can operate at transmission speeds of 4 Mbps or 16 Mbps. Due to the increasing popularity of Ethernet, the use of Token Ring in school environments has decreased.

FDDI

Fiber Distributed Data Interface (FDDI) is a network protocol that is used primarily to interconnect two or more local area networks, often over large distances. The access method used by FDDI involves token-passing. FDDI uses a dual ring physical topology. Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new complete ring. A major advantage of FDDI is speed. It operates over fiber optic cable at 100 Mbps.

protocol Summary

protocol	Cable	Speed	topology
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps	Linear Bus, Star, Tree
Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star
LocalTalk	Twisted Pair	.23 Mbps	Linear Bus or Star
Token Ring	Twisted Pair	4 Mbps - 16 Mbps	Star-Wired Ring
FDDI	Fiber	100 Mbps	Dual ring

Other protocols

VTP, ARP, IPX, OSPF, RARP, NFS, BOOTP, NNTP, IRC, RADIUS, Soap, Telnet, RIP, SSH.

Chapter – 18

troubleshooting LaN Network

troubleshoot basic connectivity issues

To troubleshoot basic connectivity issues and verify name resolution between computers, follow these steps in the order in which they are provided until you isolate and resolve the issue.

Step 1: Verify the physical connection between computers

The back of each network adapter in a desktop computer has visible lights. These lights indicate a good connection. If you are using a network hub, or a switch to connect the computers, make sure that the network hub or the switch is turned on and that the lights are illuminated for each client connection. This indicates a good link.

Step 2: Make sure that all computers have TCP/IP installed

This step is especially important with Microsoft Windows 95-based computers. By default, Windows 95-based computers do not have TCP/IP installed. If you are using computers that run Windows 95, Microsoft Windows 98, or Microsoft Windows Millennium Edition on the network, you can look for TCP/IP by using the Network item in Control Panel. If TCP/IP is not installed, you must install it to communicate with Windows XP-based computers on the network. TCP/IP is always installed in Windows XP.

Step 3: Make sure that the network configuration includes the IP addresses

Collect network configuration information from at least two computers on the network by using the adapter status. Then, make sure that the assigned IP addresses match the home-network configurations described in the “Home-network structures and their configurations” section. Follow these steps:

1. Click **Start**, click **run**, type **ncpa.cpl** and then click **OK**.
2. Locate and right-click the icon that represents this computer’s connection to the home network, and then click **Status**.
3. Click the **Support tab**, and then under Connection status, locate the IP addresses.

If the assigned IP addresses do not match the topology that this article described in the “Home-network structures and their configurations” section, the computer that is assigning the addresses may not be available. This is likely to be true if 169.254.x.y addresses are in a configuration where you expect a different address range.

To change the configuration so that the addresses on the home network adapter for each computer are in the same range, determine which address is correct based on the network topology. To do this, check whether one computer receives an address in the range 192.168.0.x, and another receives an address in the range 169.254.x.y. When you isolate which computer has the incorrect address, troubleshoot the computer that has the incorrect address.

Note:- For Windows 95-based computers in a network that uses 169.254.x.y addressing, you must configure IP addresses manually. For information about how to do this, see the online Help for Windows 95.

Step 4: Make sure that firewall features are not enabled on the home network adapters

Verify that the Internet Connection Firewall (ICF) or Windows Firewall (WF) feature is not enabled on the adapters that you use to connect the computers to the home network. If these features are enabled on these adapters, you cannot connect to share resources on other computers in the network. Note:-Edgeless networks are the exception. You can use ICF with edgeless networks if you take additional measures to enable connectivity in the home network.

Step 5: test connectivity between computers by using the “ping” command

To use the ping command to test connectivity between two computers on the network, on one of the computers, click Start, click Run, type command and then click OK. At the command prompt, type ping x.x.x.x (where x.x.x.x is the IP address of the other computer), and then press ENTER. If the ping command is successful, and the computers can connect correctly After you have verified connectivity and name resolution between computers, you can troubleshoot the connectivity for file and printer sharing.

Tracert traceroute Ping Arp Netstat Nbtstat NetBIOS Ipconfig winipcfg nslookup

tracert / traceroute

tracert: Determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination with incrementally increasing Time to Live (TTL) field values. The path displayed is the list of near-side router interfaces of the routers in the path between a source host and a destination. The near-side interface is the interface of the router that is closest to the sending host in the path. Used without parameters, tracert displays help.

This diagnostic tool determines the path taken to a destination by sending ICMP Echo Request messages with varying Time to Live (TTL) values to the destination. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it.

Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP Time Exceeded message to the source computer. Tracert determines the path by sending the first Echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 30 by default and can be specified using the -h parameter.

The path is determined by examining the ICMP Time Exceeded messages returned by intermediate routers and the Echo Reply message returned by the destination. However, some routers do not return Time Exceeded messages for packets with expired TTL values

and are invisible to the `tracert` command. In this case, a row of asterisks (*) is displayed for that hop.

examples:

To trace the path to the host named `www.google.co.in` type: **tracert www.google.co.in**

To trace the path to the host named `www.google.com` and prevent the resolution of each IP address to

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Fithraw>tracert www.google.co.in
Tracing route to www.l.google.com [216.239.61.104]
over a maximum of 30 hops:
  0  1  1 ms    1 ms    1 ms    192.168.1.1
  1  49 ns   43 ms   47 ms   1.subnet125-164-192.speedy.telkon.net.id [125.164.192.11]
  2  90 ns   89 ms   59 ms   125.160.1.17
  3  244 ns  243 ms  249 ms  203.208.191.161
  4  248 ns  249 ms  *      ge-0-1-7-0.sngtp-dx2.ix.singtel.com [203.208.151.181]
  5  415 ns  397 ms  381 ms  74.125.50.225
  6  382 ns  387 ms  385 ms  209.85.243.156
  7  378 ns  385 ms  387 ms  209.85.254.179
  8  378 ns  381 ms  379 ms  sn-in-f104.google.com [216.239.61.104]
Trace complete.
C:\Documents and Settings\Fithraw>
```

Its name, type:

tracert -d www.google.com

To trace the path to the host named `www.google.com` and use the loose source route `10.12.0.1-10.29.3.1-10.1.44.1`, type:

tracert -j 10.12.0.1 10.29.3.1 10.1.44.1 www.google.com

Syntax

```
tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] [TargetName]
```

Parameters

-d Prevents `tracert` from attempting to resolve the IP addresses of intermediate routers to their names. This can speed up the display of `tracert` results.

-h MaximumHops Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.

-j HostList Specifies that Echo Request messages use the Loose Source Route option in the IP header with the set of intermediate destinations specified in `HostList`. With loose source routing, successive intermediate destinations can be separated by one or multiple routers. The maximum number of addresses or names in the host list is 9. The `HostList` is a series of IP addresses (in dotted decimal notation) separated by spaces.

-w Timeout Specifies the amount of time in milliseconds to wait for the ICMP Time Exceeded or Echo Reply message corresponding to a given Echo Request message to be received. If not received within the time-out, an asterisk (*) is displayed. The default time-out is 4000 (4 seconds).

ping

Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.

```

C:\K:\WINNT\system32\cmd.exe
G:\>
G:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

G:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

G:\>

```

You can use ping to test both the computer name and the IP address of the computer. If pinging the IP address is successful, but pinging the computer name is not, you might have a name resolution problem. In this case, ensure that the computer name you are specifying can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.

To test a TCP/IP configuration by using the ping command:

1. To quickly obtain the TCP/IP configuration of a computer, open Command Prompt, and then type **ipconfig**. From the display of the ipconfig command, ensure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.
2. At the command prompt, ping the loopback address by typing **ping 127.0.0.1**
3. Ping the IP address of the computer.
4. Ping the IP address of the default gateway. If the ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.
5. Ping the IP address of a remote host (a host that is on a different subnet). If the ping command fails, verify that the remote host IP address is correct, that the remote host

is operational, and that all of the gateways (routers) between this computer and the remote host are operational.

6. Ping the IP address of the DNS server. If the ping command fails, verify that the DNS server IP address is correct, that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

arp - address resolution protocol

Displays and modifies entries in the Address Resolution Protocol (ARP) cache, which contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses. There is a separate table for each Ethernet or Token Ring network adapter installed on your computer.

Syntax

```
arp [-a [InetAddr] [-N lfaceAddr]] [-g [InetAddr] [-N lfaceAddr]] [-d InetAddr [lfaceAddr]]
[-s InetAddr EtherAddr [lfaceAddr]]
```

Parameters

Used without parameters, ping displays help

-a [InetAddr] [-N lfaceAddr] *Displays current ARP cache tables for all interfaces. To display the ARP cache entry for a specific IP address, use arp -a with the InetAddr parameter, where InetAddr is an IP address. To display the ARP cache table for a specific interface, use the -N lfaceAddr parameter where lfaceAddr is the IP address assigned to the interface. The -N parameter is case-sensitive.*

-g [InetAddr] [-N lfaceAddr] *Identical to -a.*

-d InetAddr [lfaceAddr] *Deletes an entry with a specific IP address, where InetAddr is the IP address. To delete an entry in a table for a specific interface, use the lfaceAddr parameter where lfaceAddr is the IP address assigned to the interface. To delete all entries, use the asterisk (*) wildcard character in place of InetAddr.*

-s InetAddr EtherAddr [lfaceAddr] *Adds a static entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr. To add a static ARP cache entry to the table for a specific interface, use the lfaceAddr parameter where lfaceAddr is an IP address assigned to the interface.*

examples:

To display the ARP cache tables for all interfaces, type:

arp -a

To display the ARP cache table for the interface that is assigned the IP address 10.0.0.99, type:

```

C:\WINDOWS\system32\cmd.exe
Z:\>arp -a

Interface: 10.253.15.72 --- 0x4
Internet Address      Physical Address      Type
10.253.1.2           00-12-3f-ed-3f-2c    dynamic
10.253.1.6           00-13-72-51-d5-a9    dynamic
10.253.1.13          00-03-ff-5b-f1-c8    dynamic
10.253.1.18          00-03-ff-36-9b-48    dynamic
10.253.1.25          00-11-43-de-91-15    dynamic
10.253.1.26          00-11-43-e7-97-fc    dynamic
10.253.1.35          00-14-22-17-c8-91    dynamic
10.253.100.1         00-15-2b-46-50-00    dynamic
10.253.100.2         00-09-0f-83-3b-8a    dynamic

Z:\>

```

arp -a -N 10.0.0.99

To add a static ARP cache entry that resolves the IP address 10.0.0.80 to the physical address 00-AA-00-4F-2A-9C, type:

arp -s 10.0.0.80 00-aa-00-4F-2a-9C

```

C:\WINNT\System32\cmd.exe
C:\>ARP -s

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

-a          Displays current ARP entries by interrogating the current
           protocol data. If inet_addr is specified, the IP and Physical
           addresses for only the specified computer are displayed. If
           more than one network interface uses ARP, entries for each ARP
           table are displayed.
-g          Same as -a.
inet_addr  Specifies an internet address.
-N if_addr Displays the ARP entries for the network interface specified
           by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
           wildcarded with * to delete all hosts.
-s          Adds the host and associates the internet address inet_addr
           with the Physical address eth_addr. The Physical address is
           given as 6 hexadecimal bytes separated by hyphens. The entry
           is permanent.
eth_addr   Specifies a physical address.
if_addr    If present, this specifies the internet address of the
           interface whose address translation table should be modified.
           If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a .... Displays the arp table.

C:\>

```

Netstat

Displays active TCP connections, ports on which the computer is listening, Ethernet

statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols).

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\yongmo.FSMY>netstat -nb

Active Connections

Proto Local Address          Foreign Address        State                 PID
TCP   10.70.1.71:1306        10.70.0.10:1910       ESTABLISHED          2580
[Communicator.exe]
TCP   10.70.1.71:1308        10.70.0.10:1910       ESTABLISHED          2580
[Communicator.exe]
TCP   10.70.1.71:1319        10.70.0.10:1910       ESTABLISHED          2580
[Communicator.exe]
TCP   10.70.1.71:1334        10.70.0.10:1910       ESTABLISHED          2580
[Communicator.exe]
TCP   10.70.1.71:1581        10.70.0.10:1910       ESTABLISHED          2800
[OUTLOOK.EXE]
TCP   10.70.1.71:1854        10.70.0.10:1910       ESTABLISHED          2580
[Communicator.exe]
TCP   10.70.1.71:2109        10.70.0.10:1910       ESTABLISHED          2580
[Communicator.exe]

```

Netstat provides statistics for the following:

- Proto - The name of the protocol (TCP or UDP).
- Local Address - The IP address of the local computer and the port number being used. The name of the local computer that corresponds to the IP address and the name of the port is shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).
- Foreign Address - The IP address and port number of the remote computer to which the socket is connected. The names that corresponds to the IP address and the port are shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).

(state) Indicates the state of a TCP connection. the possible states are as follows:

- CLOSE_WAIT
- CLOSED
- ESTABLISHED
- FIN_WAIT_1
- FIN_WAIT_2
- LAST_ACK
- LISTEN

- SYN_RECEIVED
- SYN_SEND
- TIMED_WAIT

Syntax

netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]

Parameters

Used without parameters, netstat displays active TCP connections.

-a *Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.*

-e *Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.*

-n *Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.*

-o *Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.*

-p *Shows connections for the protocol specified by Protocol. In this case, the Protocol can be tcp, udp, tcpv6, or udpv6. If this parameter is used with -s to display statistics by protocol, Protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.*

-s *Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The -p parameter can be used to specify a set of protocols.*

-r *Displays the contents of the IP routing table. This is equivalent to the route print command.*

Interval *Redisplays the selected information every Interval seconds. Press CTRL+C to stop the redisplay. If this parameter is omitted, netstat prints the selected information only once.*

/? - Displays help at the command prompt.

Nbtstat

Displays NetBIOS over TCP/IP (NetBT) protocol statistics,

```

C:\WINNT\System32\cmd.exe
C:\>nbtstat -A 192.168.1.105
Local Area Connection:
Node IpAddress: [192.168.1.107] Scope Id: []

        NetBIOS Remote Machine Name Table

    Name                Type             Status
-----                -
WIN2K2                 <00>            UNIQUE          Registered
WIN2K2                 <20>            UNIQUE          Registered
WORKGROUP              <00>            GROUP           Registered
WIN2K2                 <03>            UNIQUE          Registered
WORKGROUP              <1E>            GROUP           Registered
WORKGROUP              <1D>            UNIQUE          Registered
_._MS_BROWSE_._        <01>            GROUP           Registered
ADMINISTRATOR         <03>            UNIQUE          Registered

    MAC Address = 00-0C-29-02-CB-45

C:\>

```

NetBIOS

NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. Nbtstat allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS).

Nbtstat command-line parameters are case-sensitive.

Syntax

```
nbtstat [-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]
```

Parameters

Used without parameters, nbtstat displays help.

-a RemoteName Displays the NetBIOS name table of a remote computer, where RemoteName is the NetBIOS computer name of the remote computer. The NetBIOS name table is the list of NetBIOS names that corresponds to NetBIOS applications running on that computer.

-A IPAddress Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer.

-c Displays the contents of the NetBIOS name cache, the table of NetBIOS names and their resolved IP addresses.

-n Displays the NetBIOS name table of the local computer. The status of Registered indicates that the name is registered either by broadcast or with a WINS server.

-r Displays NetBIOS name resolution statistics. On a Windows XP computer that is configured to use WINS, this parameter returns the number of names that have been resolved and registered using broadcast and WINS.

-R Purges the contents of the NetBIOS name cache and then reloads the #PRE-tagged entries from the Lmhosts file.

-RR Releases and then refreshes NetBIOS names for the local computer that is registered with WINS servers.

-s Displays NetBIOS client and server sessions, attempting to convert the destination IP address to a name.

-S Displays NetBIOS client and server sessions, listing the remote computers by destination IP address only.

***Interval** Redisplays selected statistics, pausing the number of seconds specified in Interval between each display. Press CTRL+C to stop redisplaying statistics. If this parameter is omitted, nbtstat prints the current configuration information only once.*

/? - Displays help at the command prompt.

Ipconfig

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. This command is most useful on computers that are configured to obtain an IP address automatically. This enables users to determine which TCP/IP configuration values have been configured by DHCP, Automatic Private IP Addressing (APIPA), or an alternate configuration.

- If the Adapter name contains any spaces, use quotation marks around the adapter name (that is, "Adapter Name").
- For adapter names, ipconfig supports the use of the asterisk (*) wildcard character to specify either adapters with names that begin with a specified string or adapters with names that contain a specified string.
- For example, **Local*** matches all adapters that start with the string Local and ***Con*** matches all adapters that contain the string Con.

Syntax

`ipconfig [/all] [/renew [Adapter]] [/release [Adapter]] [/flushdns] [/displaydns]`

Parameters

Used without parameters, `ipconfig` displays the IP address, subnet mask, and default gateway for all adapters.

/all Displays the full TCP/IP configuration for all adapters. Without this parameter, `ipconfig` displays only the IP address, subnet mask, and default gateway values for each adapter. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.

/renew [Adapter] Renews DHCP configuration for all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use `ipconfig` without parameters.

/release [Adapter] Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP address configuration for either all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included. This parameter disables TCP/IP for adapters configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use `ipconfig` without parameters.

/flushdns Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.

/displaydns Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.

examples:

To display the basic TCP/IP configuration for all adapters, type:

- `ipconfig`

To display the full TCP/IP configuration for all adapters, type:

- `ipconfig /all`

To renew a DHCP-assigned IP address configuration for only the Local Area Connection adapter, type:

- `ipconfig /renew "Local Area Connection"`

To flush the DNS resolver cache when troubleshooting DNS name resolution problems, type:

- `ipconfig /flushdns`

To display the DHCP class ID for all adapters with names that start with Local, type:

- `ipconfig /showclassid Local`

To set the DHCP class ID for the Local Area Connection adapter to TEST, type:

- `ipconfig /setclassid "Local Area Connection" TEST`

winipcfg

This utility allows users or administrators to see the current IP address and other useful information about your network configuration. You can reset one or more IP addresses. The Release or Renew buttons allow you to release or renew one IP address. If you want to release or renew all IP addresses click Release All or Renew All. When one of these buttons is clicked, a new IP address is obtained from either the DHCP service or from the computer assigning itself an automatic private IP address. **to use the winipcfg utility:**

1. Click Start, and then click Run and type winipcfg
2. Click More Info.
3. To see the addresses of the DNS servers the computer is configured to use, click the ellipsis (...) button to the right of DNS Servers.
4. To see address information for your network adapter(s), select an adapter from the list in Ethernet Adapter Information.

nslookup

Nslookup (Name Server lookup) is a UNIX shell command to query Internet domain name servers.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\TARUN KUMAR>nslookup
Default Server:  triband-del-59.179.243.70.bo1.net.in
Address:  59.179.243.70

> set type=mx
Server:  triband-del-59.179.243.70.bo1.net.in
Address:  59.179.243.70

Non-authoritative answer:
gmail.com      MX preference = 10, mail exchanger = alt1.gmail-smtp-in.1.google
               MX preference = 10, mail exchanger = alt2.gmail-smtp-in.1.google
gmail.com      MX preference = 50, mail exchanger = gsmtp147.google.com
gmail.com      MX preference = 50, mail exchanger = gsmtp183.google.com
gmail.com      MX preference = 5, mail exchanger = gmail-smtp-in.1.google.com

gmail.com      nameserver = ns4.google.com
gmail.com      nameserver = ns1.google.com
gmail.com      nameserver = ns2.google.com
gmail.com      nameserver = ns3.google.com
gmail-smtp-in.1.google.com internet address = 209.85.143.27
gmail-smtp-in.1.google.com internet address = 209.85.143.114
alt1.gmail-smtp-in.1.google.com internet address = 209.85.133.114
alt1.gmail-smtp-in.1.google.com internet address = 209.85.133.27
alt2.gmail-smtp-in.1.google.com internet address = 209.85.133.27
alt2.gmail-smtp-in.1.google.com internet address = 209.85.135.114
gsmtp147.google.com internet address = 209.85.147.27
gsmtp183.google.com internet address = 64.233.183.27
ns1.google.com internet address = 216.239.32.10
ns2.google.com internet address = 216.239.34.10
ns3.google.com internet address = 216.239.36.10
ns4.google.com internet address = 216.239.38.10

```

Definitions

- **Nameserver:** These are the servers that the internet uses to find out more about the domain. Usually they are an ISP's computer.
- **Mailserver:** Where email is sent to.
- **Webserver:** The domains website.
- **Ftpserver:** FTP is file transfer protocol, this server is where files may be stored.
- **hostname:** The name of the host as given by the domain.
- **real hostname:** This is hostname that you get by reverse resolving the IP address, may be different to the given hostname.
- **Ip address:** Unique four numbered identifier that is obtained by resolving the hostname.

troubleshooting peer to peer Workgroup Network

1. error Message:

Windows XP takes a long time to open a shared disk or folder on a computer running Windows 95, 98, or Me

Description: This is a different problem than My Network Places taking a long time to open. This problem occurs after you double click a shared disk or folder.

possible Solutions:

Disable searching for scheduled tasks by deleting this registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Explorer\ RemoteComputer\NameSpace\ {D6277990-4C6A-11CF-8D87-00AA0060F5BF}

2. error Message:

Network Connection Has IP Address 169.254.x.x

Description: The network card is configured to obtain an IP address automatically, and it's connected to a network with a DHCP server: hardware router, another computer running Internet Connection Sharing, cable modem, DSL modem, etc. But it gets a 169.254.x.x IP address, which indicates that it can't communicate with the DHCP server:

possible Solutions:

- Connect the computer using a different Ethernet cable or hub/switch/router port.
- Download and install the latest firmware for the hardware router.
- Disable XP's Internet Connection Firewall on the local area network connection.
- The card is configured to automatically sense network speed and duplex mode, but auto-sensing is failing. Configure the speed and duplex mode manually. For example, most switches and routers use 100 Mb speed and full duplex. To make the settings, right click the network connection and click Properties | Configure | Advanced.
- Un-install the network card and move it to a different slot.
- If you have a cable modem connection, turn off the computer, turn off the cable modem, and wait a few minutes. Turn on the cable modem, and then turn on the computer

3. error Message:

Renewing a DHCP lease fails, with error message "An error occurred while renewing interface <name> the system cannot find the file specified."

Description: Network connection configured to obtain an IP address automatically has IP address 0.0.0.0

possible Solutions:

Make sure that the DHCP Client service is running:

1. Right click My Computer, and click Manage.
2. Double click Services and Applications.
3. Double click Services.
4. Double click DHCP Client. If the Service status is stopped, click Start.
5. Set the Startup type to Automatic.

4. error Message:

Computers can ping each other by IP address, but not by name.

Description: An attempt to ping a computer by name gets the message Ping request could not find host >computer name<. Please check the name and try again.

possible Solutions:

Make sure that NetBIOS Over TCP/IP is enabled.

5. error Message:

Network Cable Unplugged

Description: Don't take this message literally - there are many causes besides not having a cable physically plugged into the network card. The message really means that the network card doesn't detect a live link to another device on the other end of the cable.

possible Solutions:

1. Download and install the latest network card driver program.
2. Check the cabling - a bad cable will prevent link detection. Substitute a cable that's known to be good.
3. Check the link lights on the device on the other end of the cable, whether it's a hub, switch, router, or a NIC in another computer. It should show a live link to the NIC. If it doesn't, try a different port.
4. Auto-detecting speed and duplex mode can be unreliable. Set them manually. Most routers and switches use 100Mb, full duplex. Hubs can only use half duplex

6. error Message:

The list of servers for this workgroup is not currently available

possible Solutions:

Make sure that the Computer Browser service is running on at least one Windows XP computer on the network: * Right click My Computer, and click Manage. * Double click Services and Applications. * Double click Services. * Double click Computer Browser. If the Service status is Stopped, click Start. * Set the Startup type to Automatic.

7. error Message:

Unable to browse the network. The network is not accessible.

Description: This error message appears on a computer running Windows 95/98/Me.

possible Solutions:

Make sure that: * The user is logged on. Click Start | Log Off >user name< and log back on. * The Computer Browser service is running on at least one Windows XP computer on the network.

8. error Message:

Computer A Can Ping Computer B, but not Vice Versa.

possible Solutions:

This is almost always caused by an improperly configured firewall on Computer A.

9. error Message:

XP's Network Setup Wizard Says That No Network Card Is Installed

possible Solutions:

XP's Network Setup Wizard sometimes fails to recognize an installed and working network card. This is because the NIC's driver program doesn't respond correctly to all of the queries that the Wizard makes when it's looking for a NIC. Configure the card's TCP/IP properties manually.

10. error Message:

One Computer Can't Access Some Web Sites, but Other Computers Can

possible Solutions:

Look for the Windows Hosts file on the problem computer: * Windows 95/98/Me: C:\Windows\Hosts * Windows 2000: C:\WinNT\System32\Drivers\Etc\Hosts * Windows XP: C:\Windows\System32\Drivers\Etc\Hosts Open it with a text editor and you'll probably find lines with the names of the sites that you can't access. Delete those lines, save the file, and try again. If those are the only lines in the file, delete the file. Be sure to save it with a file name of just Hosts, with no file type. If your editor saves it as Hosts.txt, rename it to just Hosts. The Hosts file can be created by "web accelerator" programs that store name-to-IP address translations. This might speed up access by a tiny amount, but it causes problems when a site's IP address changes.

11. error Message:

PING: transmit failed, error code 65

Description: This error message occurs when you try to ping any IP address.

possible Solutions:

A firewall program has been incompletely removed. Re-install it, then remove it.

12. error Message:

A shared disk or folder doesn't appear in My Network Places

Description: The disk or folder is shared correctly on another computer, but it doesn't appear.

possible Solutions:

* Click adds a network place and follows the prompts to add it. Browse to it through Entire Network, or specify the path name using the form \\computer\share. * Click View workgroup computers, and then click the computer that has the shared disk or folder.

13. error Message:

I have enable NetBIOS over TCP/IP but ipconfig /all shows NetBIOS over TCP/IP disable

Description: For some reasons, you have enabled NetBIOS over TCP/IP on W2K/XP but using ipconfig /all still shows NetBIOS over TCP/IP disable.

possible Solutions:

The alternative solution will be installing NetBEUI to all computers.

14. error Message:

I can't see a computer even I can ping **computername**

Description: Sometimes, you may be able to ping or net view \\computer, but can't see it in My Network Places.

possible Solutions:

If this is a case, you may want to check the workgroup or domain, make sure they are in the same group or domain. Also check the computer browser issue. In the most cases, you may be able to use the computer resources if it enables file and printer sharing and logon the same logon.

15. error Message:

Loading NetBEUI works but not NetBIOS over TCP/IP

possible Solutions:

In general, computer browser performance improves with fewer protocols or network cards on a computer. This is one of reasons why NetBEUI is not loaded WinXP by default. If loading NetBEUI make the workgroup to see each but not enabling NetBIOS over TCP/IP, this is not name resolution issue. This is because of some reasons such as a firewall running.

16. error Message:

Logon ID works on win9x but not W2K/XP

Description: You can logon all workstations with different OS such as win9x, w2k and xp. If logon win9x, you can access any network resources; but if you logon w2k/xp, you will get access denied fro accessing any network resources.

possible Solutions:

Have your administrator to re-set your password.

17. error Message:

One computer cannot access the Internet

Description: You have a network with a router connecting to the Internet. All computers except one can't access the Internet. That computer can ping most other computers' IPs except the router's LAN IP.

possible Solutions:

Check the router settings and make sure MAC Address Control doesn't deny that computer.

18. error Message:

* Unable to browse the network". The network is not present or not stated when click MS Windows

Network under Entire Network.

* The service has not been started" when using net view or net send.

* You may not be able to logon.

possible Solutions:

Problems with workstation service you may need to check workstation service and make sure it is running on the computer.

Control panel → administrative tools → services → workstation (This service should start)

19. error Message:

* You may receive "System error 53 has occurred. The network path was not found" when using net view \\computername from a remote computer.

* The service has not been started when using net share.

* You may receive "\\computername is not accessible. Then network path was not found" when trying to browse the computer from My Network Places.

* You may receive "System error 51 has occurred. The remote computer is not available" when using net use to map the computer drive.

possible Solutions:

Problems with server service you may need to check server service and make sure it is running on the computer.

Control panel → administrative tools → services → server (This service should start)

20. error Message:

Win9x can't see Win2000/XP

Description: By default, Win2000/XP disables NetBIOS over TCP/IP (NetBul) for selected clients. In a peer-to-peer network without WINS, Win9x will be unable to browse, locate, or create file and print share connections to a Windows 2000 computer with NetBIOS disabled.

possible Solutions:

You must setup the Win2000/XP to uses NetBIOS over TCP/IP to communicate with prior versions of Windows NT and other clients, such as Microsoft Windows 95. Alternatively, you may want to add NetBEUI on all workstations in the peer-to-peer network.

21. error Message:

Zone Alarm may disable file sharing

Description: You setup a peer-to-peer network correctly but no one can see one of the networking computers and the computer can't see others. Later you find that Installing ZA prevents file sharing because Zone Alarm will consider all other machines on the network as entrusted and will not allow them to communicate with the machine ZA is installed on.

possible Solutions:

Disabling Zone Alarm.

To fix this, in the firewall section "ZONE" tab use the ADD button to specify which Ip's or range of ip's are local, it would also be a good idea to specify which NIC is local on a multi-homed machine. To do that,

Go to Security >> Advance button and select the "local zone contents" tab then click Add and specify which ip or range of ip are local also specify local interface on multi-homed machine.

To troubleshoot a home network issue, use the Windows XP Home and Small Office Networking Troubleshooter in Help and Support Center to try to isolate and resolve the issue. To do this, follow these steps:

- Click **Start**, and then click **help and Support**.
- Under Pick a Help Topic, click **Networking and the Web**.
- Under Networking and the Web, click **Fixing networking or Web problems**, and then click **Home and Small Office Networking Troubleshooter**.
- Answer the questions in the troubleshooter to try to find a solution. If the troubleshooter resolves the issue, you are finished.

If the troubleshooter does not resolve the issue, then go through the process given below

home-network structures and their configurations

Before you troubleshoot home networking issues, first determine the network structure you are using. The network structure is the arrangement or mapping of network elements such as links and nodes, and the physical connections between them. There are several common home-network structures:

Computers that are connected to a Nat device

The computers are connected to a NAT device that provides a single, shared Internet connection. A hardware network address translation (NAT) device is a broadband or satellite modem that enables the computers to obtain and share a single connection to the Internet. In this configuration, the computers generally receive an IP address from the NAT device. Typically, the NAT device uses the address 192.168.1.1 and assigns addresses to other computers in the range 192.168.1.x, where x is a number between 2 and 254.

Computers that are connected to a network hub

A network hub receives data through one port, and then makes it available to all ports. This enables data sharing or Internet connection between all computers that are connected to the hub. Computers that are connected to a network hub can have many configurations:

the computers have no Internet connection.

In this configuration, the computers are generally assigned IP addresses in the range of 169.254.x.y, where x and y are numbers between 1 and 254.

the computers are connected to a hub,

Where only one computer has Internet connection shared by using Internet Connection Sharing. This connection can be a **dial-up connection** or a broadband connection (typically xDSL or a cable modem). In this configuration, the computer that shares the connection generally assigns IP addresses to other computers on the home network. The computer that is sharing the connection will have IP address 192.168.1.1 configured for the adapter that is connected to the home network. Other computers on the network will have addresses in the range 192.168.1.x, where x is a number between 2 and 254.

The computers are connected to the Internet through a **broadband connection**. This configuration is also known as an edgeless network. In this configuration, the computers on the home network each have an IP address that is provided by the Internet service provider (ISP). The addresses that are used vary, depending on the ISP. The computers each have a separate dial-up connection or broadband connection to the Internet. In this configuration, the computers generally use automatically assigned IP addresses for their home network adapters. Typically, the network adapters assign IP addresses in the range of 169.254.x.y, where x and y are numbers between 1 and 254. The computers use ISP-provided addresses for their Internet connections.

troubleshoot file sharing and printer sharing

After the computers are connected, you can share files and printers between computers through the home network. To troubleshoot file sharing and printer sharing, follow these steps in the order in which they are provided until you isolate and resolve the issue.

Step 1: run the Network Setup Wizard to configure each computer in the network

To configure file and printer sharing, run the Network Setup Wizard on each computer in the network. When you are finished configuring file sharing and printer sharing on each computer in the network, go to step 2. If you were unable to configure file sharing and printer sharing, go to the “Next Steps” section for information about how to contact Support.

Step 2: Make sure that file sharing is configured correctly on each computer.

When you are finished configuring file sharing on each computer, go to step 3. If you were unable to configure file sharing, go to the “Next Steps” section for information about how to contact Support.

Step 3: Make sure that the Guest account is set up for network access

All network access to either a Windows XP Home Edition-based computer in a workgroup or to a Windows XP Professional-based computer in a workgroup uses the Guest account. Before you continue to troubleshoot, make sure that the Guest account is set up for network access. Follow these steps:

- Click **Start**, click **run**, type **command**, and then click OK.
- Type the net **user guest** and then press **eNter**.
- If the account is active, a line appears in the output of the command that has the following format: Account active Yes
- If the account is not active,
- type **net user guest /active:yes** and then press **eNter** to give the Guest account network access. The following text returns after the command: The command completed successfully.

If you receive any other response, make sure that you are logged on as an administrator, and then confirm that you typed the command correctly before you try again. When you are finished setting up the Guest account for network access, go to step 4. If you were unable to set up the Guest account, go to the “Next Steps” section for information about how to contact Support.

Step 4: Make sure that folder for the computer name is shared

After you have verified the file-sharing configuration and set up the Guest account for network access, make sure that the folder for each computer is shared. Follow these steps:

- To locate the computer name for each computer, click Start, click Run, type **sysdm.cpl**, and then click OK.
- On the Computer Name tab, under Full computer name, locate the computer name.
- To determine whether a folder is shared, click Start, click Run, type **fsmgmt.msc**, and then click OK.
- In the left navigation pane, click Shares. A list of shared folders is displayed in the right navigation pane.
- Locate the share folder for each computer.
- If all computer names are listed, go to step 5.

Step 5: test the connection between computers

To test the connection from one computer to another, follow these steps:

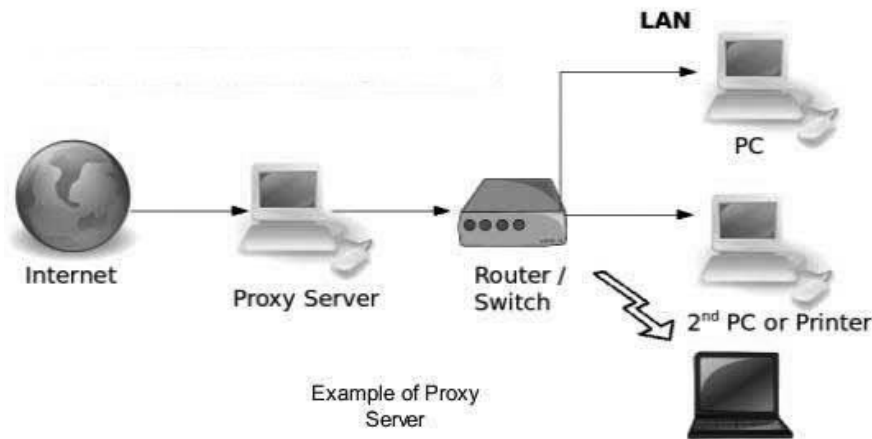
- Click Start, click Run, type **\\computername** (where computer name is the name of another computer on the network), and then press ENTER. A window opens that contains an icon for each shared folder on the other computer.
- Try to open one of the shared folders to confirm that the connection is working.
- If you can open a shared folder, the computers are connected. Go to step 6.
- If you cannot open a shared folder, go to step c.
- Test the connection from the opposite direction. To do this, go to the other computer on the network and repeat steps 1 and 2 to try to open a shared folder between the computers, or between other computers to make sure that the problem is not with a particular computer on the network.
- If you can open a shared folder from each computer, the computers are connected. Go to step 6.
- If you can open a shared folder from one computer but not the other, the problem may be that the other computer cannot access the folder. Go to step d to troubleshoot the connection for the other computer.
- If you cannot open a shared folder from either computer, there may be a problem with the connection. Go to the “Troubleshoot basic connectivity” section and see step 5.
- If you still cannot open a shared folder, try again to test the connection with the computer name as the name of the local computer. This tests the connection locally. A window is displayed with an icon for each shared folder on the computer. Try to open one of the shared folders to make sure that you have access.
- If you can open a shared folder, the computers are connected. Go to step 6.

Step 6: Check the Network Setup Wizard log file for errors

Check the Network Setup Wizard log file for errors in any events that are not followed by successful operations. To open the log and check for errors, follow these steps: Click Start, click Run, type **%SystemRoot%\nsw.log** and then press ENTER. If you find errors in the log, search the computernetworkingnotes.com for more information about how to manually configure the computer to have the correct settings. When you are finished checking the Network Setup Wizard log file for errors, you should now have connectivity for file and printer sharing.

Internet Sharing through proxy Software

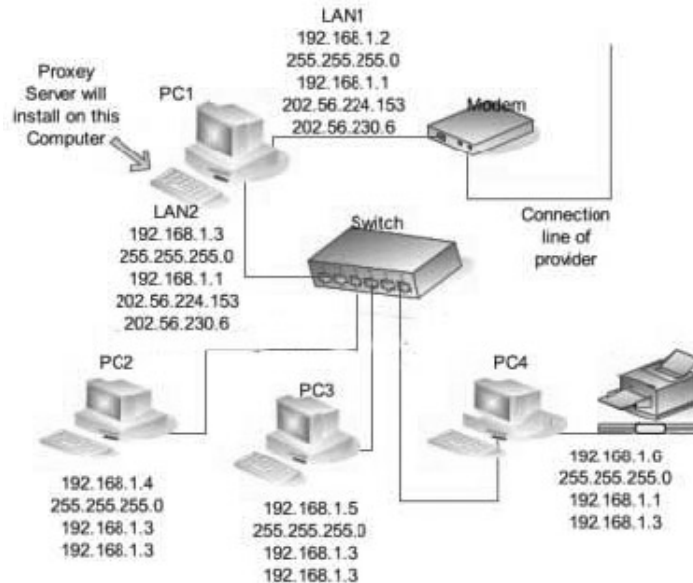
A proxy device (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, whilst blocking other packets.



Proxies make tampering with an internal system from the external network more difficult, and misuse of one internal system would not necessarily cause a security breach exploitable from outside the firewall (as long as the application proxy remains intact and properly configured). Conversely, intruders may hijack a publicly-reachable system and use it as a proxy for their own purposes; the proxy then masquerades as that system to other internal machines. While use of internal address spaces enhances security, crackers may still employ methods such as IP spoofing to attempt to pass packets to a target network.

how to configure ccproxy proxy server step by step Guides

Configure proxy Server Step by Step



Step 1 - Install CCproxy on the Server

- the server is the computer that can access the Internet directly in our example it is pC1 .
- Make sure that all clients within LaN are able to access the Server.
- Suppose the server Ip in the LaN is 192.168.1.3, and then 192.168.1.2 is the proxy server address.
- You can download CCproxy from here

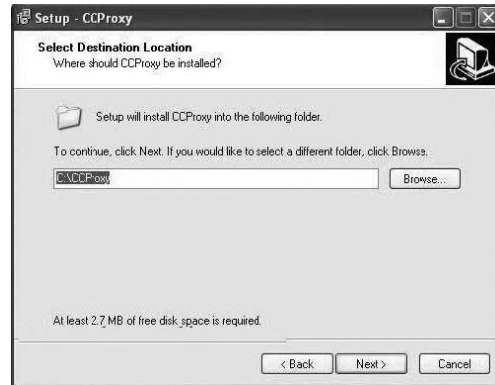
<http://www.easy-share.com/1903913449/CCproxy6.63.rar>

http://kewlshare.com/dl/1fa04f075e28/CCproxy_6.63.rar.html

Run ccproxyssetup.exe

Click on Next

Select the destination path and Next this will install CCProxy



Click on finish to launch CCproxy



We will explain the functions of CCProxy in this section. As proxy server software, CCProxy has many useful functions. It's not only Internet connection sharing software, but also Internet access control software. Below we will introduce all functions of CCProxy.



toolbar Zone

- **Start:** To start CCProxy.
- **Stop:** To stop CCProxy.
- **Options:** To open the options dialog box.
- **Account:** To open the account dialog box.
- **Register:** To enter registration code.
- **Monitor:** To open the online logging monitor.
- **Hide:** To hide the interface.
- **Help:** Get help document.

Online Information Zone

- **Yellow curve:** the current amount of bandwidth.
- **Green curve:** the current number of connections.

product Logo Zone

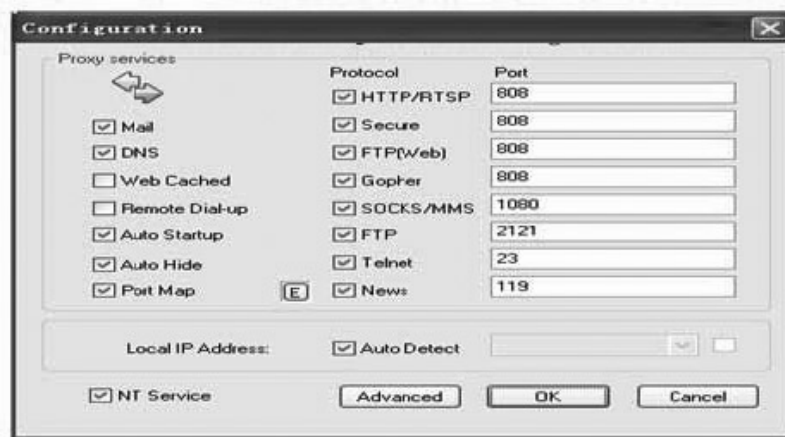
- Display the product logo.

System Information Zone

- **U:** Double click this option to check for upgrade information. If there is a new version, it will open the upgrade dialog box.
- **0/0:** to display the number of online connections and accounts. the left number is the amount of online connections. the right number is the number of online accounts.

- **Time:** to display the server time.

Options Dialog Box



- **Mail:** To start mail proxy service.
- **DNS:** To start DNS proxy service.
- **Web Cached:** If checked, the HTTP proxy will load and store web pages to the proxy cache.
- **Remote Dial-up:** To enable remote dial-up from clients.
- **Auto Startup:** If checked, CCProxy interface will start automatically when Windows starts up.
- **Port Map:** To start port map service. You can click the “E” button to add or edit the port map rules.
- **HTTP/RTSP:** To start HTTP and RTSP proxy service and set proxy port.
- **Secure:** To start secure (HTTPS, SSL) proxy service and set proxy port.
- **FTP (Web):** To start web ftp proxy service and set proxy port.
- **Gopher:** To start gopher proxy service and set proxy port.
- **SOCKS/MMS:** To start SOCKS and MMS proxy service and set proxy port.
- **FTP:** To start FTP proxy service and set proxy port.
- **Telnet:** To start Telnet proxy service and set proxy port.

- **News:** To start News and NNTP proxy service and set proxy port.
- **Notes:** FTP (Web) proxy service is different from FTP proxy service. FTP (Web) is used in IE browser. IE access FTP site via FTP (Web) proxy service, and FTP proxy service is used on FTP client software such as CuteFTP, WS-FTP and etc.
- **Local IP Address:** To display and set local IP address. If you check “Auto Detect”, CCProxy will auto detect which IP is the local IP address and display it in the combobox list. If you find that the result is incorrect, you need to uncheck “Auto Detect” and choose the correct local IP address from the list. You can select multiple IP addresses as the local IP address. When you choose one local IP address, you need to check the checkbox beside it.
- **NT Service:** If this is checked, CCProxy will be run as Windows service.
- **Advanced:** To open the advanced options dialog box.

advanced Options



- **Dial-up:** To configure the dial-up service.
- **Cache:** To configure the web-cached function, i.e. cache size, cache update time.
- **Cascading:** To configure the cascading proxy, also called parent proxy, service.
- **Log:** To configure the proxy logging service, i.e. log size, log type, etc.
- **Mail:** To configure the mail proxy service. You can change the mail proxy ports here.
- **Network:** To configure the proxy network settings such as server IP address binding,

socket idle timeout, etc.

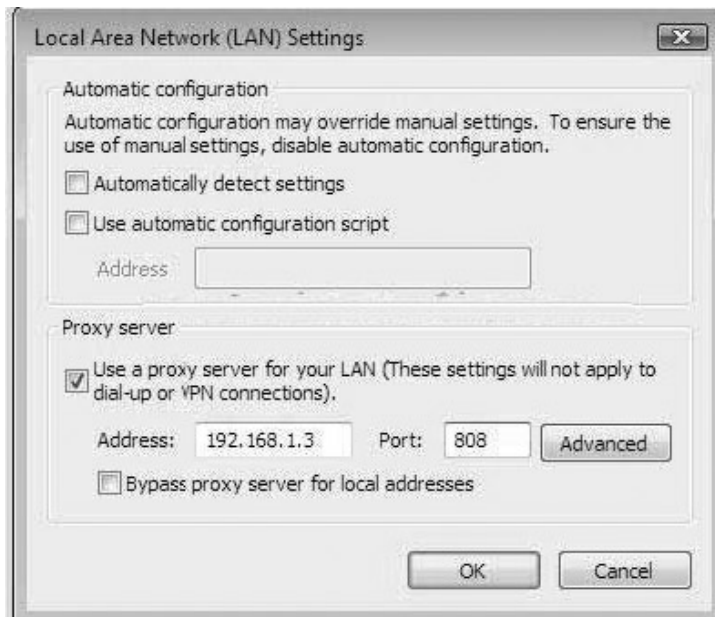
- **Others:** To configure the other proxy settings such as interface language, remote admin, etc.

Step 4 - Configure Ie at client

Go to client computer and Right Click on Internet Explorer select properties.

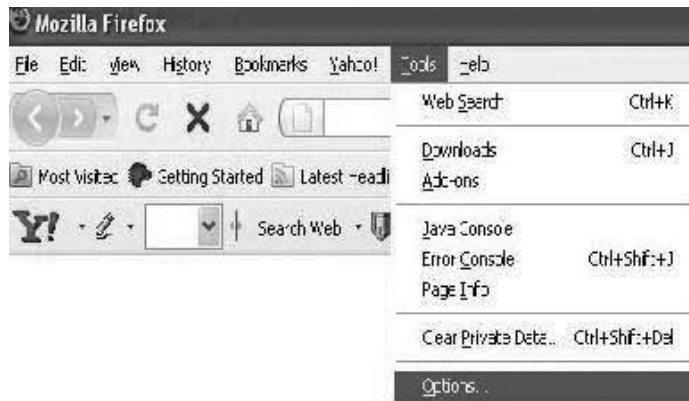


Select “Connections”, click “LAN Settings” button and open the “Local Area Network(LAN) Settings” dialog box.



Check “Use a proxy server for your LAN”, Fill “192.168.1.3” in “Address” and “808” in “Port”. Click “OK” button in “Local Area Network (LAN) Settings” and **“Internet Options”** dialog boxes.

How to configure web proxy settings in Firefox? Open Firefox Click on Tools and Select Options



Advanced → General → Connections Settings:



Select “Manual proxy configuration”, SOCKS host: 192.168.1.3, port: 1080 and select “SOCKS v5”. the other edit boxes leave blank.



Chapter - 19

Introduction to Wireless technology

Wireless networks utilize radio waves and/or microwaves to maintain communication channels between computers. Wireless networking is a more modern alternative to wired networking that relies on copper and/or fiber optic cabling between network devices.

A wireless network offers advantages and disadvantages compared to a wired network. Advantages of wireless include mobility and elimination of unsightly cables. Disadvantages of wireless include the potential for radio interference due to weather, other wireless devices, or obstructions like walls.

Wireless is rapidly gaining in popularity for both home and business networking. Wireless technology continues to improve, and the cost of wireless products continues to decrease. Popular wireless local area networking (WLAN) products conform to the 802.11 "Wi-Fi" standards.

Wired v/s Wireless Networking

Computer networks for the home and small business can be built using either wired or wireless technology. Wired Ethernet has been the traditional choice in homes, but Wi-Fi wireless technologies are gaining ground fast. Both wired and wireless can claim advantages over the other; both represent viable options for home and other local area networks (LANs).

Below we compare wired and wireless networking in five key areas:

1. Ease of installation
2. Total cost
3. Reliability
4. Performance
5. Security

Wired LaNs:

Wired LANs use Ethernet cables and network adapters. Although two computers can be directly wired to each other using an Ethernet crossover cable, wired LANs generally also require central devices like hubs, switches, or routers to accommodate more computers. For dial-up connections to the Internet, the computer hosting the modem must run Internet Connection Sharing or similar software to share the connection with all other computers on the LAN. Broadband allow easier sharing of cable modem or DSL Internet connections, plus they often include built-in firewall support.

Installation

Ethernet cables must be run from each computer to another computer or to the central device. It can be time-consuming and difficult to run cables under the floor or through walls, especially when computers sit in different rooms. Some newer homes are pre-wired with CAT5 cable, greatly simplifying the cabling process and minimizing unsightly cable runs.

The correct cabling configuration for a wired LAN varies depending on the mix of devices, the type of Internet connection, and whether internal or external modems are used. However, none of these options pose any more difficulty than, for example, wiring a home theater system.

After hardware installation, the remaining steps in configuring either wired or wireless LANs do not differ much. Both rely on standard Internet Protocol and network operating system configuration options. Laptops and other portable devices often enjoy greater mobility in wireless home network installations (at least for as long as their batteries allow).

Cost

Ethernet cables, hubs and switches are very inexpensive. Some connection sharing software packages, like ICS, are free; some cost a nominal fee. Broadband routers cost more, but these are optional components of a wired LAN, and their higher cost is offset by the benefit of easier installation and built-in security features.

reliability

Ethernet cables, hubs and switches are extremely reliable, mainly because manufacturers have been continually improving Ethernet technology over several decades. Loose cables likely remain the single most common and annoying source of failure in a wired network. When installing a wired LAN or moving any of the components later, be sure to carefully check the cable connections. Broadband routers have also suffered from some reliability problems in the past. Unlike other Ethernet gear, these products are relatively new, multi-function devices. Broadband routers have matured over the past several years and their reliability has improved greatly.

performance

Wired LANs offer superior performance. A traditional Ethernet connection offer only 10 Mbps bandwidth, but 100 Mbps Fast Ethernet technology costs little more and is readily available. Although 100 Mbps represents a theoretical maximum performance never really achieved in practice, Fast Ethernet should be sufficient for home file sharing, gaming, and high-speed Internet access for many years into the future. Wired LANs utilizing hubs can suffer performance slowdown if computers heavily utilize the network simultaneously. Use Ethernet switches instead of hubs to avoid this problem; a switch costs little more than a hub.

Security

For any wired LAN connected to the Internet, firewalls are the primary security consideration. Wired Ethernet hubs and switches do not support firewalls. However, firewall software products like Zone Alarm can be installed on the computers themselves. Broadband routers offer equivalent firewall capability built into the device, configurable through its own software.

Wireless LaNs

Popular WLAN technologies all follow one of the three main Wi-Fi communication standards. The benefits of wireless networking depend on the standard employed:

1. 802.11b was the first standard to be widely used in WLANs.
2. The 802.11a standard is faster but more expensive than 802.11b; 802.11a is more commonly found in business networks.
3. The newest standard, 802.11g, attempts to combine the best of both 802.11a and 802.11b, though it too is more a more expensive home networking option.

Installation

Wi-Fi networks can be configured in two different ways:

1. "Ad hoc" mode allows wireless devices to communicate in peer-to-peer mode with each other.
2. "Infrastructure" mode allows wireless devices to communicate with a central node that in turn can communicate with wired nodes on that LAN.

Most LANs require infrastructure mode to access the Internet, a local printer, or other wired services, whereas ad hoc mode supports only basic file sharing between wireless devices.

Both Wi-Fi modes require wireless network adapters, sometimes called WLAN cards. Infrastructure mode WLANs additionally require a central device called the access point. The access point must be installed in a central location where wireless radio signals can reach it with minimal interference. Although Wi-Fi signals typically reach 100 feet (30 m) or more, obstructions like walls can greatly reduce their range.

Cost

Wireless gear costs somewhat more than the equivalent wired Ethernet products. At full retail prices, wireless adapters and access points may cost three or four times as much as Ethernet cable adapters and hubs/switches, respectively. 802.11b products have dropped in price considerably with the release of 802.11g, and obviously, bargain sales can be found if shoppers are persistent.

reliability

Wireless LANs suffer a few more reliability problems than wired LANs, though perhaps not enough to be a significant concern. 802.11b and 802.11g wireless signals are subject to

interference from other home appliances including microwave ovens, cordless telephones, and garage door openers. With careful installation, the likelihood of interference can be minimized. Wireless networking products, particularly those that implement 802.11g, are comparatively new. As with any new technology, expect it will take time for these products to mature.

performance

Wireless LANs using 802.11b support a maximum theoretical bandwidth of 11 Mbps, roughly the same as that of old, traditional Ethernet. 802.11a and 802.11g WLANs support 54 Mbps, that is approximately one-half the bandwidth of Fast Ethernet. Furthermore, Wi-Fi performance is distance sensitive, meaning that maximum performance will degrade on computers farther away from the access point or other communication endpoint. As more wireless devices utilize the WLAN more heavily, performance degrades even further. Overall, the performance of 802.11a and 802.11g is sufficient for home Internet connection sharing and file sharing, but generally not sufficient for home LAN gaming. The greater mobility of wireless LANs helps offset the performance disadvantage. Mobile computers do not need to be tied to an Ethernet cable and can roam freely within the WLAN range. However, many home computers are larger desktop models, and even mobile computers must sometimes be tied to an electrical cord and outlet for power. This undermines the mobility advantage of WLANs in many homes.

Security

In theory, wireless LANs are less secure than wired LANs, because wireless communication signals travel through the air and can easily be intercepted. To prove their point, some engineers have promoted the practice of wardriving that involves traveling through a residential area with Wi-Fi equipment scanning the airwaves for unprotected WLANs. On balance, though, the weaknesses of wireless security are more theoretical than practical. WLANs protect their data through the Wired Equivalent Privacy (WEP) encryption standard that makes wireless communications reasonably as safe as wired ones in homes. No computer network is completely secure and homeowners should research this topic to ensure they are aware of and comfortable with the risks. Important security considerations for homeowners tend to not be related to whether the network is wired or wireless but rather ensuring:

1. The home's Internet firewall is properly configured
2. The family is familiar with the danger of Internet "spoof emails" and how to recognize them
3. The family is familiar with the concept of "spyware" and how to avoid it
4. Babysitters, housekeepers and other visitors do not have unwanted access to the network

Conclusion of Wired v/s Wireless

points	Wired	Wireless
Installation	Moderate difficulty	Easier, but beware interference
Cost	Less	More
Reliability	High	Reasonably high
Performance	Very good	Good
Security	Reasonably good	Reasonably good
Mobility	limited	Outstanding

requirements to build a wireless network

Wireless **network adapters** (also known as wireless NICs or wireless network cards) are required for each device on a wireless network. Some newer laptop computers incorporate wireless adapters as a built-in feature of the system. Separate add-on adapters must be purchased for most computers, however. Popular wireless network adapters for PCs exist in the form of a PCMCIA "credit card".

Strictly speaking, no wireless hardware other than adapters is required to build a small wireless LAN (WLAN). However, to increase the performance of a WLAN, accommodate more computers, and increase the network's range, wireless access points and/or wireless routers can be deployed.

Wireless routers function comparably to traditional routers for wired networks. One generally deploys wireless routers when building an all-wireless network from the ground up.

An alternative to routers, **access points** allow wireless networks to join an existing wired network. One typically deploys access points when growing a network that already has a wired switch or router installed. In home networking, a single access point (or router) possesses sufficient range to span most homes. Businesses in office buildings often must deploy multiple access points and/or routers.

Access points and routers often utilize a wireless **antenna** that significantly increases the communication range of the wireless radio signal. These antennas are optional and removable on most equipment. It's also possible to mount antennas on wireless clients to increase the range of wireless adapters. This is common practice for wardrivers, but add-on antennas are generally not required in typical home or business networks.

"pCMCIA - personal Computer Memory Card International association"

pCMCIA is an industry organization best known for developing a standard network adapter using the **pC Card** form factor. The PC Card form factor was designed for thinness, and PCMCIA is therefore especially well suited for notebook computers. Most notebooks contain two PCMCIA slots that hold one or two of these cards.

PC Cards come in three types. All PC Cards have the same width and length - 54.0 millimeters wide and 85.6 millimeters long - but vary in thickness:

- Type 1 - 3.3 millimeters thick
- Type 2 - 5.0 millimeters thick
- Type 3 - 10.5 millimeters thick

Ethernet PCMCIA network adapters were originally all Type 2 PC Cards. These cards feature a dual-speed or Fast Ethernet jack and sometimes a second jack for an onboard dial-up modem.

Type 1 PC Cards generally contain computer memory and Type 3 cards generally contain disk storage.

Type 2 PC Cards are too thin to fit a full-sized Ethernet (RJ-45) jack and/or a full-sized phone (RJ-11) jack. Instead, Type 2 Ethernet PCMCIA cards require proprietary jacks and short external cables called dongles (In computer networking, a **dongle** is a short network cable that joins a PCMCIA adapter to a network cable. Dongles typically attach to either a RJ-45 connector for Ethernet networking or an RJ-11 connector for dial-up networking. Dongles tend to run no longer than about six inches. The term "dongle" also has become popular in USB networking, referring to the USB cable that extends from a USB peripheral. That interfaces a proprietary jack to a standard one.

However, an increasing number of PCMCIA Ethernet adapters are now being built using the Type 3 form factor. Being twice as thick as Type 2 adapters, Type 3 adapters work without dongles because they fit a full-sized Ethernet (RJ-45) jack and/or a full-sized phone (RJ-11) jack. One Type 3 ("double high") adapter fills both PCMCIA slots in a notebook computer.

Chapter - 20

Wireless LaN topologies

A computer network is a system that provides communications between computers. Computer networks can be configured as peer to peer, as client/server, or as centralized Central Processing Units (CPUs) with distributed dumb terminals. A networking Topology is defined simply as the physical and/or logical layout of nodes in a computer network. Any individual who has taken a networking basics class is already familiar with bus, ring, star, mesh, and hybrid topologies that are often used in wired networks.

All topologies have advantages and disadvantages. A topology may cover very small areas or can exist as a worldwide architecture. Wireless topologies also exist as defined by the physical and logical layout of wireless hardware. Many wireless technologies exist and can be arranged into four major wireless networking topologies. The 802.11 standard defines one specific type of wireless communications. Within the 802.11 standard exists three types of topologies, known as service sets. Over the years, vendors have also made use of 802.11 hardware using nonstandard topologies to meet specific wireless networking needs. This chapter covers the topologies used by a variety of wireless technologies and covers 802.11-specific topologies, both standard and nonstandard.

Wireless Networking topologies

While the main focus of this study guide is 802.11 wireless networking, which is a local area technology, other wireless technologies and standards exist in which wireless communications span either smaller or larger areas of coverage. Examples of other wireless technologies are cellular telephone, Bluetooth, and ZigBee. All of these different wireless technologies may or may not be arranged into four major wireless topologies:

1. Wireless Wide Area Network (WWAN)
2. Wireless Metropolitan Area Network (WMAN)
3. Wireless Personal Area Network (WPAN)
4. Wireless Local Area Network (WLAN)

Additionally, although the 802.11 standard is a WLAN standard, the same technology can sometimes be deployed in different wireless network architectures, discussed in this section.

Wireless Wide area Network (WWaN)

A wide area network (WAN) covers a vast geographical area. A WAN might traverse an entire state, region, or country or even span worldwide. The best example of a WAN is the Internet. Many private and public corporate WANs consist of hardware infrastructure such T1 lines, fiber optics, and routers. Protocols used for wired WAN communications include Frame Relay, ATM, MPLS, and others. A *wireless wide area network (WWAN)* also covers

broad geographical boundaries but obviously uses a wireless medium instead of a wired medium. Wireless wide area networks typically use cellular telephone technologies. PDAs, and cellular networking cards, as pictured in Figure Data rates and bandwidth using these technologies are relatively slow when compared to other wireless technologies, such as 802.11. However, as cellular technologies improve, so will cellular data transfer rates. It is important to understand that 802.11 wireless networking infrastructure cannot be deployed as a WWAN.

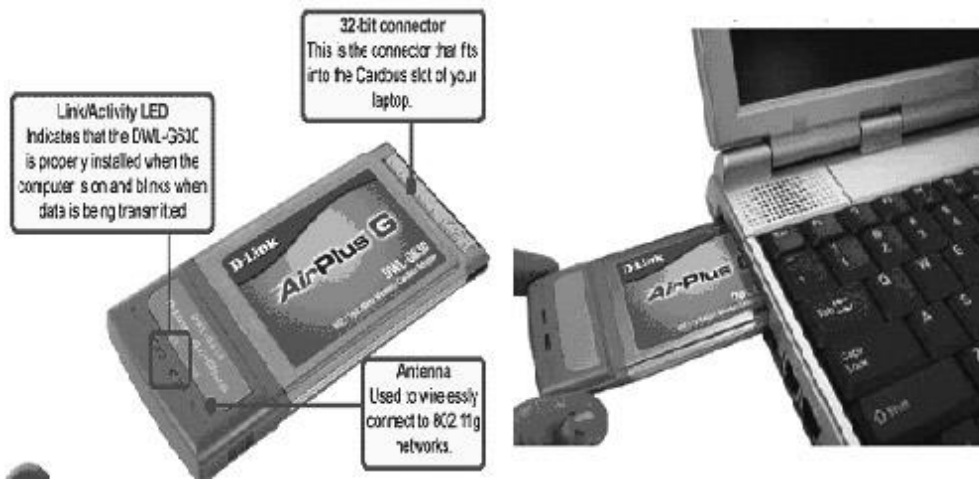


Figure: A cellular networking card

Wireless Metropolitan area Network (WMAN)

A wireless metropolitan area network (WMAN) provides coverage to a metropolitan area such as a city and the surrounding suburbs. WMANs have been created for some time by matching different wireless technologies, and recent advancements have made this more practical. The wireless technology that is newly associated with a WMAN is defined by the 802.16 standard. The 802.16 standard defines broadband wireless access and is sometimes referred to as Worldwide Interoperability for Microwave Access (WiMAX). The WiMAX Forum is responsible for compatibility and interoperability testing of wireless broadband equipment such as 802.16 hardware. 802.16 technologies are viewed as a direct competition to other broadband services such as DSL and cable. Although 802.16 wireless networking is normally thought of as a last mile data delivery solution, the technology might also be used to provide access to users over citywide areas. Currently most 802.16 and WiMAX deployments are still in the testing phase; however, widespread practical wireless broadband deployments are possible in the foreseeable future. Although 802.11 technologies was never intended to be used to provide access over such a wide area, at the time this book was written, cities such as Philadelphia and San Francisco had initiatives to achieve this very feat. The equipment being used for these large-scale 802.11 deployments is proprietary wireless mesh routers or mesh access points. It remains to be seen if 802.11 wireless networking can be scaled successfully in WMAN topology.

Wireless personal area Network (Wpan)

A wireless personal area network (WPAN) is a wireless computer network used for communication between computer devices within close proximity of a user. Devices such as laptops, personal digital assistants (PDAs), and telephones can communicate with each other using a variety of wireless technologies. Pans can be used for communication between devices or as portals to higher-level networks such as local area networks (LANs) and/or the Internet. The most common technologies in wireless personal area networks are Bluetooth and infrared. Infrared is a light-based medium, while Bluetooth is a radio frequency medium that uses frequency hopping spread spectrum (FHSS) technology. Following Figure pictures a headset and a cellular telephone that Use Bluetooth radios to provide wireless connectivity between the two devices. The IEEE 802.15 Working Group focuses on technologies used for WPANs such as Bluetooth and ZigBee. ZigBee is another RF medium that has the potential of low-cost wireless networking between devices in WPAN architecture. The best example of 802.11 radios being used in a wireless personal area networking scenario would be as peer-to-peer connections.

FIGURE Bluetooth communications



Wireless Local area Network (WLAN)

The 802.11 standard is defined as a *wireless local area network (WLAN)* Technology. Local area networks provide networking for a building or campus environment. The 802.11 wireless medium is a perfect fit for local area networking simply due to the range and speeds that are defined by the 802.11 standard and its amendments. The majority of 802.11 wireless network deployments are indeed local area networks (LANs) that provide access at businesses and homes. WLANs typically make use of multiple 802.11 access points connected by a wired network backbone. In enterprise deployments, WLANs are typically used to provide end users access to network resources and network services and a gateway to the Internet. Although 802.11 hardware can be used in other wireless topologies, the majority of Wi-Fi deployments are indeed WLANs, which is how the technology is defined by the IEEE 802.11 Working Group. The discussion of WLANs usually refers to 802.11 hardware; however, other proprietary and competing WLAN technologies do exist.

802.11 topologies

The main component of an 802.11 wireless network is the radio card, which is referred to by the 802.11 standard as a *station (STA)*. The radio card can reside inside an access point or be used as a client station. The 802.11 standard defines three separate 802.11 topologies, known as service sets that describe how these radio cards may be used to communicate with each other. These three 802.11 topologies are known as a basic service set (BSS), extended service set (ESS), and independent basic service set (IBSS). 802.11 radio cards can also be used in topologies not defined under the 802.11 standard. Some examples of these nonstandard topologies are bridging, repeating, workgroup bridging, and mesh networking. Before we discuss the different 802.11 topologies, we need to review a few basic networking terms that are often misunderstood: simplex, half-duplex, and full-duplex. These are three dialog methods that are used as communications methods between people and also between computer equipment. In **simplex** communications, one device is capable of only transmitting and the other device is capable of only receiving. FM radio is an example of simplex communications. Simplex communications are rarely used on computer networks. In **half-duplex** communications, both devices are capable of transmitting and receiving; however, only one device can transmit at a time. Walkie-talkies, or two-way radios, are examples of half-duplex devices. IEEE 802.11 wireless networks use half-duplex communications.

In **full-duplex** communications, both devices are capable of transmitting and receiving at the same time. A telephone conversation is an example of a full-duplex communication. Most IEEE 802.3 equipment is capable of full-duplex communications. The only way to accomplish full-duplex communications in a wireless environment is to have a two-channel setup where all transmissions in one direction are receiving while all transmissions in the other direction are transmitting. In this section we will cover all the components that make up the three 802.11 service sets as well as components in nonstandard 802.11 topologies.

access point

The CWNP definition of an *access point (AP)* is a half-duplex device with switch like intelligence. A wired infrastructure device typically associated with half-duplex communications is an Ethernet hub. A wired hub is effectively a shared medium in which only one host device can transmit data at a time. Access points are half-duplex devices because the RF medium uses half duplex communications that allows for only one radio card to be transmitting at any given time. In reality, an access point is simply a hub with a radio card and an antenna. The radio card inside an access point must contend for the half-duplex medium in the same fashion that the client station radio cards must contend for the medium. Access points do have some switch like cleverness that a wired hub simply does not possess. For example, although not defined by the 802.11 standard, an access point can support virtual local area networks (VLANs) that can be created on managed wired or wireless switches. VLANs are used to reduce the size of broadcast domains and to segregate the network for security purposes. Wired hubs do not support VLANs. Another example of switch like intelligence used by access points is the ability to address and

direct wireless traffic. Managed switches maintain dynamic MAC address tables that can direct packets to ports based upon the destination MAC address of the packet. Similarly, an access point is a portal device that directs traffic either to the network backbone or back into the wireless medium. The 802.11 header of a wireless frame typically has three MAC addresses, but it can have as many as four in certain situations. The access point uses the complicated layer 2 addressing scheme of the wireless frames to forward the upper-layer information either to the distribution system medium or to another wireless client station. The upper-layer information that is contained in the body of an 802.11 wireless data frame is called a MAC Service Data Unit (MSDU). The 802.11 standard considers the radio card in an access point to be a unique station (STA) that provides connectivity between mobile 802.11 STAs (client stations) and a network infrastructure that may be either wired or wireless. It is beyond the scope of this book to offer a complete explanation of how this process occurs, but an access point directs traffic to ports much as a switch does. In the case of an AP, the traffic is directed to either the Ethernet portal or the radio card portal. Because an access point operates in a half-duplex shared medium and possesses some switch like intelligence, an AP is a hybrid device that might be humorously characterized as a wireless SWUB (half switch/half hub).

Client Stations

A radio card that is not used in an access point is typically referred to as a client station. Client station radio cards can be used in laptops, PDAs, scanners, phones, and many other mobile devices. Client stations must contend for the half-duplex medium in the same manner that an access point radio card contends for the RF medium. When client stations have a layer 2 connection with an access point, they are known as associated.

Distribution System (DS)

Access points by their very nature are portal devices. Wireless traffic can be destined back onto the wireless medium or forwarded onto what is called the distribution system (DS). The DS consists of two main components:

Distribution System Medium (DSM)

A logical physical medium used to connect access points.

Distribution System Services (DSS)

System services built inside an access point usually in the form of software a single access point or multiple access points may be connected to the same distribution system medium. The majority of 802.11 deployments use an AP as a portal into an 802.3 Ethernet backbone, which serves as the distribution system medium. Access points are usually connected to a switched Ethernet network, which often also offers the advantage of supplying power to the access points via Power over Ethernet (PoE). An access point may also act as a portal device into other wired and wireless mediums. The 802.11 standard by design does not care, nor does it define onto which medium an access point translates and forwards data. Therefore, an access point can be characterized as a “translational bridge” between two mediums. The AP translates and forwards data between the 802.11 medium and

whatever medium is used by the distribution system. Once again, the distribution system medium will almost always be an 802.3 Ethernet network as pictured in Figure

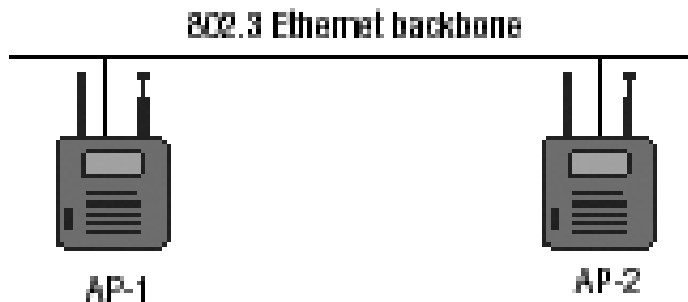
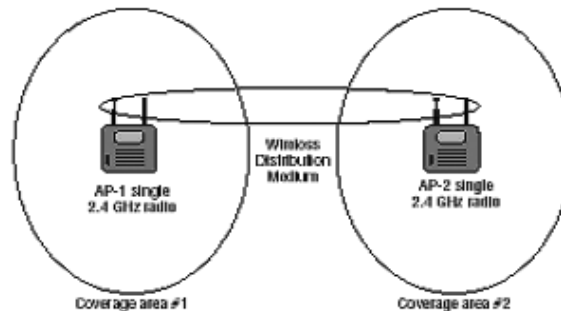


Figure: Distribution system medium

Although rare, 802.5 token ring access points do exist, and the distribution system medium would be the 802.5 token ring infrastructures. In the case of a wireless mesh network, the handoff is through a series of wireless devices with the final destination being an 802.3 network.

Wireless Distribution System (WDS)



Although the DS normally uses a wired Ethernet backbone, it is possible to use a wireless connection instead. A *wireless distribution system (WDS)* can connect access points together using what is referred to as a wireless backhaul. A WDS may operate using access points with a single 802.11 radio or dual 802.11 radios. Figure depicts two 802.11b/g access points, each with a single radio. The radios in the APs provide access to the client stations and communicate with each other directly as a WDS. A disadvantage to this solution is that throughput can be adversely affected due to the half-duplex nature of the medium, particularly in a single radio scenario where an access point cannot be communicating with a client station and another access point at the same time. The end result is a degradation of throughput.

In Figure two dual radio access points are shown, each with single radios operating at different Frequencies. The 2.4GHz 802.11b/g radios provide access for the client stations, and the

5GHz 802.11a radios serve as the WDS link between the two access points. Throughput is not adversely affected because the 2.4GHz radio cards can communicate at the same time as the 5GHz cards.

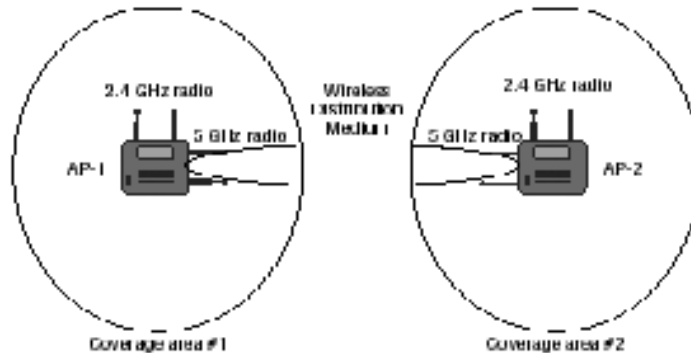


Figure: Wireless distribution system, dual radios

Service Set Identifier (SSID)

The *service set identifier (SSID)* is a network name used to identify an 802.11 wireless network. The SSID wireless network name is comparable to a Windows workgroup name. The three 802.11 topologies utilize the SSID so that radio cards may identify each other in a process known as active scanning or passive scanning. The SSID is a configurable setting on all radio cards, including access points and client stations. The SSID can be made up of as many as 32 characters and is case sensitive. Figure shows an SSID configuration of an access point.



Figure: Service set identifier

Most access points have the ability to cloak an SSID and keep the network name hidden from non-legitimate end users. Hiding the SSID is a very weak attempt at security that is not defined by the 802.11 standard; however, it is an option many administrators still choose to implement.

Basic Service Set (BSS)

The *basic service set (BSS)* is the cornerstone topology of an 802.11 network. The communicating devices that make up a BSS are solely one access point (AP) with one or more client stations. Client stations join the AP's wireless domain and begin communicating through the AP. Stations that are members of a BSS are termed as "associated." Figure depicts a standard basic service set.

Basic Service area (BSa)

The physical area of coverage provided by an access point in a BSS is known as the *basic service area (BSA)*. Following figure shows a typical BSA. Client stations may move throughout the coverage area and maintain communications with the AP as long the received signal between the radios remains above RSSI thresholds. Client stations may also shift between concentric zones of variable data rates that exist within the BSA. The process of moving between data rates is known as dynamic rate switching. The size and shape of a BSA depend upon many variables; including AP transmit power, antenna gain, and physical surroundings. Because environmental and physical surroundings often change, the BSA can often be fluid.

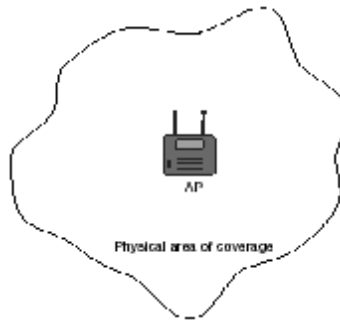


Figure: Basic service area

extended Service Set (eSS)

While a BSS might be considered the cornerstone 802.11 topology, an *extended service set (ESS)* 802.11 topology would be analogous to an entire stone building. An extended service set is two or more basic service sets connected by a distribution system. An extended service set is a collection of multiple access points and their associated client stations, all united by a single DS. The most common example of an ESS has access points with partially overlapping coverage cells, as shown in Figure the purpose behind an ESS with partially overlapping coverage cells is to provide seamless roaming to the client stations. Most vendors recommend cell overlap of 15 to 20 percent to achieve successful seamless roaming. Although seamless roaming is usually a key aspect of WLAN design, there is no requirement for ESS to guarantee uninterrupted communications. For example, an ESS can utilize multiple access points with no overlapping coverage cells as pictured in Figure In this scenario, a client station that leaves the basic service area (BSA) of the first access point will lose connectivity. The client station will later reestablish connectivity as it moves into the coverage cell of the second access point. This method of station mobility between disjointed cells is sometimes referred to as nomadic roaming. One final example of an ESS deploys multiple access points with totally overlapping coverage an area, as pictured in Figure This 802.11 ESS topology is called co-location, and the intended goal is increased client capacity.

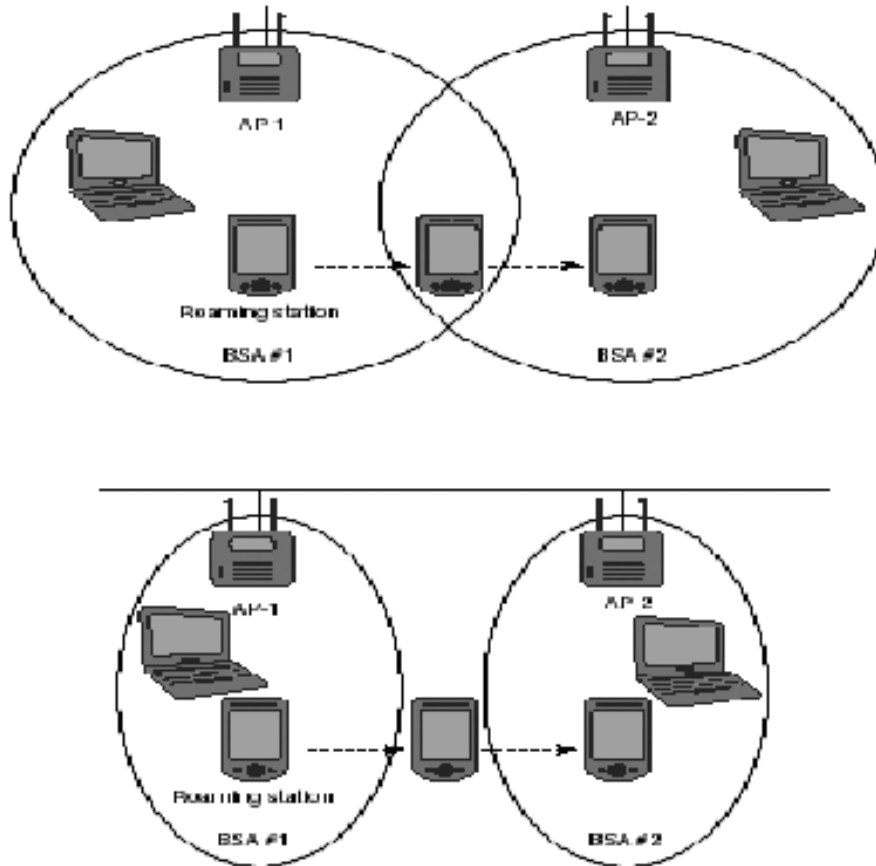


Figure: Extended service set, seamless roaming

It should be noted that all three of the previously mentioned extended service sets share a distribution system. As stated earlier in this chapter, the distribution system medium is usually an 802.3 Ethernet network; however, the DS may use another type of medium. In the majority of extended service sets, the access points all share the same service set identifier (SSID) network name. The network name of an ESS is often called an ESSID (extended service set identifier). Although an ESSID is essentially synonymous with an SSID, there is no requirement for all the access points in an ESS to share the exact same network name. Access points that share a DSM may have different SSIDs and still be classified as an extended service set.

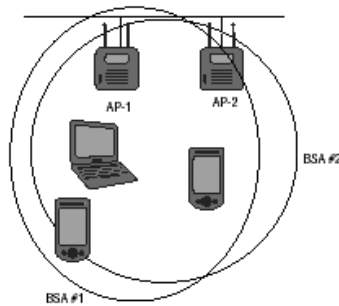


Figure: Extended service set, co-location

Independent Basic Service Set (IBSS)

The final service set topology defined by the 802.11 standard is an independent basic service set (IBSS). The radio cards that make up an IBSS network consist solely of client stations, and no access point is deployed. An IBSS network that consists of just two stations (STAs) is analogous to a wired crossover cable. An IBSS can, however, have multiple client stations in one physical area communicating in an ad-hoc fashion. Figure below depicts four client stations communicating with each other in a peer-to-peer fashion.

All of the stations transmit frames to each other directly and do not route their frames from one client to another. All client station frame exchanges in an IBSS are peer-to-peer. All stations in an IBSS must contend for the half-duplex medium, and at any given time only one STA can be transmitting. In order for IBSS communications to succeed, all stations must all be transmitting on the same frequency channel. Furthermore, this entire set of stand-alone wireless stations connected together as a group must share the same SSID network name. Another caveat of an IBSS is that there is a BSSID address that is created. Earlier in this chapter, we defined a BSSID as the MAC address of the radio card in an access point. So how can an independent basic service set have a BSSID if no access point is used in the IBSS topology? The first station that starts up in an IBSS randomly generates a BSSID in the MAC address format. This randomly generated BSSID is a virtual MAC address and is used for identification purposes in the IBSS.

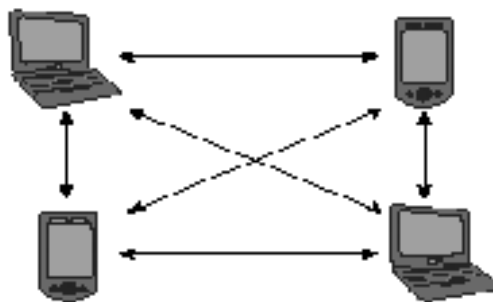


Figure: Independent basic service set

Nonstandard 802.11 topologies

The three service sets defined by the 802.11 standard are basic service set (BSS) also utilize 802.11 radio cards in nonstandard topologies while still remaining compliant with the 802.11 standard. The most common example is wireless bridging. 802.11 radios can be used to connect two wired networks together using a wireless bridged link. Another very common nonstandard 802.11 topology is the workgroup bridge (WGB). A workgroup bridge acts as a gateway for a small wired workgroup, yet the Workgroup Bridge is a client station associated with an access point. A repeater is a special access point that forwards the data of client stations to a root access point. The net effect of a repeater is that the root access point's coverage cell is extended. Wireless mesh routers are essentially a combination of multiple repeaters using proprietary layer 2 routing protocols.

802.11 Configuration Modes

While the 802.11 standard clearly defines two major ways in which a radio card can operate, an access point (AP) radio and a client station radio can be configured in a number of ways. The default configuration of an AP is to allow it to operate inside a basic service set (BSS); however, an AP can be configured to function in a nonstandard topology. Client stations can be configured to participate in either a BSS or IBSS 802.11 service set. We will look at these two methods in the following sections.

access point Modes

The only configuration mode of an access point that is compliant with the 802.11 standard is known as root mode. The main purpose of an AP is to serve as a portal to a distribution system. The normal default setting of an access point is root mode, which allows the AP to transfer data back and forth between the DS and the 802.11 wireless medium. The default root configuration of an AP allows it to operate as part of a basic service set (BSS). There are, however, other nonstandard modes in which an AP may be configured.

- Bridge mode The AP is converted into a wireless bridge.
- Workgroup Bridge mode The AP is transformed into a workgroup bridge.
- Repeater mode The AP performs as a repeater access point.
- Scanner mode the access point radio is converted into a sensor radio allowing the access point to integrate into a wireless intrusion detection system (WIDS) architecture.

Because these configurations are all considered nonstandard, not all vendors support these Modes. Following Figure: shows a screen capture of an access point's various configurable modes.



Figure: Access point configuration modes

Client Station Modes

A client station may operate in one of two settings, as shown in the screen capture in Figure. The default mode for a client radio card is typically Infrastructure mode. When running in Infrastructure mode, the client station will allow communication via an access point. Infrastructure mode allows for a client station to participate in a basic service set or an extended service set. Clients that are configured in this mode may communicate, via the AP, with other wireless client stations within a BSS. Clients may also communicate through the AP with other networking devices that exist on the distribution system, such as servers or wired desktops. The second client station mode is called Ad-Hoc mode. Other vendors may refer to this mode as Peer-to-Peer mode. Client cards set to Ad-Hoc mode participate in an independent basic service set (IBSS) topology and do not communicate via an access point. All station transmissions and frame exchanges are peer-to-peer.



Figure: Client station configuration modes

Chapter - 21

radio Frequency (rF)

To properly design, deploy, and administer an 802.11 wireless network, in addition to understanding the OSI model and basic networking concepts, you must broaden your understanding of many other networking technologies. For instance, when administering an Ethernet network, you typically need a comprehension of TCP/IP, bridging, switching, and routing. The skills to manage an Ethernet network will also aid you as a Wi-Fi administrator because most 802.11 wireless networks act as “portals” into wired networks. The IEEE only defines the 802.11 technologies at the Physical layer and the MAC sub layer of the Data-Link layer. In order to fully understand the 802.11 technology, it is necessary to have a clear concept of how wireless works at the first layer of the OSI model, and at the heart of the Physical layer is radio frequency (RF) communications.

In a wired LAN, the signal is confined neatly inside the wire and the resulting behaviors are anticipated. However, just the opposite is true for a wireless LAN. Although the laws of physics apply, RF signals move through the air in a sometimes very unpredictable manner. Since RF signals are not saddled inside an Ethernet wire, you should always try to envision a wireless LAN as an “ever changing” network.

What Is an rF (radio Frequency) Signal

An RF signal starts out as an electrical *alternating current (AC)* signal that is originally generated by a transmitter. This AC signal is sent through a copper conductor (typically a coaxial cable) and radiated out of an antenna element in the form of an electromagnetic wireless signal. Changes of electron flow in an antenna, otherwise known as current, produce changes in the electromagnetic fields around the antenna. An alternating current is an electrical current with a magnitude and direction that varies cyclically, as opposed to direct current, the direction of which stays in a constant form. The shape and form of the AC signal—defined as the *waveform*—is what is known as a sine wave, as shown in Figure . Sine wave patterns can also be seen in light, sound, and the ocean.

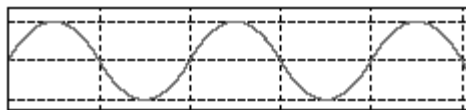


Figure: A sine wave

An RF signal radiates in a continuous pattern that is governed by certain properties such as wavelength, frequency, amplitude, phase, and polarity. Additionally, electromagnetic signals can travel through mediums of different materials or travel in a perfect vacuum. When an RF signal travels through a vacuum, it moves at the speed of light, which is approximately 300,000,000 meters per second, or 186,000 miles per second. RF signals travel using a variety or combination of movement behaviors. These movement behaviors are referred to as *propagation* behaviors. We will discuss some of these propagation

behaviors in this chapter, including absorption, reflection, scattering, refraction, diffraction, amplification, and attenuation.

Identifying radio Frequency Characteristics

In every RF signal exists characteristic that are defined by the laws of physics:

1. Polarity
2. Wavelength
3. Frequency
4. Amplitude
5. Phase

We will look at each of these in more detail in the following sections.

polarity

When the movement of the electron flow changes direction in an antenna, electromagnetic waves that change and move away from the antenna are also produced. The waves consist of two component fields: the electrical (E-field) and the H-field, which is magnetic. Think of a wave as a physical disturbance that transfers energy back and forth between these two fields. These fields are at right angles to each other, and the transfer of energy between these fields is known as *oscillation*. Polarization is the vertical or horizontal positioning of an antenna. The orientation of the antenna affects the *polarity* of the signal. The electric field always resides parallel in the same orientation (plane) of the antenna element. As shown in Figure the parallel plane is called the E-plane and the plane that is perpendicular to the antenna element is known as the H-plane.

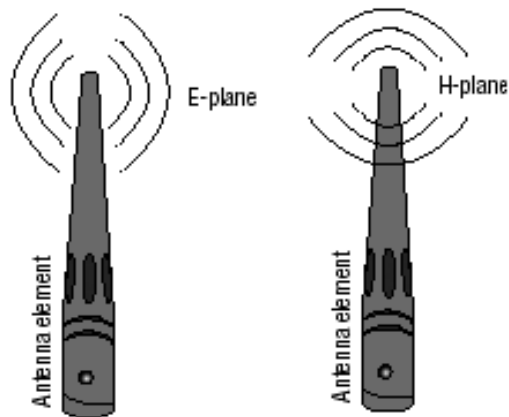


Figure: Polarity, E-plane, and H-plane

Wave polarity is defined as the position and direction of the electric field (E-field), as referenced to the surface of the earth. If an antenna element is positioned vertically, then the E-field is also vertical. Vertical polarization is when the E-field is perpendicular to

the earth. If an antenna element is positioned horizontally, then the electric field is also horizontal. Antenna element. Horizontal polarization is when the E-field is parallel to the earth. Antennas will often have polarity markings indicating which direction is vertical or horizontal.

Wavelength

As stated earlier, an RF signal is an alternating current (AC) that continuously changes between a positive and negative voltage. An oscillation, or cycle, of this alternating current is defined as a single change from up to down to up, or as a change from positive to negative to positive. A wavelength is the distance between the two successive crests (peaks) or two successive troughs (valleys) of a wave pattern. In simpler words, a wavelength is the distance that a single cycle of an RF signal actually travels. The Greek symbol λ (lambda) represents wavelength. It is very important to understand the following statement: The higher the frequency, the less distance the propagated wave will travel. AM radio stations operate at much lower frequencies than wireless LAN radios. For instance, WSB-AM in Atlanta broadcasts at 750 KHz and has a wavelength of 1,312 feet, or 400 meters. That is quite a distance for one single cycle of an RF signal to travel. In contrast, some radio navigation satellites operate at a very high frequency, near 252 GHz, and a single cycle of the satellite's signal has a wavelength of less than .05 inches, or 1.2 millimeters. Figure displays a comparison of these two extremely different types of RF signals. The majority of wireless LAN (WLAN) radio cards operate in either the 2.4 GHz frequency range or the 5 GHz range. In Figure you see a comparison of a single cycle of the two different frequency WLAN radio cards.

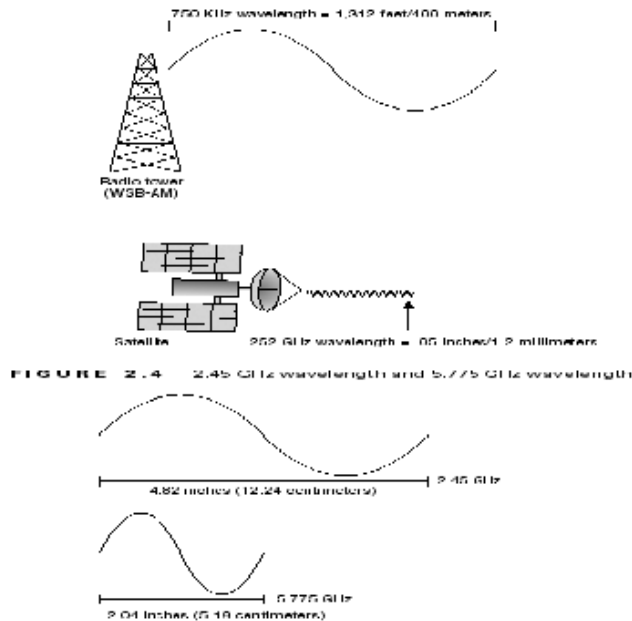


Figure: 750 KHz wavelength and 252 GHz wavelength

As you can see by these illustrations, the wavelengths of the different frequency signals are different because, although each signal only cycles one time, the waves travel dissimilar distances. In Figure you see the formulas for calculating wavelength distance in either inches or centimeters.

above figure: Wavelength formulas

Inches: wavelength = 11.811/frequency (GHz)

Centimeters: wavelength = 30/frequency (GHz)

Frequency

An RF signal cycles in an alternating current in the form of an electromagnetic wave. You also know that the distance traveled in one signal cycle is the wavelength. But what about how often an RF signal cycles. *Frequency* is the number of times a specified event occurs within a specified time interval. A standard measurement of frequency is hertz (Hz), which was named after the German physicist Heinrich Rudolf Hertz. An event that occurs once in 1 second is equal to 1 Hz. An event that occurs 325 times in 1 second is measured as 325 Hz. The frequency at which electromagnetic Wave's cycle is also measured in hertz. Thus, the number of times an RF signal cycles in 1 second is the frequency of that signal. Different metric prefixes can be applied to the hertz (Hz) measurement of radio frequencies:

1 hertz (Hz) = 1 cycle per second

1 kilohertz (KHz) = 1,000 cycles per second

1 megahertz (MHz) = 1,000,000 (million) cycles per second

1 gigahertz (GHz) = 1,000,000,000 (billion) cycles per second

So when we are talking about 2.4 GHz WLAN radio cards, the RF signal is oscillating 2.4 billion times per second!

amplitude

Another very important property of an RF signal is the amplitude, which simply can be characterized as the signal's strength or power. Amplitude can be defined as the maximum displacement of a continuous wave. With RF signals, the amplitude corresponds to the electrical field of the wave. When you look at an RF signal in an oscilloscope, the amplitude is represented by the positive crests and negative troughs of the sine wave. See that (λ) represents wavelength and (y) represents the amplitude. The first signal's crests and troughs have more magnitude, thus it has more amplitude. The second signal's crests and troughs have decreased, and therefore the signal has less amplitude. Note that although the signal strength (amplitude) is different, the frequency of the signal remains constant. A variety of factors can cause an RF signal to lose amplitude, otherwise known as attenuation, which we will discuss later in this chapter in the section "Loss (Attenuation)." Different types of RF technologies require varying degrees of transmit power. AM radio stations may transmit narrow band signals with as much power as 50,000 watts. The radio cards in most indoor 802.11 access points have a transmit power range between 1

milliwatt (mW) and 100 mW. You will learn later that Wi-Fi radio cards can actually receive signals with amplitudes as low as billionths of a milliwatt.

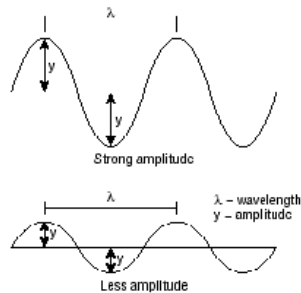


Figure: Amplitude

phase

Phase is not a property of just one RF signal but instead involves the relationship between two or more signals that share the same frequency. The phase involves the relationship between the position of the amplitude crests and troughs of two waveforms. Phase can be measured in distance, time, or degrees. If the peaks of two signals with the same frequency are in exact alignment at the same time, they are said to be *in phase*. Conversely, if the peaks of two signals with the same frequency are not in exact alignment at the same time, they are said to be *out of phase*. Figure illustrates this concept. What is important to understand is the effect that phase has on amplitude when radio cards receive multiple signals. Signals that have 0 (zero) degrees phase separation (in phase) actually combine their amplitude, which results in a received signal of much greater signal strength, or twice the amplitude. If two RF signals are 180 degrees out of phase (the peak of one signal is in exact alignment with the trough of the second signal), they cancel each other out and the effective received signal strength is null. Depending on the amount of phase separation of two signals, the received signal strength may be either cumulative or diminished.

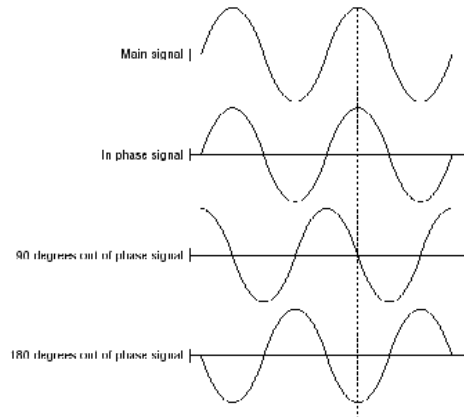


Figure: Phase

RF Components

Many components contribute to the successful transmission and reception of an RF signal. Following Figure shows the key components that will be covered in this section. In addition to understanding the function of the components, it is important to understand how the strength of the signal is specifically affected by each of the components.

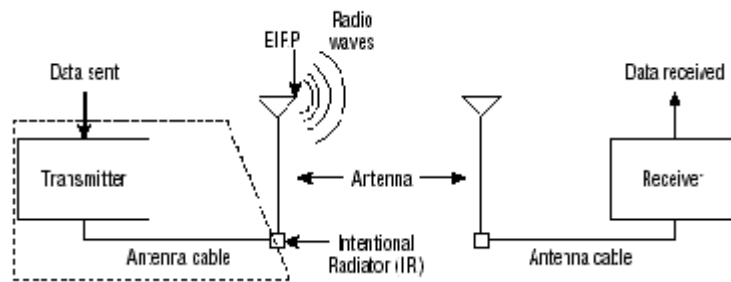


Figure: RF components

transmitter

The transmitter is the initial component in the creation of the wireless medium. The computer hands the data off to the transmitter, and it is the transmitter's job to begin the RF communication. When the transmitter receives the data, it will begin generating an alternating current (AC) signal. This AC signal determines the frequency of the transmission. For an 802.11, 802.11b, or 802.11g transmissions, the AC signal will oscillate around 2.4 billion times per second. For an 802.11a transmission, the AC signal will oscillate around 5 billion times per second. This oscillation determines the frequency of the radio wave. The transmitter will take the data provided and modify the AC signal using a modulation technique to encode the data into the signal. This modulated AC signal is now a carrier signal, containing the data to be transmitted. The carrier signal is then transported either directly to the antenna or through a cable to the antenna. In addition to generating a signal at a specific frequency, the transmitter is responsible for determining the amplitude, or what is more commonly referred to as the power level, of the signal. The higher the amplitude of the wave, the more powerful the wave is and the further it will travel. The power levels that the transmitter is allowed to generate are determined by the local regulatory body, such as the Federal Communications Commission (FCC) in the United States.

antenna

An antenna provides two functions in a communication system. When connected to the transmitter, it collects the AC signal that it receives from the transmitter and directs, or radiates, the RF waves away from the antenna in a pattern specific to the antenna type. When connected to the receiver, it takes the RF waves that it receives through the air and directs the AC signal to the receiver. The receiver converts the AC signal to bits and bytes. As you will see later in this chapter, the signal that is received is much less than the

signal that is generated. This signal loss is analogous to two people trying to talk to each other from opposite ends of a football field. Due to distance alone (free space), the yelling from one end of the field may be heard as barely louder than a whisper on the other end. The signal of an antenna is usually compared or referenced to an *isotropic radiator*. An isotropic radiator is a point source that radiates signal equally in all directions. The sun is probably one of the best examples of an isotropic radiator. It generates equal amounts of energy in all directions. Unfortunately, it is not possible to manufacture an antenna that is a perfect isotropic radiator. The structure of the antenna itself influences the output of the antenna; similar to the way the structure of a light bulb affects the bulb's ability to emit light equally in all directions. There are two ways to increase the power output from an antenna. The first is to generate more power at the transmitter, as stated in the previous section. The other is to direct, or focus, the RF signal that is radiating from the antenna. This is similar to how you can focus light from a flashlight. If you remove the lens from the flashlight, the bulb is typically not very bright and radiates in almost all directions. To make the light brighter, you could use more powerful batteries, or you could put the lens back on. The lens is not actually creating more light. It is focusing the light that was radiating in all different directions into a narrow area. Some antennas radiate waves as the bulb without the lens does, while some radiate focused waves as the flashlight with the lens does.

receiver

The receiver is the final component in the wireless medium. The receiver takes the carrier signal that is received from the antenna and translates the modulated signals into 1s and 0s. It then takes this data and passes it to the computer to be processed. The job of the receiver is not always an easy one. The signal that is received is a much less powerful signal than what was transmitted due to the distance it has traveled and the effects of free space path loss. The signal is also often altered due to interference from other RF sources and multipath.

Intentional radiator (Ir)

The FCC Code of Federal Regulations (CFR) Part 15 defines an *intentional radiator (IR)* as “a device that intentionally generates and emits radio frequency energy by radiation or induction.” Basically, it's something that is specifically designed to generate RF as opposed to something that generates RF as a byproduct of its main function, such as a motor that incidentally generates RF noise. Regulatory bodies such as the FCC limit the amount of power that is allowed to be generated by an IR. The IR consists of all the components from the transmitter to the antenna but not including the antenna, as seen in Figure 3.1. The power output of the IR is thus the sum of all the components from the transmitter to the antenna, again not including the antenna. The components making up the IR include the transmitter, all cables and connectors, and any other equipment (grounding, lightning arrestors, amplifiers, attenuators, etc.) between the transmitter and the antenna. The power of the IR is measured at the connector that provides the input to the antenna. Since this is the point where the IR is measured and regulated, we often refer to this point alone as the IR. Using the flashlight analogy, the IR is all of the components

up to the light bulb socket but not the bulb and lens. This is the raw power, or signal, that is provided, and now the bulb and lens can focus the signal.

equivalent Isotropically radiated power (eirp)

Equivalent Isotropically radiated power (EIRP) is the highest RF signal strength that is transmitted from a particular antenna. To understand this better, think of our flashlight example for a moment. Let's assume that the bulb without the lens generates 1 watt of power. When you put the lens on the flashlight, it focuses that 1 watt of light. If you were to look at the light now, it would appear much brighter. If you were to measure the brightest point of the light that was being generated by the flashlight, due to the effects of the lens, it may be equal to the brightness of an 8 watt bulb. So by focusing the light, you are able to make the equivalent isotropically radiated power of the focused bulb equal to 8 watts. As you learned, antennas are capable of focusing or directing RF energy. This focusing capability can make the effective output of the antenna much greater than the signal entering the antenna. Because of this ability to amplify the output of the RF signal, regulatory bodies such as the FCC limit the amount of EIRP from an antenna. In the next section of this chapter you will learn how to calculate how much power is actually being provided to the antenna (IR) and how much power is coming out of the antenna (EIRP).

Units of power and Comparison

When an 802.11 wireless network is designed, two key components are coverage and performance. A good understanding of RF power, comparison, and RF mathematics can be very helpful during the network design phase. In this section, we will introduce you to an assortment of units of power and units of comparison. It is important to know and understand the different types of units of measurement and how they relate to each other. Some of the numbers that you will be working with will represent actual units of power and others will represent relative units of comparison. Actual units are ones that represent a known or set value. To say that a man is 6 feet tall is an example of an actual measurement. Since the man's height is a known value, in this case feet, you know exactly how tall he is. Relative units are comparative values comparing one item to a similar type of item. For example, if you wanted to tell someone how tall the man's wife is using comparative units of measurement, you could say that she is $\frac{5}{6}$ his height. You now have a comparative measurement: if you know the actual height of either one, you can then determine how tall the other is. Comparative units of measurement are useful when working with units of power. As you will see later in this chapter, we can use these comparative units of power to compare the area that one access point can cover versus another access point. Using simple mathematics, we can determine things such as how many watts are needed to double the distance of a signal from an access point. Following Table below categorizes the different units.

Table: Units of Measure

Units of Power	Units of Comparison
Watt (W)	Decibel (dB)
Milliwatt (mW)	dBi
dBm	dBd

active and passive Gain

You can increase the signal that is radiated out of the antenna (EIRP) by increasing the output of the transmitter, which in turn increases the amount of power provided to the antenna (Intentional Radiator) and thus the amount of power from the antenna (EIRP). When the power is increased by some type of electrical device, such as the transmitter or, an amplifier, the increase is referred to as active gain. Another method of increasing power that you also learned about in the previous chapter is to direct or focus the power. When power is focused, the amount provided to the antenna does not change. It is the antenna acting like a lens on a flashlight that increases the power output by concentrating the RF signal in a specific direction. Since the gain from the antenna was created by shaping or concentrating the signal, and not by increasing the overall power, this increase is referred to as *passive gain* (Passive gain is caused by focusing the existing power, while active gain is Caused by adding more power.)

antenna types

There are three main categories of antennas:

Omni-directional

Omni-directional antennas radiate RF in a fashion similar to the way a table or floor lamp radiates light. They are designed to provide general coverage in all directions.

FIGURE 4.4 Half-wave dipole antenna

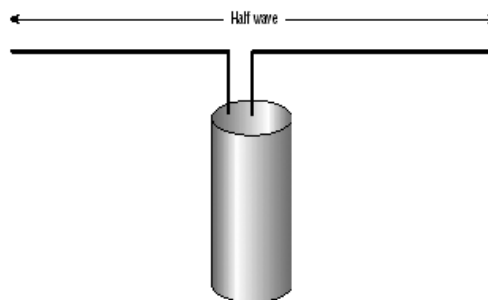
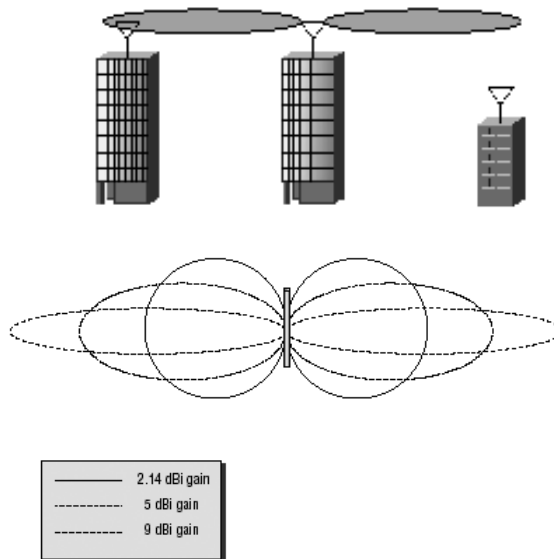


Figure: Vertical radiation patterns of omni-directional antennas

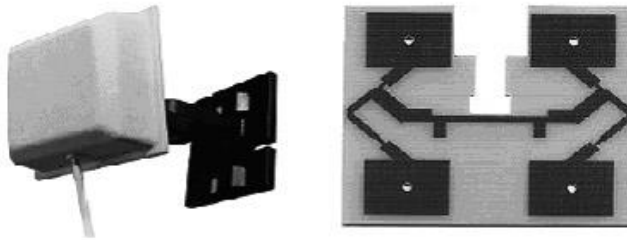
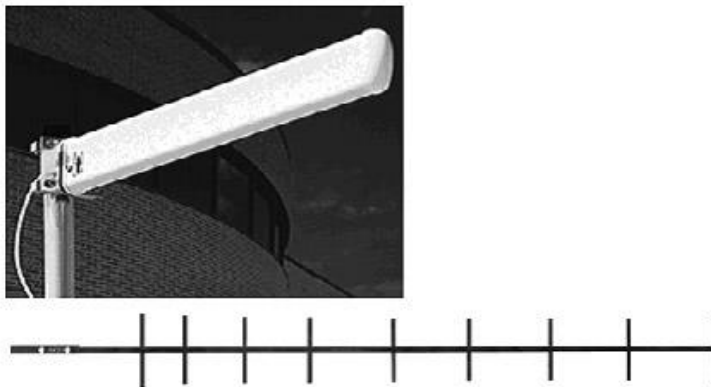
FIGURE 4.5 Improperly installed omni-directional antennas



Semi-directional

Semi-directional antennas radiate RF in a fashion similar to the way a wall sconce is designed to radiate light away from the wall or the way a street lamp is designed to shine light down on a street or a parking lot, providing a directional light across a large area. It is common to use semi-directional antennas to provide a network bridge between two buildings in a campus environment or down the street from each other. Longer distances would be served by highly-directional antennas. There are three types of antennas that fit into the semi-directional category:

- *Patch*
- *Panel*
- *Yagi* (pronounced “YAH-gee”)

FIGURE The exterior of a patch antenna and the internal antenna element**FIGURE** The exterior of a yagi antenna and the internal antenna element

highly-directional

Highly-directional antennas radiate RF in a fashion similar to the way a spotlight is designed to focus light on a flag or a sign. Each type of antenna is designed with a different objective in mind. Highly-directional antennas are strictly used for point-to-point communications, typically to provide network bridging between two buildings. They provide the most focused, narrow beam width of any of the antenna types. There are two types of highly-directional antennas: parabolic dish and grid antennas. The parabolic dish antenna is similar in appearance to the small digital satellite TV antennas that can be seen on the roofs of many houses. The grid antenna resembles the rectangular grill of a barbecue, with the edges slightly curved inward. The spacing of the wires on a grid antenna is determined by the wavelength of the frequencies that the antenna is designed for. Because of the high gain of highly-directional antennas, they are ideal for long-distance communications as far as 35 miles (58 km). Due to the long distances and narrow beam width, highly-directional antennas are affected more by antenna wind loading, which is antenna movement or shifting caused by wind. Even slight movement of a highly-directional antenna can cause the RF beam to be aimed away from the receiving antenna, interrupting the communications. In high-wind environments, grid antennas, due to the spacing between the wires, are less susceptible to wind load and may be a better choice. Another option in high-wind environments is to choose an antenna with a wider

beam width. In this situation, if the antenna were to shift slightly, due to its wider coverage area, the signal would still be received. No matter which type of antenna is installed, the quality of the mount and antenna will have a huge effect in reducing wind load.

phased array

A *phased array antenna* is actually an antenna system and is made up of multiple antennas that are connected to a signal processor. The processor feeds the individual antennas with signals of different relative phases, creating a directed beam of RF signal aimed at the client device. Because it is capable of creating narrow beams, it is also able to transmit multiple beams to multiple users simultaneously. Phased array antennas do not behave like other antennas since they can transmit multiple signals at the same time. Because of this unique capability, they are often regulated differently by the local RF regulatory agency. Phased array antennas are extremely specialized, expensive, and not commonly used in the 802.11 market. In fact, the leading manufacturer of 802.11 phase array antenna systems recently went out of business. It is an interesting and very capable technology; however, time will tell whether it has a future in the 802.11 market.

Sector antennas

Sector antennas are a special type of high-gain, semi-directional antennas that provide a pie shaped coverage pattern. These antennas are typically installed in the middle of the area where RF coverage is desired and placed back to back with other sector antennas. Individually, each antenna services its own piece of the pie, but as a group, all of the pie pieces fit together and provide omni-directional coverage for the entire area. Unlike other semi-directional antennas, a sector antenna generates very little RF signal behind the antenna (*back lobe*) and therefore does not interfere with the other sector antennas that it is working with. The horizontal beam width of a sector antenna is from 60 to 180 degrees, with a narrow vertical beam width of from 7 to 17 degrees. Sector antennas typically have a gain of at least 10 dBi. Installing a group of sector antennas to provide omni-directional coverage for an area provides many benefits over installing a single omni-directional antenna. To begin with, sector antennas can be mounted high over the terrain and tilted slightly downward, with the tilt of each antenna at an angle appropriate for the terrain it is covering. Omni-directional antennas can also be mounted high over the terrain; however, if an omni-directional antenna is tilted downward on one side, the other side will be tilted upward. Since each antenna covers a separate area, each antenna can be connected to a separate transceiver and can transmit and receive independently of the other antennas. This would provide the capability for all of the antennas to be transmitting at the same time, providing much greater throughput. A single omni-directional antenna would be capable of transmitting to only one device at a time. The last benefit of the sector antennas over a single omni-directional antenna is that the gain of the sector antennas is much greater than the gain of the omni-directional antenna, providing a much larger coverage area. Sector antennas are used extensively for cellular telephone communications and are starting to be used for 802.11 networking.

Selecting the proper location of installing the rF antenna:**antenna Mounting**

As was stated earlier in this chapter, proper installation of the antenna is one of the most important tasks to ensure an optimally functioning network. The following are key areas to be concerned with when installing antennas:

1. Placement
2. Mounting
3. Appropriate use
4. Orientation
5. Alignment
6. Safety
7. Maintenance

placement

The proper placement of an antenna is dependent upon the type of antenna. When installing omni-directional antennas, it is important to place the antenna at the center of the area where you want coverage. Remember that lower-gain omni-directional antennas provide broader vertical coverage while higher-gain omni-directional antennas provide a wider but much flatter coverage. Be careful not to place high-gain omni-directional antennas too high above the ground because the narrow vertical coverage may cause the antenna to provide insufficient signal to clients located on the ground. When installing directional antennas, make sure that you know both the horizontal and vertical beam widths so that you can properly aim the antennas. Also make sure that you are aware of the amount of gain that the antenna is adding to the transmission. If the signal is too strong, it will overshoot the area that you are looking to provide coverage to. This is a security risk, and you should decrease the amount of power that the transceiver is generating to reduce the coverage area. Not only is it a security risk, overshooting your coverage area is considered rude. If you are installing an outdoor directional antenna, in addition to concerns regarding the horizontal and vertical beam widths, make sure that you have correctly calculated the Fresnel zone and mounted the antenna accordingly.

Mounting

After deciding where to place the antenna, the next step is to decide how to mount it. Many antennas, especially outdoor antennas, are mounted on masts or towers. It is common to use mounting clamps and U-bolts to attach the antennas to the masts. For mounting directional antennas, specially designed tilt-and-swivel mounting kits are available to make it easier to aim and secure the antenna. If the antenna is being installed in a windy location (what roof top or tower isn't windy), make sure that you take into consideration wind load and that you properly secure the antenna. There are numerous ways of mounting antennas indoors. Two common concerns are aesthetics and security. Many

organizations, particularly ones that provide hospitality-oriented services such as hotels and hospitals, are concerned about the aesthetics of the installation of the antennas. Specialty enclosures and ceiling tiles can help to hide the installation of the access points and antennas. Other organizations, particularly schools and public environments, are concerned with securing the access points and antennas from theft or vandalism. An access point can be locked in a secure enclosure, with a short cable connecting it to the antenna. There are even ceiling tiles with antennas built into them, invisible to anyone walking by. If security is a concern, mounting the antenna high on the wall or ceiling can also minimize unauthorized access.

appropriate Use

Make sure that indoor antennas are not used for outdoor communications. Outdoor antennas are specifically built to withstand a wide range of temperatures that they may be exposed to. Outdoor antennas are also built to stand up to other elements, such as rain, snow, and fog. In addition to installing the proper antenna, make sure that the mounts that you use are designed for the environment in which you are installing them.

alignment

Before installing an antenna, make sure you read the manufacturer's recommendations for mounting it. This suggestion is particularly important when installing directional antennas. Since directional antennas may have different horizontal and vertical beamwidths, and since directional antennas can be installed with different polarization, proper alignment can make the difference between being able to communicate and not. The first step is to make sure you have decided on a polarization. Next, decide on the mounting technique and ensure that it is compatible with the mounting location. Then the antennas can be aligned. Once that occurs, the cables and connectors can be either proofed and secured from movement.

Safety

We can't emphasize enough the importance of being careful when installing antennas. Most of the time, the installation of an antenna involves climbing ladders, towers, or rooftops. Gravity and wind have a way of making an installation difficult for both the climber and the people below helping. Plan the installation before you begin, making sure you have all of the tools and equipment that you will need to install the antenna. Unplanned stoppages of the installation and relaying forgotten equipment up and down the ladder add to the risk of injury. Be careful when working with your antenna or near other antennas. Highly-directional antennas are focusing high concentrations of RF energy. This large amount of energy can be dangerous to your health. Do not power on your antenna while you are working on it, and do not stand in front of other antennas that are near where you are installing your antenna. When installing antennas (or any device) on ceilings, rafters, or masts, make sure they are properly secured. Even a 1-pound antenna can be deadly if it falls from the rafters of a warehouse. If you will be installing antennas as part of your job, we recommend that you take an RF health and safety course. These courses will teach you the FCC and the U.S. Department of Labor Occupational Safety and Health

Administration (OSHA) regulations and how to be safe and compliant with the standards. If you need an antenna installed on any elevated structure, such as a pole, tower, or even a roof, consider hiring a professional installer. Professional climbers and installers are trained and in some places certified to perform these types of installations. In addition to the training, they have the necessary safety equipment and proper insurance for the job. If you are planning to install wireless equipment as a profession, you should develop a safety policy that is blessed by your local occupational safety representative. You should also receive certified training on climbing safety in addition to RF safety training. First aid and CPR training is also highly recommended.

Maintenance

There are two types of maintenance: preventative and diagnostic. When installing an antenna, it is important to prevent problems from occurring in the future. This seems like simple advice, but since antennas are often difficult to get to after they have been installed, it is especially prudent advice. Two key problems that can be minimized with proper preventative measures are wind damage and water damage. When installing the antenna, make sure all of the nuts, bolts, screws, and so on are tightened. Also make sure all of the cables are properly secured so that they are not thrashed about in the wind.

To help prevent water damage, cold shrink tubing or coaxial sealant can be used to minimize the risk of water getting into the cable or connectors. Heat shrink tubing should not be used because the cable can be damaged by the heat that is necessary to shrink the wrapping. Silicone should also not be used as air bubbles can form under the silicone and moisture can collect. Another cabling technique is the drip loop. A drip loop prevents water from flowing down the cable and onto a connector or into the hole where a cable exits the building. Any water that is flowing down the cable will continue to the bottom of the loop and then drip off. Antennas are typically installed and forgotten about until they break. It is advisable to periodically perform a visual inspection of the antenna. If the antenna is not easily accessible, a pair of binoculars or a camera with a very high zoom lens can make this a simple task.

Chapter - 22

IEEE 802.11 Standards

“Overview of Wireless Standards and Organizations,” the Institute of Electrical and Electronics Engineers (IEEE) is the professional society that creates and maintains standards that we use for communications, such as the 802.3 Ethernet standards for wired networking. The IEEE has assigned working groups for several wireless communication standards. For example, the 802.15 working group is responsible for personal area network (PAN) communications using radio frequencies. Some of the technologies defined within the 802.15 standard include Bluetooth and ZigBee. Another example is the 802.16 standard, which is overseen by the Broadband Wireless Access Working Group; the technology is often referred to as Wi-MAX. The focus of this book is the technology as defined by the IEEE 802.11 standard, which provides for local area network (LAN) communications using radio frequencies (RF). The 802.11 Working Group comprises 250+ wireless companies and has over 650 active members. It consists of standing committees, study groups, and numerous *task groups*

Overview of the IEEE 802.11 Standard

The original 802.11 standard was published in June 1997 as IEEE Std. 802.11-1997, and it is often referred to as 802.11 Prime because it was the first WLAN standard. The standard was revised in 1999, reaffirmed in 2003, and published as IEEE Std. 802.11-1999 (R2003). The IEEE specifically defines 802.11 technologies at the Physical layer and the MAC sub layer of the Data-Link layer. By design, the 802.11 standard does not address the upper layers of the OSI model, although there are interactions between the 802.11 MAC layer and the upper layers for parameters such as quality of service (QoS). The PHY Task Group (PHY) worked in conjunction with the MAC Task Group (MAC) to define the original 802.11 standard. The PHY Task Group (PHY) developed three Physical layer specifications:

Infrared (Ir)

Infrared technology uses a light-based medium. Although an infrared medium was indeed defined in the original 802.11 standard, the implementation is obsolete.

Frequency hopping Spread Spectrum (FhSS)

Radio frequency signals can be defined as narrowband signals or as spread spectrum signals. An RF signal is considered spread spectrum when the bandwidth is wider than what is required to carry the data. Frequency Hopping is a spread spectrum technology that was first patented during World War II. Frequency Hopping 802.11 radio cards are often called clause 14 devices due to the clause that referenced them in the original 802.11 standard.

Direct sequence spread spectrum (DSSS)

Direct sequence is another spread spectrum technology that is frequently used and easiest to implement. DSSS 802.11 radio cards are often known as clause 15 devices. As defined by 802.11 Prime, the frequency space in which either FHSS or DSSS radio cards can transmit is the license free 2.4 GHz *Industrial, Scientific, and Medical (ISM)* band. DSSS 802.11 radio cards can transmit in channels subdivided from the entire 2.4 to 2.4835 GHz ISM band. The IEEE is more restrictive for FHSS radio cards, which are permitted to transmit on 1 MHz sub carriers in the 2.402 to 2.480 GHz range of the 2.4 GHz ISM band. Chances are that you will not be working with older legacy 802.11 equipment since most WLAN deployments use technologies as defined by newer 802.11 amendments. WLAN companies had the choice of manufacturing either clause 14 FHSS radio cards or clause 15 DSSS radio cards. Because spread spectrum technologies differ, they cannot communicate with each other and often have a hard time coexisting. Spread spectrum signals are analogous to oil and water because they do not mix well. Therefore, it is important to understand that an 802.11 DSSS radio cannot communicate with an 802.11 FHSS radio. The majority of legacy WLAN deployments used frequency hopping, but some DSSS solutions were available as well. *Data rates* defined by the original 802.11 standard were 1 Mbps and 2 Mbps. Keep in mind that a data rate is the available bandwidth and not actual throughput. Due to medium access methods, aggregate throughput is typically 1/2 or less of the available data rate bandwidth.

802.11 Frame Format vs. 802.3

Frame Format

All of the IEEE 802 frame formats share similar characteristics, and the 802.11 frame is no exception. Since the frames are similar, it makes it easier to translate the frames as they move from the 802.11 wireless networks to the 802.3 wired networks and vice versa.

One of the differences between 802.3 Ethernet and 802.11 wireless frames is the frame size. Unlike 802.3, which will typically transport frames of up to 1,518 bytes, 802.11 is capable of transporting frames of up to 2,304 bytes of “upper layer” data. This means that as the data moves between the wireless and the wired network, the access point may receive a data frame that is too large for the wired network. This is rarely a problem thanks to TCP/IP. Since most networks use TCP/IP, and since TCP/IP typically has an IP maximum transmission unit (MTU) size of 1,500 bytes, these IP packets can be handled by both 802.11 and 802.3 frames. Another difference between 802.3 and 802.11 frames is the MAC addressing fields. 802.3 frames have two MAC address fields, whereas 802.11 frames have four address fields. These four address fields will contain either three or four MAC addresses. The contents of these four fields can include the following MAC addresses: receiver address (RA), transmitter address (TA), basic service set identifier (BSSID), destination address (DA), and source address (SA). Even though the number of address fields is different, both 802.3 and 802.11 use the same MAC address format. The first three octets are known as the Organizationally Unique Identifier (OUI) and the last three octets are known as the extension identifier.

CSMa/Ca vs. CSMa/CD

Network communication requires a set of rules to provide controlled and efficient access to the network medium. *Media access control (MAC)* is the generic term used when discussing the different methods of access. There are many ways of providing media access. The early mainframes used polling, which sequentially checked each terminal to see if there was data to be processed. Later, token-passing and contention methods were used to provide access to the media. Two forms of contention that are heavily used in today's networks are *Carrier Sense Multiple Access with Collision Detection (CSMA/CD)*

And *Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)*. CSMA/CD is well known and is used by Ethernet networks. CSMA/CA is not as well known and is used by 802.11 networks. Stations using either access method must first listen to see if any other device is transmitting. If another device is transmitting, then the station must wait until the medium is available. The difference between CSMA/CD and CSMA/CA exists when a client wants to transmit and no other clients are presently transmitting. A CSMA/CD node can immediately begin transmitting. If a collision occurs while a CSMA/CD node is transmitting, the collision will be detected and the node will temporarily stop transmitting. 802.11 wireless stations are not capable of transmitting and receiving at the same time, so therefore they are not capable of detecting a collision during their transmission. For this reason, 802.11 wireless networking uses CSMA/CA instead of CSMA/CD to try to avoid collisions.

Chapter - 23

802.11 Network Security architecture

Introduction

When you're securing a wireless 802.11 network, three major components are normally Required strong encryption Mutual authentication Segmentation because data is transmitted freely and openly in the air, proper protection is needed to ensure data privacy, so strong encryption is needed. The function of most wireless networks is to provide a portal into some other network infrastructure, such as an 802.3 Ethernet backbone. The wireless portal must be protected and therefore an authentication solution is needed to ensure that only authorized users may pass through the portal via a wireless access point. The wireless network should always be treated as untrusted and should also be segmented in some fashion from the wired infrastructure.

encryption

802.11 wireless networks operate in license-free frequency bands and all data transmissions travel in the open air. Protecting data privacy in a wired network is much easier because physical access to the wired medium is more restricted. However, physical access to wireless transmissions is available to anyone in listening range. Therefore, using cipher encryption technologies to obscure information is mandatory. A cipher is an algorithm used to perform encryption. The two most common algorithms used to protect data are the RC4 algorithm (RC stands for Ron's Code or Rivest's Cipher) and the Advanced Encryption Standard (AES) algorithm. Some ciphers encrypt data in a continuous stream while others encrypt data in blocks. The RC4 algorithm is a streaming cipher used in technologies that are often used to protect Internet traffic, such as Secure Sockets Layer (SSL). The RC4 algorithm is used to protect 802.11 wireless data and is incorporated into two encryption methods known as WEP and TKIP. The AES algorithm, originally named the Rijndael algorithm, is a block cipher that offers much stronger protection than the RC4 streaming cipher. AES is used to encrypt 802.11 wireless data using an encryption method known as Counter mode with Cipher Block Chaining–Message Authentication Code (CCMP), which will also be discussed later in this chapter. The AES algorithm encrypts data in fixed data blocks with choices in encryption key strength of 128, 192, or 256 bits. The AES cipher is the mandated algorithm of the United States government for protecting both sensitive and classified information.

aaa

AAA is a computer security concept that refers to authentication, authorization, and accounting. Authentication is the verification of user identity and credentials. Users must identify themselves and present credentials such as usernames and passwords or digital certificates. More secure authentication systems exist that require multifactor authentication, where at least two sets of different credentials must be presented. Authorization involves granting access to network resources and services. Before

authorization to network resources can be granted, proper authentication must occur. Accounting is tracking the use of network resources by users. It is an important aspect of network security, used to keep a paper trail of who used what resource and when and where. A record is kept of user identity, which resource was accessed, and at what time. Keeping an accounting trail is often a requirement of many industry regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Segmentation

While it is of the utmost importance to secure an enterprise wireless network utilizing both strong encryption and an AAA solution, an equally important aspect of wireless security is segmentation. Prior to the introduction of stronger authentication and encryption techniques, wireless was viewed as an untrusted network segment. Therefore, before the ratification of the 802.11i security amendment, the wireless segment of a network was always treated as the untrusted segment while the wired 802.3 network was considered the trusted segment. However, if the proper encryption and authentication solutions are deployed, the wireless network can be just as secure if not more so than the wired segments of a network. It is still important to segment users in proper groups, much like what is done on any traditional network. Once authorized onto network resources, users can be further restricted as to what resources may be accessed and where they can go. Segmentation can be achieved through a variety of means, including firewalls, routers, VPNs, and VLANs. The most common wireless segmentation strategy often used in 802.11 enterprise WLANs is layer 3 segmentation using Virtual LANs (VLANs).

Legacy 802.11 Security

The original 802.11 standard defined very little in terms of security. The authentication methods first outlined in 1997 basically provided an open door into the network infrastructure. The encryption method defined in the original 802.11 standard has long been cracked and is considered inadequate for data privacy. In the following sections, you will learn about the legacy authentication and encryption methods that were the only defined standards for 802.11 wireless securities from 1997 until 2004.

Legacy authentication

The original 802.11 standard specifies two different methods of authentication: Open System authentication and Shared Key authentication. Open System authentication provides authentication without performing any type of client verification. It is essentially a two-way exchange between the client and the access point. The client sends an authentication request and the access point then sends an authentication response. Because Open System authentication does not require the use of any credentials, every client gets authenticated and therefore authorized onto network resources once they have been associated. Static WEP encryption is optional with Open System authentication but may be used to encrypt the data frames after Open System authentication and association occur.

Static Wep encryption

Wired Equivalent Privacy (WEP) is a layer 2 encryption method that uses the RC4 streaming cipher. The original 802.11 standard defined 64-bit WEP as the default encryption method. The three main intended goals of WEP encryption include confidentiality, access control, and data integrity. The primary goal of confidentiality was to provide data privacy by encrypting the data before transmission. WEP also provides access control, which is basically a crude form of authorization. Client stations that do not have the same matching static key as an access point are refused access to network resources. A data integrity checksum known as the Integrity Check Value (ICV) is computed on data before encryption and used to prevent data from being modified.

MaC Filters

Every network card has a physical address known as a MAC address. This address is a 12-digit hexadecimal number. 802.11 client stations each have unique MAC addresses, and as you have already learned, 802.11 access points use MAC addresses to direct frame traffic. Most vendors provide MAC filtering capabilities on their access points. MAC filters can be configured to either allow or deny traffic from specific MAC addresses.

Most MAC filters apply restrictions that will allow traffic only from specific client stations to pass through based on their unique MAC addresses. Any other client stations whose MAC addresses are not on the allowed list will not be able to pass traffic through the virtual port of the access point and onto the distribution system medium. It should be noted that MAC addresses can be “spoofed,” or impersonated, and any amateur hacker can easily bypass any MAC filter by spoofing an allowed client station’s address. Because of spoofing and because of all the administrative work that is involved with setting up MAC filters, MAC filtering is not considered a reliable means of security for wireless enterprise networks.

SSID Cloaking

Remember in *Star Trek* when the Klingons “cloaked” their spaceship but somehow Captain Kirk always found the ship anyway? Well there is a way to “cloak” your service set identifier (SSID). Access points typically have a setting called Closed Network or Broadcast SSID. By either enabling a closed network or disabling the broadcast SSID feature, you can hide, or cloak, your wireless network name. When you implement a closed network, the SSID field in the beacon frame is null (empty), and therefore passive scanning will not reveal the SSID to client stations that are listening to beacons. Many wireless client software utilities transmit probe requests with null SSID fields when actively scanning for access points. Additionally, there is a very popular and freely available software program called NetStumbler that is used by individuals to discover wireless networks.

Shared Key authentication

Shared Key authentication uses WEP to authenticate client stations and requires that a static WEP key be configured on both the station and the access point. In addition to WEP being mandatory, authentication will not work if the static WEP keys do not match. The authentication process is similar to Open System authentication but includes a challenge

and response between the AP and client station. Shared Key authentication occurs with an exchange of eight frames between the station and the access point, as described in the following list and seen in Figure shows a packet capture of the eight frames that are exchanged between the client and the access point:

1. In the first step, the client station sends an authentication frame to the access point. The Frame indicates that Shared Key authentication is being used. (Frame 245)
2. The access point then replies to the station with an ACK. (frame 246)
3. Inside the body of a second authentication frame, the access point now sends a challenge of 128 octets of clear text to the client station. (Frame 247)
4. The station then replies to the access point with an ACK. (frame 248)
5. The client station encrypts the challenge text using the station's static WEP key and sends it back to the access point inside the body of a third authentication frame (frame 249)
6. The access point then replies to the station with an ACK. (frame 250)
7. The access point decrypts the station's response and compares it to the challenge text. If they match, the access point will respond by sending a fourth and final authentication frame to the station confirming the success. If they don't match, the access point will respond negatively. (Frame 251)
8. The client then replies to the access point with an ACK. (frame 252)

The image shows a Wireshark packet capture window titled 'CompuShare for WiFi - Evaluation Version - Realtime Wireless Network Adaptor'. The main pane displays a list of captured packets with the following details:

No.	Protocol	MAC Addresses	Time	Size
245	MNGT/MUTH	00:40:96:A6:D4:23 => 00:40:96:36:FC:68	13:26:25.396656	30
246	CTRL/ACK	N/A => 00:40:96:A6:D4:23	13:26:25.396645	10
247	MNGT/MUTH	00:40:96:36:FC:68 => 00:40:96:A6:D4:23	13:26:25.411744	100
248	CTRL/ACK	N/A => 00:40:96:36:FC:68	13:26:25.411734	10
249	MNGT/MUTH	00:40:96:A6:D4:23 => 00:40:96:36:FC:68	13:26:25.413924	160
250	CTRL/ACK	N/A => 00:40:96:A6:D4:23	13:26:25.414206	10
251	MNGT/MUTH	00:40:96:36:FC:68 => 00:40:96:A6:D4:23	13:26:25.420156	30
252	CTRL/ACK	N/A => 00:40:96:36:FC:68	13:26:25.422267	10

The packet details pane for frame 247 shows the following structure:

- Frame 247: MNGT/MUTH (100 bytes)
 - Frame 247: CTRL/ACK (10 bytes)
 - Frame 247: MNGT/MUTH (100 bytes)

The packet bytes pane shows the raw data for frame 247, which is a management frame containing a challenge of 128 octets of clear text.

Figure: Shared Key authentication

Shared Key authentication is actually less secure than Open System authentication. With Shared Key authentication, WEP is required, and after the authentication process is completed, any simple data frames that are transmitted are encrypted using the static WEP key. With Open System authentication, WEP is not used for the authentication process, but WEP can be used to encrypt any data frames that are transmitted. So when using either method, the data is able to be encrypted and transmitted using the same process. The security problem is in the Shared Key authentication process. During Shared Key authentication, the access point sends 128 octets of clear text to the client. The client station then encrypts this clear text and sends it back to the access point.

Anyone who is eavesdropping or analyzing the packets can capture this information and now not only knows the encrypted data, but also the text version of what was encrypted. Once the challenge and response are captured, it may be easier to figure out the static encryption key. If the static WEP key is compromised, then all the data frames can be decrypted by a potential attacker. While Shared Key authentication may be a slightly stronger authentication method than Open System authentication, the potential of exposing the WEP key is a greater security risk with Shared Key authentication. Neither legacy authentication method is considered strong enough for enterprise security.

Wireless attacks

As you have learned throughout this book, the main function of 802.11 access points is to provide a portal into a wired network infrastructure. The portal must be protected with strong authentication methods so that only legitimate users with the proper credentials will be authorized to have access to network resources. If the portal is not properly protected, unauthorized users can also gain access to these resources. The potential risks of exposing these resources are endless. An intruder could gain access to financial databases, corporate trade secrets, or personal health information. Network resources can also be damaged. What would be the financial cost to an organization if an intruder used the wireless network as a portal to disrupt or shut down a SQL server or email server? If the Wi-Fi portal is not protected, any individual wishing to cause harm could upload data such as viruses, Trojan horse applications, keystroke loggers, or remote control applications. Spammers have already figured out that they can use open wireless gateways to the Internet to commence spamming activities. Other illegal activities, such as software theft and remote hacking, may also occur through an unsecured gateway.

While an intruder can use the wireless network to attack wired resources, equally at risk are all of the wireless network resources. Any information that passes through the air can be captured and possibly compromised. If not properly secured, the management interfaces of Wi-Fi equipment can be accessed. Many wireless users are fully exposed for peer-to-peer attacks. Finally, the possibility of denial of service attacks against a wireless network always exists. With the proper tools, any individual with ill intent can temporarily disable a Wi-Fi network, thus denying legitimate users access to the network resources. In the following sections you will learn about all the potential attacks that can be launched against 802.11 wireless networks.

peer-to-peer attacks

Wireless resources may also be attacked. A commonly overlooked risk is the *peer-to-peer* attack. As you have learned in earlier chapters, an 802.11 client station can be configured in either Infrastructure mode or Ad-Hoc mode. When configured in Ad-Hoc mode, the wireless network is known as an independent basic service set (IBSS) and all communications are peer-to-peer without the need for an access point. Because an IBSS is by nature a peer-to-peer connection, any user who can connect wirelessly with another user can potentially gain access to any resource available on either laptop. A common use of ad-hoc networks is to share files on the-fly. If shared access is provided, files and other assets can accidentally be exposed. A personal firewall is often used to

mitigate peer-to-peer attacks. Users that are associated to the same access point are typically just as vulnerable to peer-to-peer attacks as IBSS users. Properly securing your wireless network often involves protecting authorized users from each other since hacking at companies is often performed internally by employees. Users associated to the same access point are members of the same basic service set (BSS). Because they reside in the same wireless domain, the users are exposed to peer-to-peer attacks. In most WLAN deployments, Wi-Fi clients communicate only with devices on the wired network such as email or web servers and peer-to-peer communications are not needed. Therefore, most vendors provide some proprietary method of preventing users from inadvertently sharing files with other users.

eavesdropping

As you have learned throughout this book, 802.11 wireless networks operate in license-free frequency bands and all data transmissions travel in the open air. Access to wireless transmissions is available to anyone within listening range, and therefore strong encryption is mandatory. Wireless communications can be monitored via two eavesdropping methods: casual eavesdropping and malicious eavesdropping.

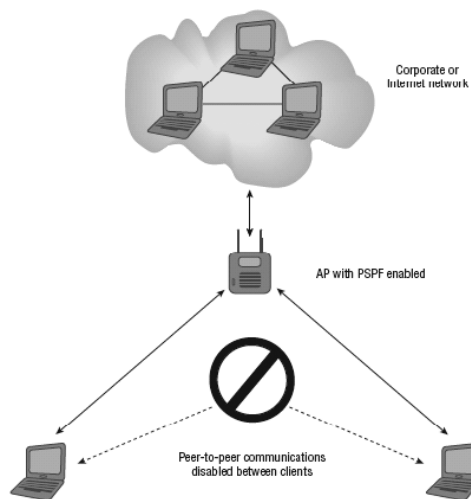


Figure: Public Secure Packet Forwarding

Casual eavesdropping is typically considered harmless and is also often referred to as War driving. Software utilities known as WLAN discovery tools exist for the purpose of finding open WLAN networks. Wardriving is strictly the act of looking for wireless networks, usually while in a moving vehicle. The most common wardriving software tool is a freeware program called NetStumbler.

encryption Cracking

You learned that Wired Equivalent Privacy (WEP) encryption has been cracked. The current WEP cracking tools that are freely available on the Internet can crack WEP encryption in

as little as 5 minutes. There are several methods used to crack WEP encryption. However, an attacker usually needs only to capture several hundred thousand encrypted packets with a protocol analyzer and then run the captured data through a WEP cracking software utility. The software utility will usually then be able to derive the secret 40-bit or 104-bit key in a matter of seconds. Once the secret key has been revealed, the attacker can decrypt any and all encrypted traffic. In other words, an attacker can now eavesdrop on the WEP-encrypted network. Because the attacker can decrypt the traffic, they can reassemble the data and read it as if there was no encryption whatsoever.

authentication attacks

The 802.11i security amendment defines for authentication either an 802.1X/EAP authentication solution or the use of a pre-shared key for authentication. The 802.11i amendment does not define which type of EAP authentication method to use, and all flavors of EAP are not created equally. Some types of EAP authentication are more secure than others. As a matter of fact, Lightweight Extensible Authentication Protocol (LEAP), one of the most commonly deployed 802.1X/EAP solutions, is susceptible to offline dictionary attacks. The hashed password response during the LEAP authentication process is crackable. An attacker merely has to capture a frame exchange when a LEAP user authenticates and then the capture file is run through an offline dictionary attack tool. The password can be derived in a matter of seconds. The user name is also seen in clear text during the LEAP authentication process. Once the attacker gets the user name and password, they are free to impersonate the user by authenticating onto the WLAN and then access any network resources that are available to that user. Stronger EAP authentication protocols exist that are not susceptible to offline dictionary attacks.

Wireless hijacking

An attack that often generates a lot of press is *wireless* hijacking, also known as the evil twin attack. The attacker configures access point software on a laptop, effectively turning a Wi-Fi client card into an access point. The access point software is configured with the same SSID that is used by a public hotspot access point. The attacker then sends spoofed disassociation or deauthentication frames, forcing users associated with the hotspot access point to roam to the evil twin access point. At this point, the attacker has effectively hijacked wireless clients at layer 2 from the original access point. The evil twin will typically be configured with a Dynamic Host Configuration Protocol (DHCP) server available to issue IP addresses to the clients. At this point, the attacker will have hijacked the users at layer 3 and now has a private wireless network and is free to perform peer-to-peer attacks on any of the hijacked clients. The attacker may also be using a second wireless card with their laptop to execute what is known as a man-in-the-middle attack, as pictured in Figure. The second wireless card is associated to the hotspot access point as a client. In operating systems, networking cards can be bridged together to provide routing. The attacker has bridged together their second wireless card with the Wi-Fi card that is being used as the evil twin access point. Once the attacker hijacks the users from the original AP, the traffic is then routed from the evil twin access point through the second Wi-Fi card right back to the original access point from which they have just been hijacked.

The result is that the users remain hijacked; however, they still have a route back through the gateway to their original network, so they never know they have been hijacked. The attacker can therefore sit in the middle and execute peer-to-peer attacks indefinitely while remaining completely unnoticed.

These attacks can also take another form in what is known as the Wi-Fi phishing attack. The attacker may also have web server software and captive portal software. Once the users have been hijacked to the evil twin access point, they will be redirected to a login web page that looks exactly like the hotspot's login page. Then the attacker's fake login page may request a credit card number from the hijacked user. Phishing attacks are very common on the Internet and are now appearing at your local hotspot. The only way to prevent a hijacking, man-in-the-middle, and/or Wi-Fi phishing attack is to use a mutual authentication solution. Mutual authentication solutions not only validate the user that is connecting to the network, they also validate the network to which the user is connecting. 802.1X/ EAP authentication solutions require that mutual authentication credentials be exchanged before a user can be authorized. A user cannot get an IP address unless authorized; therefore, they cannot be hijacked.

Denial of Service (DoS)

The attacks on wireless networks that seem to receive the least amount of attention are Denial of service (DoS) attacks. With the proper tools, any individual with ill intent can temporarily disable a Wi-Fi network by preventing legitimate users from accessing network resources. The good news is that monitoring systems exist that can detect and identify DoS attacks immediately. The bad news is that there is absolutely nothing that can be done to prevent denial of service attacks other than locating and removing the source of the attack.

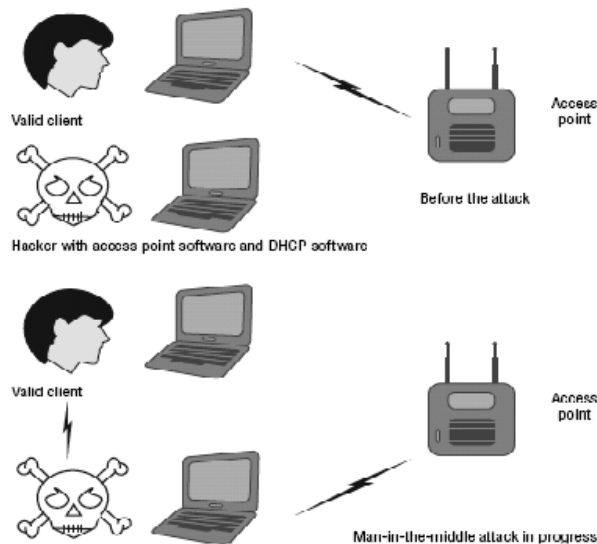


Figure: Man-in-the-middle attack

DoS attacks can occur at either layer 1 or layer 2 of the OSI model. Layer 1 attacks are known as RF jamming attacks. The two most common types of RF jamming attacks are intentional jamming and unintentional jamming. Intentional jamming attacks occur when an attacker uses some type of signal generator to cause interference in the unlicensed frequency space. Both narrowband and wideband jammers exist that will interfere with the 802.11 transmissions, either causing all data to become corrupted or causing the 802.11 radio cards to continuously defer when performing a Clear Channel Assessment (CCA). While an intentional jamming attack is malicious, unintentional jamming is more common. Unintentional interference from microwave ovens, cordless phones, and other devices can also cause denial of service. Although unintentional jamming is not necessarily an attack, it can cause as much harm as an intentional jamming attack. The best tool to detect any type of layer 1 interference, whether intentional or unintentional, is a spectrum analyzer. A spectrum analyzer is your best tool to detect a layer 1 DoS attack and a protocol analyzer or wireless IDS is your best tool to detect a layer 2 DoS attack. The best way to prevent any type of denial of service attack is physical security. The authors of this book recommend guard dogs and barbed wire. If that is not an option, there are several solutions that provide intrusion detection at layers 1, 2, and 3.

Chapter - 24

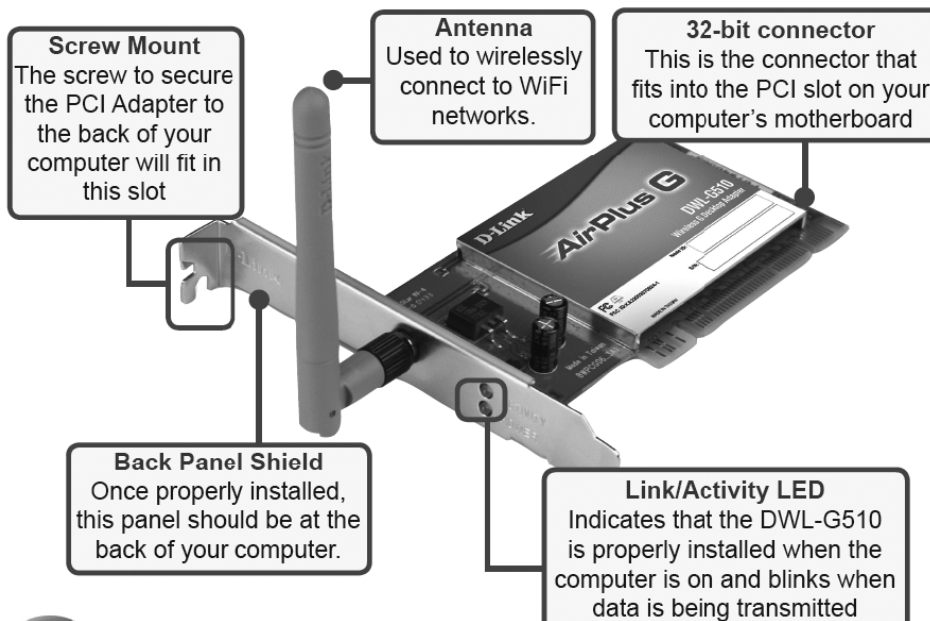
Wi- Fi Network Configuration

Now we already discussed the various parts of wireless network system so we should start creating a network.

requirement for Creating Wireless LaN you must have at least the following:

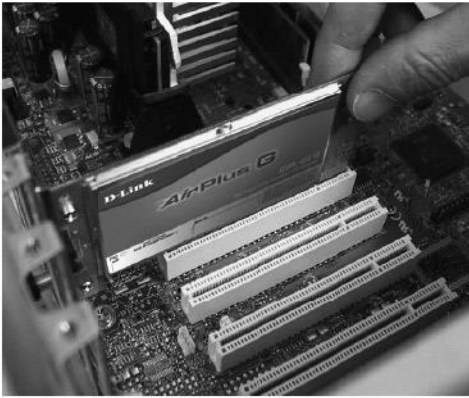
1. A desktop computer with an available 32-bit PCI slot
2. At least a 300 MHz processor and 32MB of memory
3. Wireless LAN card or DWL-G630 Air Plus G 2.4GHz Wireless Card bus Adapter
4. An 802.11g or 802.11b Access Point (for Infrastructure Mode) or another 802.11g or 802.11b wireless adapter (for Ad-Hoc; Peer-to-Peer networking Mode.)

a Wireless LaN card:



Installing the DWL-G510 Wireless pCI adapter in Your Computer

- A. Make sure to turn off your computer and unplug the power cord. Remove the back cover of the computer.
- B. Install the DWL-G510 carefully and firmly seat it into an available PCI slot (which is usually "white" or "cream" colored).



! To avoid damage caused by static electricity, make sure to properly ground yourself by first touching a metal part of your computer to discharge any static electricity before working with the DWL-G510 Wireless PCI Adapter.

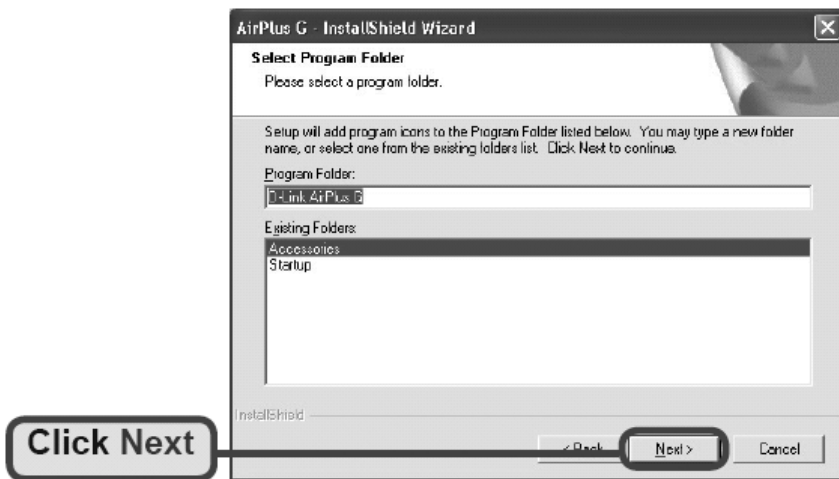
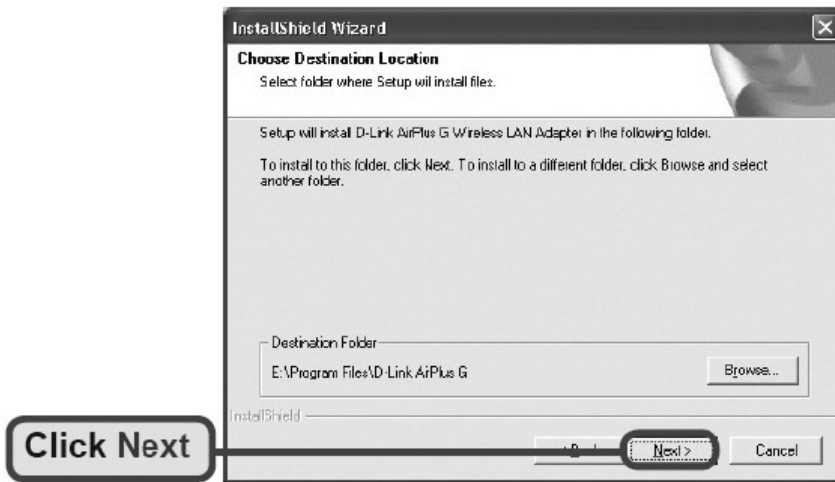
- C. Secure the DWL-G510 back panel shield with a screw.
- D. Replace the computer's cover.
- E. Place the computer back in its normal position.
- F. Attach the DWL-G510's antenna to the socket on the back panel shield.

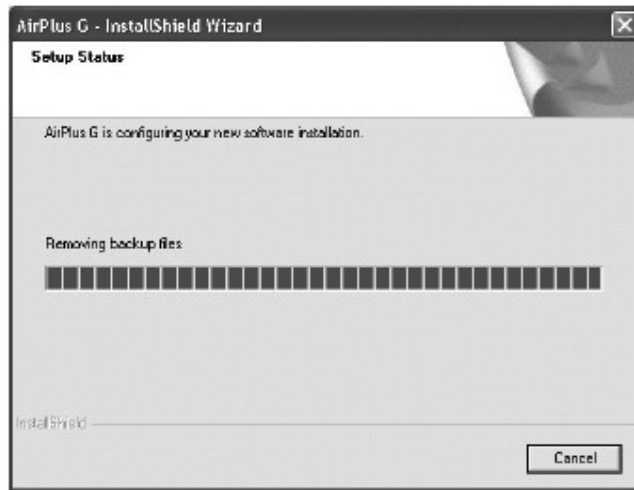
Installing Wireless card LaN Driver Software:

The step-by-step instructions that follow are shown in Windows XP. The steps and screens are similar for the other Windows operating systems

- 1) Turn on the computer and Insert the D-Link Air Plus® G DWL-G510 Driver CD in the CD-ROM drive.
- 2) If the CD Auto runs function does not automatically start on your computer, type "D:\Drivers\setup.exe." If it does start, proceed to the next screen.

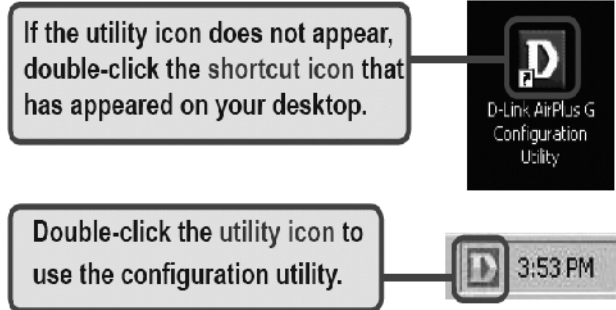






- 3) Restart Your Computer
- 4) Your Installation is Complete.

After you've continued in Windows 2000, ME, or 98SE, the D-Link Air Plus® GDWL-G510 Configuration Utility will automatically start and the utility icon will appear in the bottom right hand corner of the desktop screen (systray). If this icon appears GREEN, then you have successfully installed the DWL-G510, are connected to a wireless network and are ready to communicate.

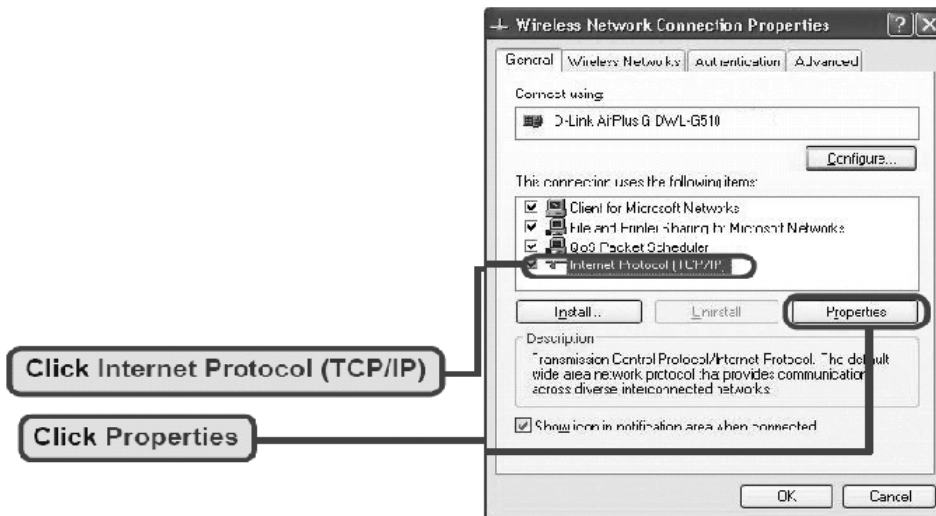


IP Address Configuration

To connect to a network, make sure the proper network settings are configured for DWL-G510.

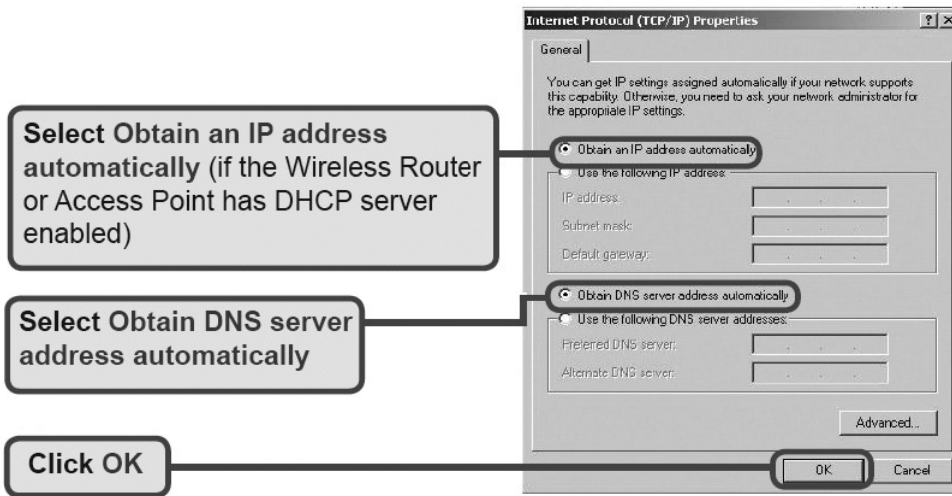
For Microsoft Windows Xp:

Go to Start > right click on My Network places > select properties > Double-click on the Network Connection associated with the DWL-G510.



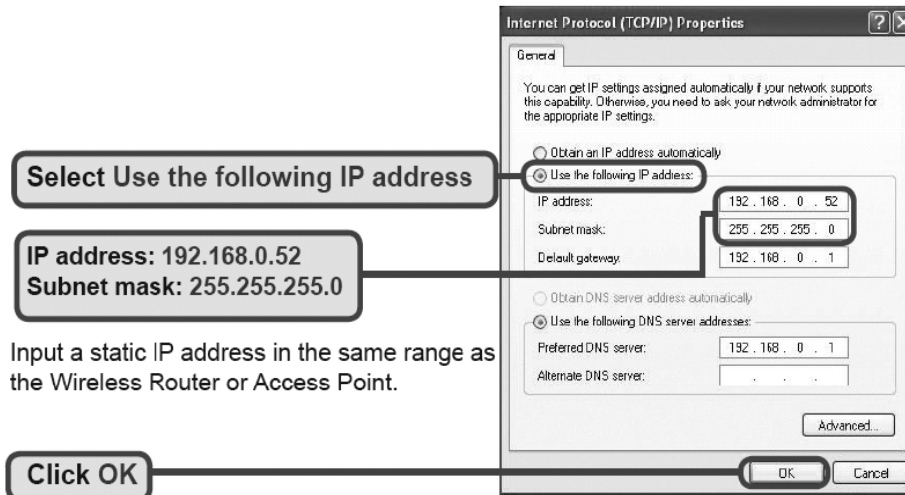
Dynamic Ip address setup

Used when a DHCP server is available on the local network. (i.e. Router)



Static Ip address setup

Used when a DHCP server is not available on the local network.



Defining workgroup name in the network: Using the Network Setup Wizard in Windows Xp.

In this section you will learn how to establish a network at home or work, using Microsoft Windows XP.

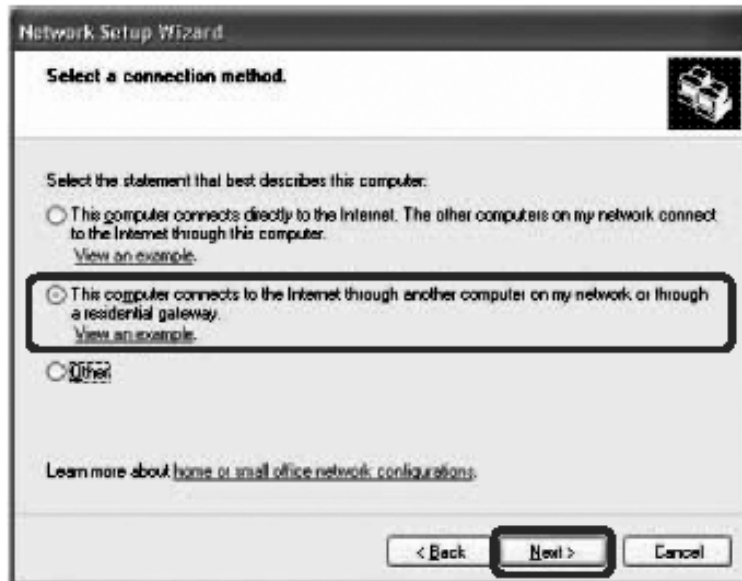
Go to Start>Control Panel>Network Connections Select Set up a home or small office network.



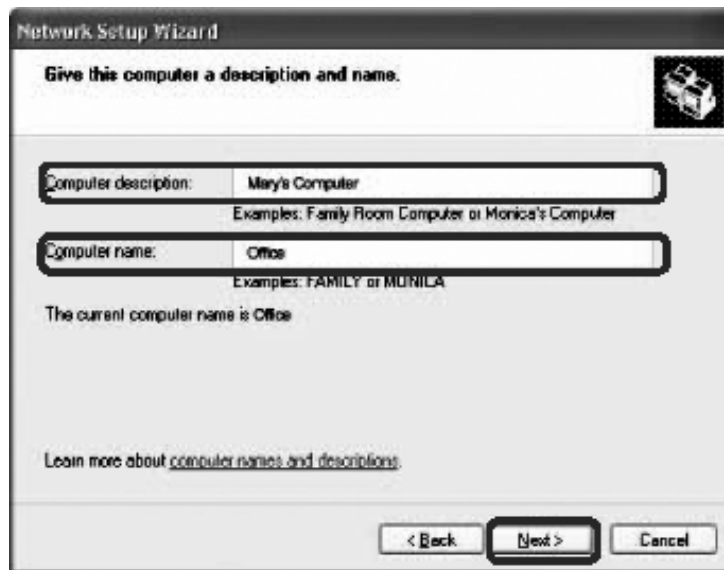
When this screen appears, click next. Please follow all the instructions in this window:



Click **Next**. In the following window; select the best description of your computer. If your computer connects to the internet through a gateway/router, select the second option as shown.



Click **Next**. Enter a **Computer description** and a **Computer name** (optional.)



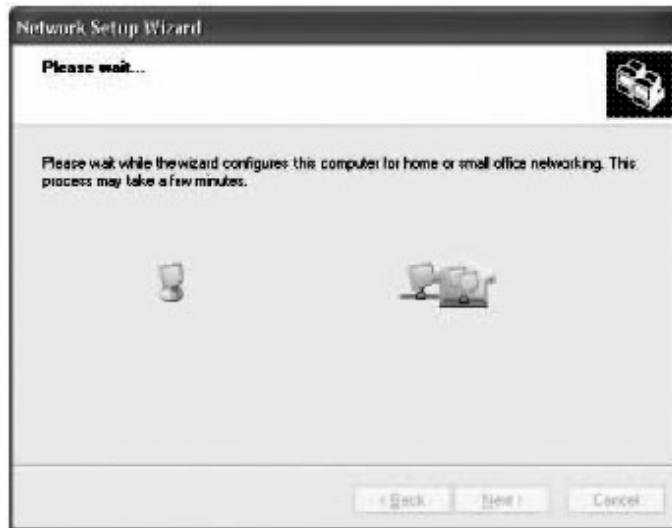
Click **Next**. Enter a **Workgroup** name. All computers on your network should have the same **Workgroup** name.



Click **Next**. Please wait while the **Network Setup Wizard** applies the changes.



When the changes are complete, click **Next**. Please wait while the **Network Setup Wizard** configures the computer. This may take a few minutes.



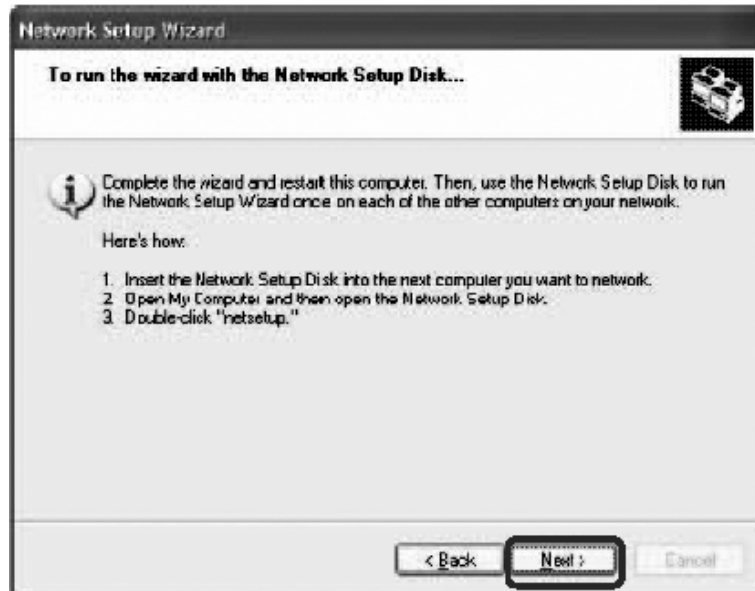
In the window below, select the option that fits your needs. In this example, **Create a Network Setup Disk** has been selected. You will run this disk on each of the computers on your network. Click Next.



Insert a disk into the Floppy Disk Drive, in this case drive **a:**.



Please read the information under **here's how** in the screen below. After you complete the **Network Setup Wizard** you will use the **Network Setup Disk** to run the **Network Setup Wizard** once on each of the computers on your network. To continue click **next**.



Please read the information on this screen, and then click **Finish** to complete the **Network Setup Wizard**.



The new settings will take effect when you restart the computer. Click **yes** to restart the computer.



You have completed configuring this computer. Next, you will need to run the **Network Setup Disk** on all the other computers on your network. After running the **Network Setup Disk** on all your computers, your new wireless network will be ready to use.

assigning hostname to the Computer

To name your computer, please follow these directions: In **Windows Xp operating system**:

- 1) **right-click** on **My Computer**.
- 2) Select **properties** and click.



- In this window, enter the **Computer name**.
- Select **Workgroup** and enter the name of the **Workgroup**.
- All computers on your network must have the same **Workgroup** name.
- Click **OK**.



- Select the **Computer Name** Tab in the System Properties window.
- You may enter a **Computer Description** if you wish this field is optional.
- To rename the computer and join a domain, Click **Change**



Verifying the network connectivity

Go to **Start > run > type cmd**. A window similar to this one will appear. Type **ping xxx.xxx.xxx.xxx**, where **xxx** is the **ip address** of the wireless router or access point. A good wireless connection will show four replies from the wireless router or access point, as shown.

```

C:\ C:\WINDOWS\system32\cmd.exe

C:\>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128

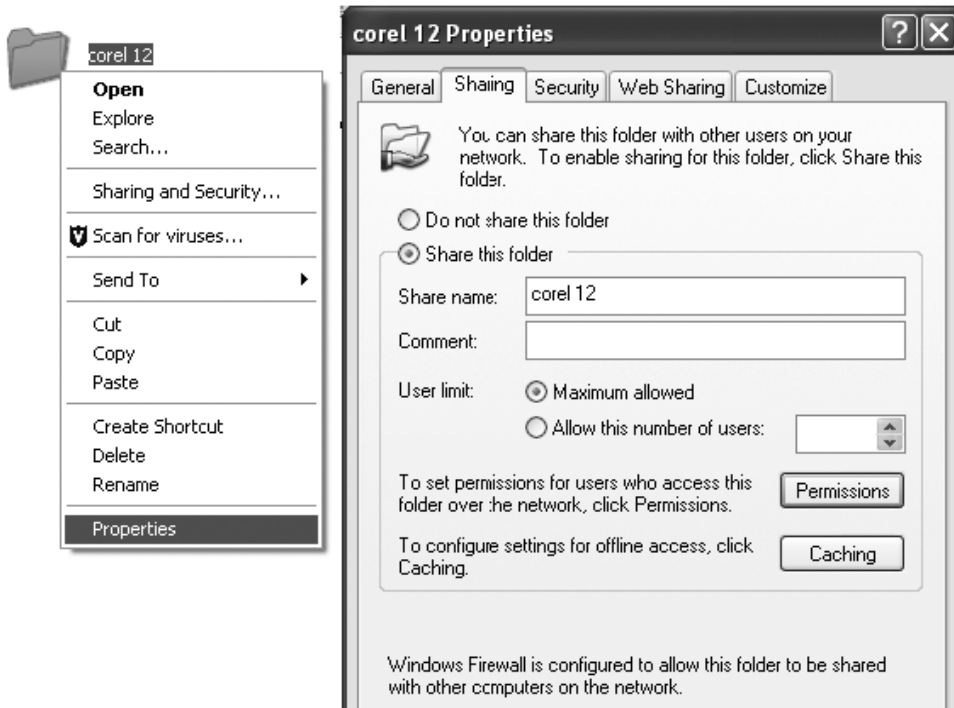
Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

Sharing the windows files & folders

Open the my computer → open the d: drive → Rt. Click on the folder properties → Go to sharing tab → Click on the Share This folder → Assign the share name (It will take default the same folder name) → Click on the permission tab → allow full control → click on apply & ok. → Click on apply & ok.



After sharing the folder it will show the shared folder with hand icon on the computer & network. And for sharing the data it must be shared on the network.



Configuring access point:

Using the Configuration Utility

If you wish to change the default settings or optimize the performance of the DWL-G700AP, D-Link has included a configuration utility for this purpose.

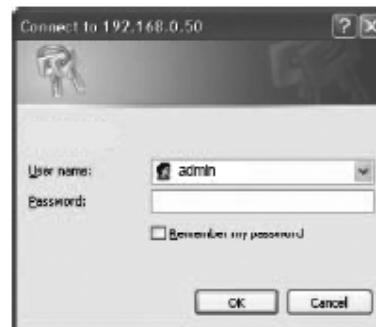
After you have completed the initial installation and the Setup Wizard (as illustrated in the Quick Installation Guide that is included with the DWL-G700AP), you can access the configuration menu, at any time, by opening the web-browser and typing in the IP address of the DWL-G700AP. The DWL-G700AP's default IP address is shown below:

- Open the web browser
- Type in the **IP address** of the DWL-G700AP. (192.168.0.50).

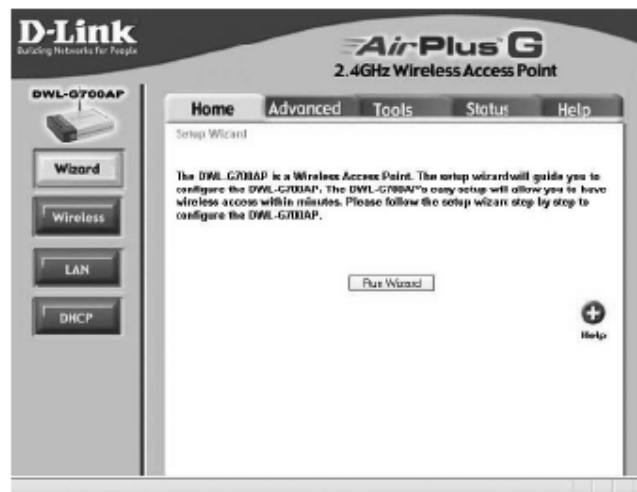


Note: If you have changed the default IP address assigned to the DWL-G700AP, make sure to enter the correct IP address.

- Type **admin** in the **User Name** field
- Leave the **Password** blank
- Click **OK**



The **Home>Wizard** screen will appear. Please refer to the *Quick Installation Guide* for more information regarding the Setup Wizard.



Using the Configuration Utility (continued)

Hexadecimal digits consist of the numbers 0-9 and the letters A-F

ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127

Home > Wireless

SSID: (Service Set Identifier) Default is the default setting. The SSID is a unique name that identifies a network. All devices on a network must share the same SSID name in order to communicate on the network. If you choose to change the SSID from the default setting, input your new SSID name in this field.

Channel: Channel 6 is the default channel. Input a new number if you want to change the default setting. All devices on the network must be set to the same channel to communicate on the network.

Authentication:

Select **Open System** to communicate the key across the network.

Select **Shared Key** to limit communication only to those devices that share the same WEP settings.

Select **WPA** to select *Wi-Fi Protected Access* in conjunction with a RADIUS server in your network.

Select **WPA-PSK** to select *Wi-Fi Protected Access* without a RADIUS server.

WEP: Select Enabled or Disabled.

WEP Encryption: Select 64-bit or 128-bit WEP encryption.

Key Type: Select Hexadecimal or ASCII key type

Keys 1-4: Input up to four encryption keys. You will select one of these to be the active key.

Apply: Click Apply to apply the changes.

Using the Configuration Utility (continued)

Home > LAN



Dynamic IP Address: Select this option if you would like to have an IP Address automatically assigned to the DWL-G700AP by a DHCP server in your network.

DHCP stands for Dynamic Host Configuration Protocol. It is a protocol for assigning dynamic IP addresses "automatically." With a DHCP Server there is no need to manually assign an IP Address.

Static IP Address: Select this option if you are manually assigning an IP Address.

IP Address: 192.168.0.50 is the default IP Address of the Access Point.

Subnet Mask: 255.255.255.0 is the default Subnet Mask. All devices on the network must have the same subnet mask to communicate on the network.

Gateway: Enter the IP Address of the router in your network

DNS Server: Enter the IP address of the DNS server. The DNS server translates domain names such as www.dlink.com into IP addresses.

IP Address

If you need to assign static IP addresses to the devices in your network, please remember that the IP address for each computer or device must be in the same IP address range as all the devices in the network. Each device must also have the same subnet mask. For example: Assign the first computer an IP address of 192.168.0.2 and a subnet mask of 255.255.255.0, the second device an IP address of 192.168.0.3 and a subnet mask of 255.255.255.0, and so on. **Note: Devices that are assigned the same IP address may not be visible on the network.**

Using the Configuration Utility (continued)

Advanced > Performance

Beacon Interval: Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. Default (100) is recommended

RTS Threshold: This value should remain at its default setting of 2,432. If you encounter inconsistent data flow, only minor modifications to the value range between 256 and 2,432 are recommended.

Fragmentation: This value should remain at its default setting

of 2,346. If you experience a high packet error rate, you may slightly increase your fragmentation threshold within the value range of 256 to 2,346. Setting the fragmentation threshold too low may result in poor performance.

DTIM Interval (Beacon Rate). (Delivery Traffic Indication Message) Enter a value between 1 and 255 (default is 3) for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

TX Rates: Select the transmission rate for the network.

Authentication:

Open System - Communicates the key across the network

Shared Key - Devices must have identical WEP settings to communicate.

WPA - WPA authentication in conjunction with a RADIUS server.

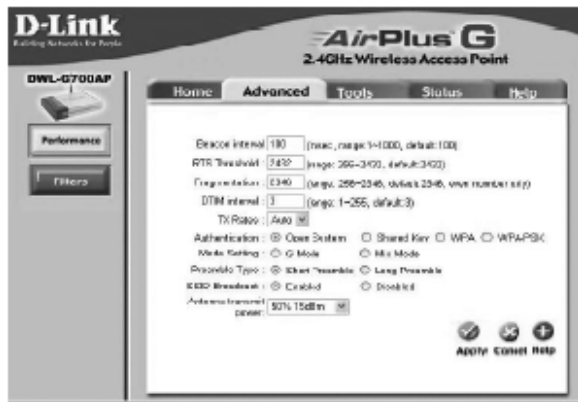
WPA-PSK - WPA authentication without a RADIUS server in the network.

Mode Setting: For utmost speed, select **G Mode** to include only 802.11g devices in your network. Select **Mix Mode** to include 802.11g and 802.11b devices in your network.

Preamble: **Long Preamble** is the default setting. (High traffic networks should use the shorter preamble type.) The preamble defines the length of the CRC block (Cyclic Redundancy Check) is a common technique for detecting data transmission errors) used in communication between the access point and the wireless network adapters.

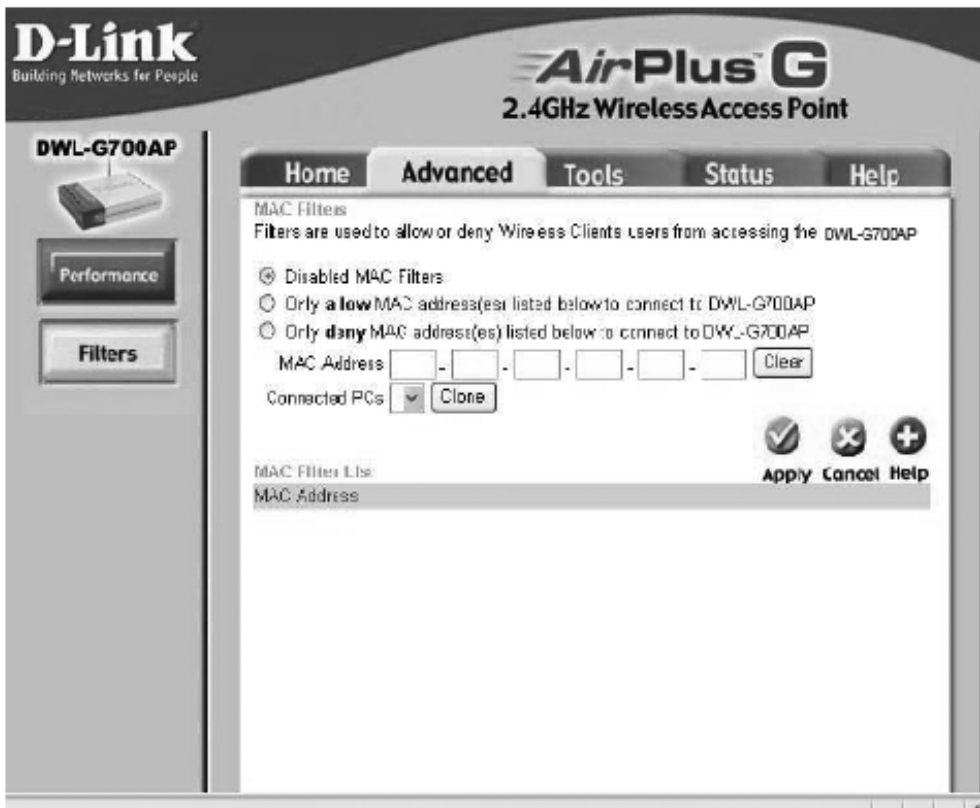
SSID Broadcast: (Service Set Identifier) Enable or Disable (default) the broadcast of the SSID name across the network. SSID is a name that identifies a wireless network. All devices on a network must use the same SSID to establish communication

Antenna Transmit Power: Select the transmission power of the antenna. Limiting antenna power can be useful for security purposes.



Using the Configuration Utility (continued)

Advanced > Filters



Use MAC Filters to allow or deny wireless clients, by their MAC addresses, from accessing the DWL-G700AP. You can manually add a MAC address or select the MAC address from the list of clients that are currently connected to the router (Connected PCs). The default setting is Disabled MAC Filters.

MAC Filter List: This list will display the MAC addresses that are in the selected filter.

Using the Configuration Utility (continued)

New Password: Enter the new password.

Confirm Password: Re-enter the password to confirm it.

Tools > Admin



Save Settings: The current system settings can be saved as a file onto the local hard drive.

Load Settings: The saved file or any other saved setting file can be loaded back on the access point. To reload a system settings file, click on **Browse** to browse the local hard drive and locate the system file to be used. Click **Load** when you have selected the file to be loaded back onto the access point.

Tools > System

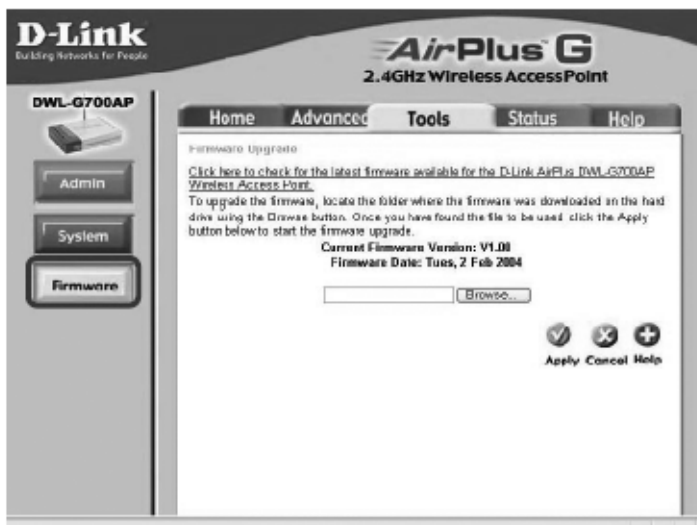


Restore: You may also reset the DWL-G700AP back to factory settings by clicking on **Restore**. Make sure to save the unit's settings before clicking on **Restore**. You will lose your current settings when you click **Restore**.

Using the Configuration Utility (continued)

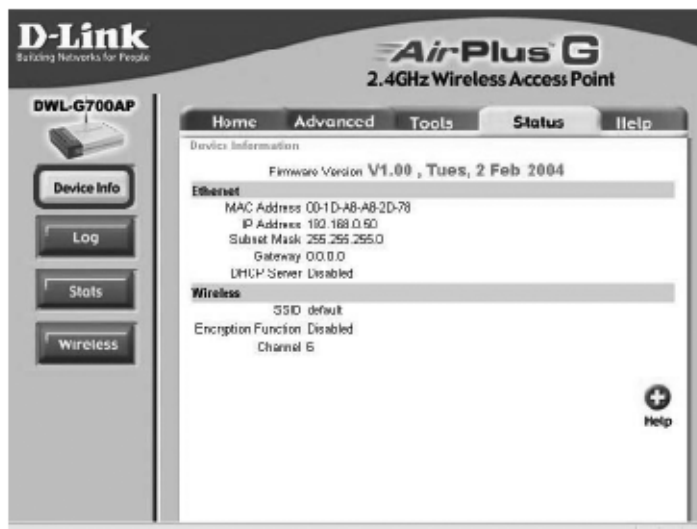
Tools > Firmware

You can upgrade the firmware of the DWL-G700AP at this page. When you click [Click here to check...](#) in this window you will be connected to D-Link's website, where you can download the latest firmware update. After you have completed the firmware download to your hard drive, click **Browse** to browse your local hard drive and locate the firmware to be used for the update. Click **Apply**.



Status > Device Info

This screen displays the current firmware version, and the current wireless and Ethernet settings of the DWL-G700AP.



Using the Configuration Utility (continued)

Status > Log



View Log

The DWL-G700AP keeps a running log of events and activities occurring on the AP. If the device is rebooted, the logs are automatically cleared. You may save the log files under Log Setting.

First Page - The first page of the log.

Last Page - The last page of the log.

Previous - Moves back one log page.

Next - Moves forward one log page.

Clear - Clears the logs completely.

Log Settings - Brings up the page to configure the logs.

Log Settings

Not only does the DWL-G700AP display the logs of activities and events, it can be setup to send these logs to another location. The logs can be sent via email to an email account.

Using the Configuration Utility (continued)

Traffic Statistics

The DWL-G700AP keeps statistics of traffic that passes through it. You are able to view the amount of packets that pass through the Ethernet and wireless portions of the network. The traffic counter will reset if the device is rebooted.

Status > Stats

D-Link Building Networks for People

AirPlus G
2.4GHz Wireless Access Point

DWL-G700AP

Home Advanced Tools **Status** Help

Traffic Statistics
Tools: Statistics Display Receiver and Transmitter Packets Passing through the DWL-G700AP

Ethernet		
Send	Total Packets	669
Recv	Total Packets	655

Wireless		
Send	Total Packets	1
Recv	Total Packets	0

Help

Connected Wireless PCs List

This list displays the MAC Addresses of connected PCs and the length of time that they have been connected.

Status > Wireless

D-Link Building Networks for People

AirPlus G
2.4GHz Wireless Access Point

DWL-G700AP

Home Advanced Tools **Status** Help

Connected Wireless PCs List

Connected Time	MAC Address

Help

Menu

Select from this menu for extra help.

Help

D-Link Building Networks for People

AirPlus G
2.4GHz Wireless Access Point

DWL-G700AP

Home Advanced Tools **Status** **Help**

Home

- Setup Wizard
- Wireless
- LAN Settings
- DHCP Server

Advanced

- Mode
- Performance
- Filter

Tools

- Administrator's Guide
- System Settings
- Firmware Upgrade

Status

- Device Information
- Log
- Stats
- Wireless

FAQs

Chapter - 25

troubleshooting WLAN

Diagnostic methods that are used to troubleshoot wired 802.3 networks should also be applied when troubleshooting a wireless local area network (WLAN). A bottoms-up approach to analyzing the OSI reference model layers also applies with wireless networking. A wireless networking administrator should always try to first determine if problems exist at layer 1 and layer 2. As with most networking technologies, most problems usually exist at the Physical layer. Simple layer 1 problems such as non-powered access points or client card driver problems are often the root cause of connectivity or performance issues. Because WLANs use radio frequencies to deliver data, troubleshooting a WLAN offers many unique layer 1 challenges not found in a typical wired environment. The bulk of this chapter will discuss the numerous potential problems that can occur at layer 1 and what solutions might be implemented to prevent or rectify the layer 1 problems.

A spectrum analyzer is often a useful tool when diagnosing layer 1 issues. After eliminating layer 1 as a source of possible troubles, a WLAN administrator should try to determine if the problem exists at the Data-Link layer. Authentication and association problems often occur due to improperly configured security and administrative settings on access points, wireless switches, and client utility software. A WLAN protocol analyzer is often an invaluable tool for troubleshooting layer 2 problems. We will discuss many coverage considerations and troubleshooting issues that may develop when deploying an 802.11 wireless network. RF propagation behaviors and RF interference will affect both the performance and coverage of your WLAN. Because mobility is usually required in a WLAN environment, many roaming problems often occur and must be addressed. The half-duplex nature of the medium also brings unique challenges typically not seen in a full-duplex environment. Different considerations also need to be given to outdoor 802.11 deployments due to weather conditions.

802.11 Coverage Considerations

Providing for both coverage and capacity in a WLAN design solves many problems. Roaming problems and interference issues will often be mitigated in advance if proper WLAN design techniques are implemented as well as a thorough site survey. In the following sections, we will discuss many considerations that should be addressed to provide proper coverage, capacity, and performance within an 802.11 coverage zone.

Dynamic rate Switching

As client station radios move away from an access point, they will shift down to lower bandwidth capabilities using a process known as *dynamic rate switching (DRS)*. Access points can support multiple data rates depending on the spread spectrum technology used by the AP's radio card. For example, an 802.11b radio supports data rates of 11, 5.5, 2, and 1 Mbps. Data rate transmissions between the access point and the client stations will shift down or up depending on the quality of the signal between the two radio cards, as

pictured in Figure. There is a correlation between signal quality and distance from the AP. As a result, transmissions between two 802.11b radio cards may be at 11 Mbps at 30 feet but 2 Mbps at 150 feet. Dynamic rate switching (DRS) is also referred to as dynamic rate shifting, adaptive rate selection, and automatic rate selection. All these terms refer to a method of speed fallback on a wireless LAN client as signal quality from the access point decreases. The objective of DRS is up shifting and downshifting for rate optimization and improved performance. Effectively, the lower data rates will have larger concentric zones of coverage than the higher data rates, as pictured in following Figure.

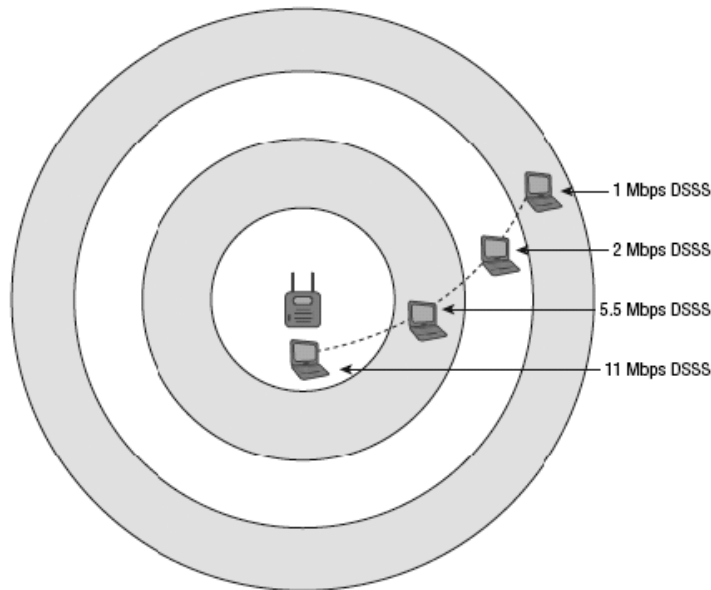


Figure: Dynamic rate switching

roaming

Roaming is the method where client stations move between RF coverage cells in a seamless manner. Client stations switch communications through different access points. Seamless communications for stations moving between the coverage zones within an Extended Service Set (ESS) is vital for uninterrupted mobility. One of the most common issues you'll need troubleshoot is problems with roaming. Roaming problems are usually caused by poor network design. Due to the proprietary nature of roaming, problems can also occur when radio cards from multiple vendors are deployed. Changes in the WLAN environment can also cause roaming hiccups. Client stations and not the access point make the decision on whether or not to roam between access points. Some vendors may involve the access point or wireless switch in the roaming decision, but ultimately, the client station initiates the roaming process with a reassociation request frame. The method in which client stations decide how to roam is entirely proprietary. All vendor client stations use roaming algorithms that can be based on multiple variables. The variable

of most importance will always be received signal strength. As the received signal from the original AP grows weaker and a station hears a stronger signal from another known access point, the station will initiate the roaming process. However, other variables such as SNR, error rates, and retransmissions may also have a part in the roaming decision. Because roaming is proprietary, a specific vendor client station may roam sooner than a second vendor client station as they move through various coverage cells. Some vendors like to encourage roaming while others use algorithms that roam at lower received signal thresholds. In an environment where a WLAN administrator must support multiple vendor radios, different roaming behaviors will most assuredly be seen. For the time being, a WLAN administrator will always face unique challenges because of the proprietary nature of roaming. In the future, the 802.11k draft and much anticipated 802.11r roaming draft will hopefully standardize many aspects of roaming. The best way to assure that seamless roaming will commence is proper design and a thorough site survey. When designing an 802.11 WLAN, most vendors recommend 15 to 20 percent overlap in coverage cells at the lowest desired signal level. The only way to determine if proper cell overlap is in place is by conducting a coverage analysis site survey. Proper site survey procedures are discussed in detail in Chapter 16. Roaming problems will occur if there is not enough overlap in cell coverage. Too little overlap will effectively create a roaming dead zone, and connectivity may even temporarily be lost. On the flip side, too much cell overlap will also cause roaming problems. For example, if two cells have 60 percent overlap, a station may stay associated with its original AP and not connect to a second access point even though the station is directly underneath the second access point. This can also create a situation in which the client device is constantly switching back and forth between the two or more APs. This often presents itself when a client device is directly under an AP and there are constant dropped frames.

Co-Channel Interference

When designing a wireless LAN, you need overlapping coverage cells in order to provide for roaming. However, the overlapping cells should not have overlapping frequencies, and only channels 1, 6, and 11 should be used in the 2.4 GHz ISM band in the United States to get the most available, non-overlapping channels. Overlapping coverage cells with overlapping frequencies causes what is known as co-channel interference (*CCI*), which causes a severe degradation in performance and throughput. If overlapping coverage cells also have frequency overlap, frames will become corrupted, retransmissions will increase, and throughput will suffer significantly.

Channel reuse

One of the most common mistakes many businesses make when first deploying a WLAN is to configure multiple access points all on the same channel. This will of course cause co-channel interference and degrade performance significantly. To avoid co-channel interference, a channel reuse design is necessary. Once again, overlapping RF coverage cells are needed for roaming but overlap frequencies must be avoided. The only three channels that meet these criteria in the 2.4 GHz ISM band are channels 1, 6, and 11 in the United States. Overlapping coverage cells therefore should be placed in a *channel*

reuse pattern similar to the one pictured in Figure 12.7. Channel reuse patterns should also be used in the 5 GHz UNII bands. All 12 802.11a channels can be used, as pictured in Figure 12.8. Due to the frequency overlap of channel sidebands, there should always be at least 2 cells between access points on the same channel. It is also a recommend practice that any adjacent cells use a frequency that is at least 2 channels apart and not use an adjacent frequency. It is necessary to always think three-dimensional when designing a channel reuse pattern. If access points are deployed on multiple floors in the same building, a reuse pattern will be necessary, such as the one pictured in Figure 12.9. A common mistake is to deploy a cookie-cutter design by performing a site survey on only one floor and then placing the access points on the same channels and same locations on each floor. A site survey must be performed on all floors, and the access points often need to be staggered to allow for a three-dimensional reuse pattern. Also, the coverage cells of each access point should not extend beyond more than one floor above and below the floor on which the access point is mounted. It is inappropriate to always assume that the coverage bleed over to other floors will provide sufficient signal strength and quality. In some cases, the floors are concrete or steel and allow very little, if any, signal coverage through.

hidden Node

Physical carrier-sense and the clear channel assessment (CCA). The CCA involves listening for 802.11 RF transmissions at the Physical layer, and the medium must be clear before a station can transmit. The problem with physical carrier sense is that all stations may not be able to hear each other. Remember that the medium is half-duplex and, at any given time, only one radio card can be transmitting. What would happen, however, if one client station that was about to transmit performed a CCA but did not hear another station that was already transmitting? If the station that was about to transmit did not detect any RF energy during the CCA, it will also transmit. The problem is that you now have two stations transmitting at the same time. The end result is a collision, and the frames will become corrupted. The frames will have to be retransmitted. The *hidden node* problem occurs when one client station's transmissions are unheard by any or all the other client stations in the basic service set (BSS).

In Figure you see the coverage area of an access point. Note that a thick block wall resides between one client station and all of the other client stations that are associated to the access point. The RF transmissions of the lone station on the other side of the wall cannot be heard by all of the other 802.11 client stations even though all the stations can hear the AP. That unheard station is the hidden node. What keeps occurring is that every time the hidden node transmits, another station is also transmitting and a collision occurs. The hidden node continues to have collisions with the transmissions from all the other stations that cannot hear it during the clear channel assessment. The collisions continue on a regular basis and so do retransmissions, with the final result being a decrease in throughput. A hidden node can drive retransmission rates above 15 to 20 percent or even higher. Retransmissions, of course, will affect throughput.

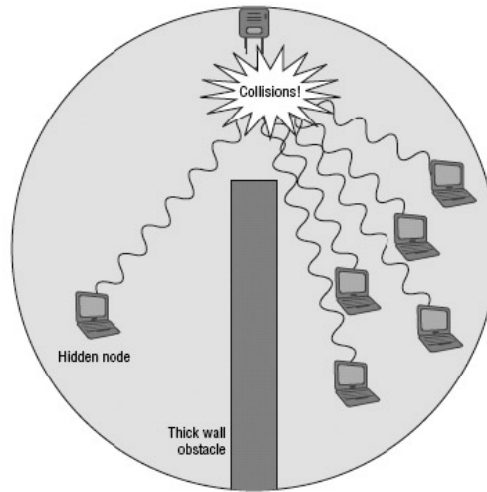


Figure: Hidden node—obstruction

The hidden node problem may exist because of several reasons. Poor WLAN design often leads to a hidden node problem. Obstacles such as a newly constructed wall or newly installed bookcase can cause a hidden node problem. A user moving behind some sort of obstacle can cause a hidden node problem. Users with wireless desktops often place their radio card underneath a metal desk and effectively transform that radio card into an unheard hidden node. The hidden node problem can also occur when two client stations are at opposite ends of an RF coverage cell and they cannot hear each other, as seen in Figure. This often happens when coverage cells are too large as a result of the access point's radio transmitting at too much power. As mentioned earlier in this chapter, it is a recommended practice to disable the data rates of 1 and 2 Mbps on an 802.11b/g access point if you are planning for capacity. Another reason for disabling those data rates is that a 1 and 2 Mbps coverage cell at 2.4 GHz can be quite large and often results in hidden nodes. If hidden node problems occur in a network planned for coverage, then RTS/CTS may be needed.

Near/Far

As stated earlier, most client stations have a fixed power output. However, the transmission power can be configured on some vendors' client radios. A low-powered client station that is a great distance from the access point could potentially become an unheard client if other high-powered stations are very close to the access point. The transmissions of the high-powered stations could raise the noise floor to a higher level that would prevent the lower-powered station from being heard, as seen in Figure. This scenario is referred to as the near/far problem.

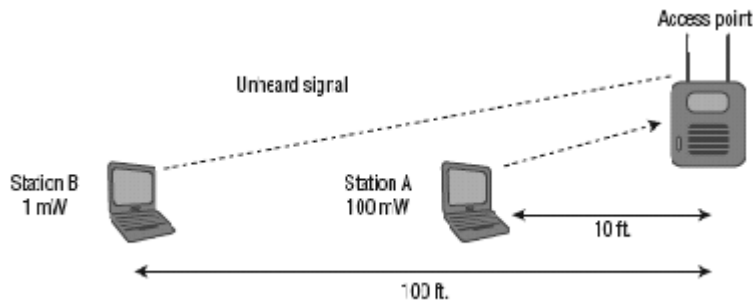


Figure: The near/far problem

The half-duplex nature of the medium usually prevents most near/far occurrences, but you can troubleshoot near/far with a protocol analyzer by looking at the frame transmissions of the suspected far station. A near/far problem exists if the frame transmissions of the far station are corrupted when listened to with the protocol analyzer near the access point but are not corrupted when listened to with the protocol analyzer near the far station. If a near/far situation does exist, the following solutions can be used to correct the problem: Decrease power to the near stations. Increase power to the remote station. Move the remote station closer to the access point. Add another access point near the far node. Please understand that the medium access methods employed by Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) usually averts the near/far problem and that it is not as common a problem of, say, hidden node or roaming issues.

Interference

Various types of interference can greatly affect the performance of an 802.11 WLAN. Interfering devices may actually prevent an 802.11 radio from transmitting. If another RF source is transmitting with strong amplitude, an 802.11 radio can sense the energy during the clear channel assessment (CCA) and defer transmission entirely. The other typical result of interference is that 802.11 frame transmissions become corrupted. If frames are corrupted due to interference, there will be excessive retransmissions and therefore throughput will be reduced significantly. There are several different types of interference:

physical interference

Narrowband interference

Wideband interference

all-band interference

Inter-symbol interference

performance

When designing and deploying a WLAN, you will always be concerned about both coverage and capacity. Various factors can affect the coverage range of a wireless cell,

and just as many factors can affect the aggregate throughput in an 802.11 WLAN. The following variables can affect the *range* of a WLAN:

transmission power rates The original transmission amplitude (power) will have an impact on the range of an RF cell. An access point transmitting at 30 mW will have a larger coverage zone than an access point transmitting a 1 mW assuming that the same antenna is used.

antenna gain Antennas are passive gain devices that focus the original signal. An access Point transmitting at 30 mW with a 6 dBi antenna will have greater range than it would if it used only a 3 dBi antenna.

antenna type Antennas have different coverage patterns. Using the right antenna will give the greatest coverage and reduce multipath and nearby interference.

Wavelength Higher frequency signals have a smaller wavelength property and will attenuate faster than a lower frequency signal with a larger wavelength. 2.4 GHz access points have greater range than 5 GHz access points.

Free space path loss In any RF environment, free space path loss (FSPL) attenuates the signal as a function of distance and frequency.

physical environment Walls and other obstacles will attenuate an RF signal due to absorption and other RF propagation behaviors. A building with concrete walls will require more access points than a building with drywall because concrete is denser and attenuates the signal faster than drywall. Proper WLAN design must take into account both coverage and capacity. The above-mentioned variables all affect range so therefore also affect coverage. Capacity performance considerations are equally as important as range considerations. Please remember that 802.11 data rates are considered bandwidth and not throughput. The following are among the many variables that can affect the *throughput* of a WLAN:

Carrier Sense Multiple access/Collision avoidance (CSMA/Ca) The medium access method that uses interframe spacing, physical carrier sense, virtual carrier sense and the random back off timer creates overhead and consumes bandwidth. The overhead due to medium contention usually is 50 percent or greater.

encryption Extra overhead is added to the body of an 802.11 data frame whenever encryption is implemented. WEP/RC4 encryption adds an extra 8 bytes of overhead per frame, TKIP/RC4 encryption adds an extra 20 bytes of overhead per frame, and CCMP/AES encryption adds an extra 16 bytes of overhead per frame. Layer 3 VPNs often use DES or 3DES encryption, both of which consume significant bandwidth.

application use Different types of applications will have variant affects in bandwidth consumption. Wi-Fi and data collection scanning typically does not require a lot of bandwidth. Other applications that require file transfers or database access often are more bandwidth intensive.

Number of clients Remember that the WLAN is a shared medium. All through put is aggregate and all available bandwidth is shared.

Interference All types of interference can cause frames to become corrupted. If frames are corrupted, they will need to be retransmitted and throughput will be affected.

Weather

When deploying a wireless mesh network outdoors or perhaps an outdoor bridge link, a WLAN administrator must take into account the adverse affect of weather conditions. The following three weather conditions must be considered.

Lightning Direct and indirect lightning strikes can damage WLAN equipment. Lightning Arrestors should be used for protection against transient currents. Solutions such as lightning rods or copper/fiber transceivers may offer protection against lightning strikes.

Wind Due to the long distances and narrow beam widths, highly directional antennas are susceptible to movement or shifting caused by wind. Even slight movement of a highly directional antenna can cause the RF beam to be aimed away from the receiving antenna, interrupting the communications. In high-wind environments, a grid antenna will typically remain more stabile than a parabolic dish. Other mounting options may be necessary to stabilize the antennas from movement.

Water Conditions such as rain, snow, and fog present two unique challenges. First, all outdoor equipment must be protected from damage from exposure to water. Water damage is often a serious problem with cabling and connectors. Connectors should be protected with drip loops and coax seal to prevent water damage. Cables and connectors should be checked on a regular basis for damage. A random should be used to protect antennas from water damage. Outdoor bridges, access points, and mesh routers should be protected from the weather elements using appropriate National Electrical Manufacturers Association (NEMA) enclosure units. Precipitation can also cause an RF signal to attenuate. A torrential downpour can attenuate a signal as much as .08 dB per mile (.05 dB per kilometer) in both the 2.4 GHz and 5 GHz frequency ranges. Over long-distance bridge links, a system operating margin (SOM) of 20 dB is usually recommended to compensate for attenuation due to rain or fog or snow.

air stratification A change in air temperature at high altitudes is known as air stratification (layering). Changes in air temperature can cause refraction. Bending of RF signals over long distance point-to-point links can cause misalignment and performance issues. K-factor calculations may be necessary to compensate for refraction over long-distance links.

UV/sun UV rays and ambient heat from rooftops can damage cables over time unless proper cable types are used.

Practical's in Networking Technology

Session- 1 (After Lec. 1)

Crimping of Cables

Duration – 30 Min.

For performing the following experiment the student must have the following requirements:

1. A long CAT5 cable which is divided into 2 parts.
2. A crimping tool to cut and crimp the wire.
3. RJ45 connectors.

Steps to perform the objectives are:

1. Divide the long CAT5 cable into 2 parts and from both the ends peel off the upper layer of the cable so that only thin colored wires are left out.
2. If you want to perform a straight crimping then arrange the colored wires into a particular color pattern. The color pattern goes in the following way.

Orange-white - Orange

Green-white - Blue

Blue-white - Green

Brown-white - Brown

Then use the RJ45 connector and insert the arranged cables into connector and then crimp the cable in RJ45 connector using crimping tool.

3. If you want to perform a crossover crimping then on one side of the wire the color coding will be the same as straight crimping that is:

Orange-white: Orange

Green-white: Blue

Blue-white: Green

Brown-white: Brown

Then use the RJ45 connector and insert the arranged cables into connector and then crimp the cable in RJ45 connector using crimping tool. And on the other side the color coding will be:

Green-white: Green

Orange-white: Blue

Blue-white: Orange

Brown-white: Brown

Then use the RJ45 connector and insert the arranged cables into connector and then crimp the cable in RJ45 connector using crimping tool.

Test your Knowledge:

1. What is the color coding of straight crimping?
Ans:
2. Which connector is used to crimp CAT5 cable?
Ans:
3. What is structured cabling? And how it is done and what are the devices required for structured caballing?
Ans:

Check List:

Sr. No.	Activity	Result
1	Crimped straight cable	
2	Crimped crossover cable	

Session 1 (Till Lec 11)

Client/Server Configuration

Duration: 45 Min.

To perform the given objective the student must have the following requirements.

1. A computer with a configuration that meets the minimum hardware requirements that is needed to install Windows Server 2003.
2. A Windows Server 2003 bootable CD.

Steps to be performed by the students to do the installation of Windows Server 2003.

1. Go to the BIOS of the machine. From the advance BIOS features set the first boot device as CD-ROM.
2. Insert the bootable CD and start the Setup.
3. Follow the instruction and format the hard disk by creating partitions.
4. The Setup will copy its files from the CD and then it restart the machine and then it will demand for the product key. Insert the product key and the next step it will ask for the number of clients that is to be attached to the server. Define the required number as per your network.

Test Your Knowledge:

1. What type of network will you suggest if you want to build a network of 10 pc in a company? (Workgroup or a Domain)
Ans:
2. Can you install a Windows Server OS in the PC with configuration

CPU: Pentium with 100 MHz

Ram: 64MB

Hard disk: 2GB

Ans:

Prepare Check List:

Activity	Result
Hardware requirements for windows 2008 server	
Default name of the Workgroup or Domain	

Session 2: For performing this experiment the student must have following requirements

1. At least one machine with Windows Sever Operating system.
2. At least one machine with any other operating system for client purpose.
3. A crossover cable to connect both machines.

Steps to be performed by the students to perform the following objective

1. First connect both machines with the crossover cable. Then go to the LAN card properties of the Server. Give a Static IP address and in the block of DNS server also insert the same IP address. Go to Advanced Tab and then go to DNS tab and then there enter the DNS name in DNS Suffix dialog box.
2. After configuring the LAN card of server configure the LAN card of the other machine (client) by giving the Static IP address and in the block of DNS server enter the IP address of SERVER. Go to Advanced Tab and then go to DNS tab and then there enter the DNS name in DNS Suffix dialog box.
3. After configuring both the LAN cards of Client and the Server go to the control panel of Server and in that click on Add Remove Programs and then click on Add/remove Windows components. Install the DNS component form networking and services.
4. Then Configure the DNS by configuring the forward and reverse lookup zones by giving the DNS name and the range of IP address that you have entered into the LAN card.
5. Restart the machine and check that the server is contacting the DNS Properly or no. To check this you have to type the command “nslookup.exe” in RUN or in command prompt.
6. To promote the Server into a domain controller after configuring DNS type the command “DCPROMO” in RUN to install the ADS (Active directory services).
7. Follow the wizard and enter the Domain name and then give a password which will help you to restore the ADS from the directory services restore mode if there is a

crash down of your ADS. This password is known as “Directory Services Restore Mode Password”. Then it will ask you to restart the machine and the Sever than will get converted into a Domain Controller.

- To connect the client machine to the server go the properties of my computer in the client machine and then in the computer name tab and in that go to change option and hen in the domain dialog box type the domain name and then enter the administrator password and the user name as administrator of the server.

Test Your Knowledge:

- What is the primary function of DNS?
Ans:
- When and for what purpose the directory services restore mode password is used?
Ans:
- What is the very first thing that you should perform in the SERVER before installing DNS?
Ans:
- What is the command which is used to check that the DNS is properly installed?
Ans:

Check List:

Sr. No.	Activity	Result
1	Both client server connected through straight cable	
2	Check DNS is properly installed in the server	
3	Verify ADS is properly installed	
4	Client is properly connected to the domain	

Session 3:

For performing this experiment the student must have following requirements:

- A server which is already promoted to a domain controller (with ADS and DNS installed).
- A client machine which is a member of the domain.

Steps to be performed by the students to perform the following objective

- Open Active directory users and computers from administrative tools. Click on the Domain and then go to users and then right click on the blank area and then go to new and then user.

2. Fill the details demanded in the user form. Give a password to the user and then click on finish. Your user gets created.
3. Test the same user in the client machine by login in that computer with the name of the user created.
4. In the same way you can create a new group or a new OU (organizational unit).

Test Your Knowledge:

1. What is a primary requirement of installing ADS?
Ans:
2. What is the difference between a user and a group?
Ans:

Check List:

Sr. No.	Activity	Result
1	ADS is installed properly	
2	User, group, OU is created	
3	The user can login in the client machine properly	

Session 1 (Till Lec 12)

Different type of Remote Management Tools

Duration: 45 Min.

To perform the experiment the students must have the following requirements:

1. Two computers with a crossover cable to connect them to each other.
2. Any windows operating system (Windows server 2003/XP) so that we can use the remote management tools.

Steps to be followed to perform the objective:

1. The student can remotely manage any system by sitting at one place only on a LAN. To take a remote desktop of a particular computer you must enable the remote desktop of the machine from the properties of my computer.
2. From other computer type the command "MSTSC" in Run and then enter. And then in the dialog box appeared type the IP address of the computer of whose remote desktop was enabled earlier by us.
3. Click on Connect and then enter the user name and it's password you can view that computer's desktop in front of you and you can manage the same computer remotely. The same thing can be performed from START → Program → accessories → connections → Remote desktop Connections.

4. You can use the other option of windows Net Meeting tool by typing the command “conf.exe” in RUN. Then just follow the wizard that appears in front of you. Enter the IP address of remote machine in IP address box and then you can remotely connect to the computer you want in the network.

Test your knowledge:

1. What is the command used for Net meeting configuration?
Ans:
2. What do you mean by Remote Management?
Ans:
3. What is the most important thing that should be done to take a remote desktop of a computer?
Ans:
4. Describe the two tools which are used for remote management?
Ans:

Check List:

Sr. No.	Activity	Result
1	Two computers must be connected to each other	
2	Windows operating system must be installed on both computers	

Session 2:

To perform the above experiments the student must have the following requirements.

1. Two computers connected to internet
2. A third party software for e.g.: Team viewer

Steps to be followed by the students to achieve the objective:

1. The student can take a remote desktop via internet if the ISP has provided a static IP address. But if the ISP has not provided the static IP address then we can use the third party software.
2. Install the Team viewer software in both the computer. Then open the main screen of the software. You will get a code on your screen. Then enter the code of the other computer’s main screen and the password that is shown below the code (of the other computer of which you want to take a remote desktop).
3. You can see the desktop of the opposite computer. The main advantage of this is that the other person can see what the person is exactly doing after taking the remote desktop of his computer.

Test your Knowledge:

1. Which tools can be used to take remote desktop via third party software?

Ans:

2. What is the main advantage of team viewer software?

Ans:

Check List:

Sr. No.	Activity	Result
1	2 computer with internet facility	
2	Third party software installed in both computers	

Session – 1 (Till Lec. 21)

Network Troubleshooting:

Duration: 30 Min.

For performing the experiments the student must have the following requirements

1. At least 2 machines with any operating system.
2. One crossover cable to connect both machines with each other.
3. At least some data must be shared on any machine to access from other one.

Steps to be performed to troubleshoot the problems which can be faced.

1. The first step is to check the physical connectivity by checking the LAN card signal.
2. If the LAN card signal does not come on the taskbar then you can check for the LAN card drivers whether the drivers are installed properly. If there are not installed properly then you can re-install it.
3. If the LAN card signal is shown and still the signal is showing the cross mark then check for the cable connectivity.
4. To check the connectivity types the command “ping IP address” in Run. (E.g.: ping 192.168.0.10)
5. If the reply comes from the IP address then the network is perfect. But if the reply does not come then you can check the crossover cable whether it is crimped properly. If it is not crimped then you can re-crimp the cable.

Test your knowledge:

1. What is the color coding of Crossover crimping?

Ans:

2. What is the primary command that is used to check the connectivity between two machines?

Ans:

3. What is the color coding of straight crimping?

Ans:

4. What is Peer to Peer networking?

Ans:

5. What is the command for checking the LAN card configuration through command prompt?

Ans:

6. What is the command to test whether the LAN card driver is properly installed?

Ans:

Check List:

Sr. No.	Activity	Result
1	2 machine connected to each other	
2	LAN driver must be installed	

Session 2 for performing the experiments the student must have the following requirements

1. At least 2 Computers.
2. One crossover cable to connect both machines with each other.
3. Any one of the two machines must be a server which is promoted to a domain controller (DNS and ADS).
4. The other machine with any OS for the client purpose.

Steps to perform the troubleshooting in the client server network:

1. First of all you have to check the basic connectivity that we have performed in session 1.
2. Check whether the client computer is connected to domain which is created in server computer.
3. If it is not connected then it will not be able to access the data on server.
4. If the user is not created properly on the server then it will not be able to login on the network (on the client machine).
5. If the data is not able to be accessed on the client machine from the user login then check the data sharing properties and there you can check the rights given to a user on the data by the administrator of server.

Test your knowledge:

1. What is a client-server network?
Ans:
2. What is safer client-server network or a workgroup network?
Ans:
3. Where do you create the users in server which can work on a network?
Ans:
4. What is to be installed first to promote a normal server into a domain controller?
Ans:

Check List:

Sr. No.	Activity	Result
1	Server with ADS and DNS installed	
2	One client machine to test the user created	
3	Both computers connected with crossover cable	

Session – 1 (Till Lec. 25)

Wireless LAN Configuration:

Duration: 30 Min.

For performing the experiments the student must have the following requirements

1. At least 2 machines with any operating system.
2. Use Dink/Linksys Access point and open default page and configure the new SSID "Practice".
3. Share data from one machine and access it from other machine.
4. Configure Secured network by using WPA/WEP/Shared shared key password authentication.
5. Configure DHCP server on Wireless LAN.

