

Experiment-1

Aim: Specifications of latest Laptops and Desktops

Latest Laptop:

DELL Alienware M17x gaming laptop

➤ **Processor:**

3rd Generation Intel® Core™ i7-3740QM Processor

➤ **Memory (RAM):**

8GB 1600MHz DDR3 SDRAM (2 x 4GB)

➤ **Cache Memory L1/L2:**

6MB Cache, up to 3.7GHz w/ Turbo

➤ **Video Card / Graphic Card:**

2GB GDDR5 Nvidia GeForce GTX 675M

➤ **Sound Card:**

Creative Sound Blaster Recon3Di High-Definition 5.1 Audio

with THX TruStudio Pro

Audio Powered by Klipsch®

➤ **Optical Drive:**

Slot-Loading 8x Super Multi Drive (DVD±R/RW) (Standard)

➤ **Motherboard (Chipset):**

Intel 940 XM

➤ **Hard Drive:**

Up to 1 TB hard drive (5400RPM)



HP ENVY Touch Smart Ultra book 4-1113tu

➤ **Processor:**

Intel® Core™ i5-3317U (1.7 GHz)

➤ **Memory (RAM):**

4 GB 1600 MHz DDR3

➤ **Cache Memory L1/L2:**

3 MB L3 cache

➤ **Video Card / Graphic Card:**

Intel HD Graphics 4000

➤ **Sound Card:**

Beats Audio™ playback.

➤ **Optical Drive:**

Not Present

➤ **Motherboard (Chipset):**

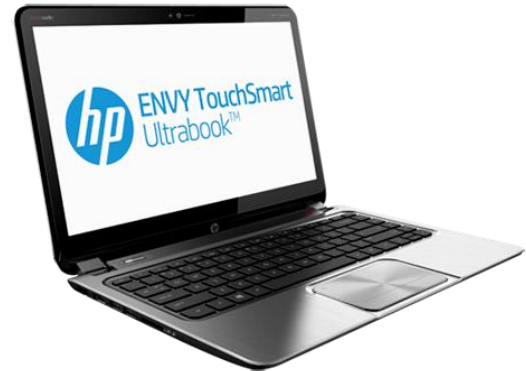
Intel HM77 Express

➤ **Hard Drive:**

Intel Smart Response and Rapid Start Technology
with 500 GB SATA (5400 rpm) and a 32GB mSATA

➤ **Pointing device:**

HP Image pad supporting Multi-Touch gestures with On/Off button



Latest Desktops

Dell Inspiron 2330 AIO

➤ **Processor:**

3rd gen Intel® Core™ i5-3330S processor (2.70 GHz with Turbo Boost 2.0 up to 3.20 GHz)

➤ **Memory (RAM):**

6GB DDR3 SO-DIMM AT 1600MHZ-1X2GB/1x4GB

➤ **Cache Memory L1/L2:**

6 MB

➤ **Video Card / Graphic Card:**

AMD Radeon HD 7650A 1GB DDR3

➤ **Sound Card:**

HD Audio w/ Waves MaxxAudio3 Integrated Basic Performance Speakers

➤ **Optical Drive:**

Blu-ray Combo Drive (BD-R, DVD+/-RW), Write to CD/DVD

➤ **Motherboard (Chipset):**

Intel V56

➤ **Hard Drive:**

Up to 1TB SATA hard drive (7200RPM)

➤ **Form Factor:**

All-in-One Desktop Computer



My Desktop : LG My pc (Studio Works)

➤ **Processor:**

Intel Pentium IV (4)

➤ **Memory (RAM):**

632 MB

➤ **Cache Memory L1/L2:**

1 MB

➤ **Video Card / Graphic Card:**

Not Present

➤ **Sound Card:**

Realtek Surround Audio

➤ **Optical Drive:**

DVD Writer Combo Drive (DVD+/-RW, CD+/-RW) 16x speed

➤ **Motherboard (Chipset):**

LGA Intel 775

➤ **Hard Drive:**

40 GB PATA HDD

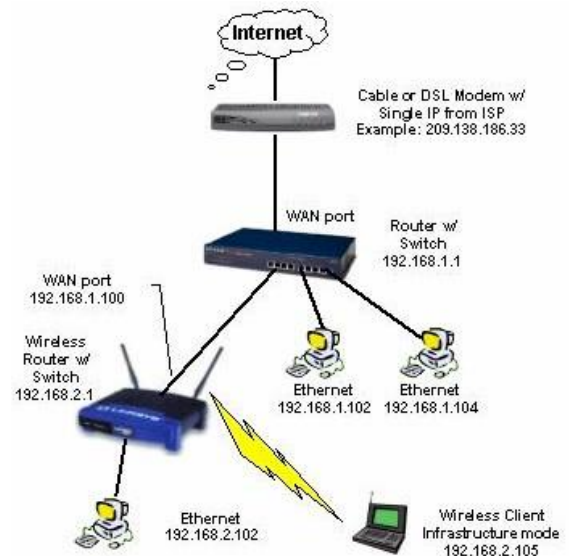


Experiment-2

Aim: Familiarization with different components of computer networking.

✓ ROUTERS:

A router is a device that forwards data packets between computer networks, creating an overlay internetwork. A router is connected to two or more data lines from different networks. When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination.



Types of Routers:

Edge Router: This type of router are placed at the edge of the ISP network, they are normally configured to external protocol like BGP (Border gateway protocol) to another BGP of other ISP or large organization.

Subscriber Edge Router: This type of router belongs to an end user (enterprise) organization. It's configured to broadcast External BGP to its provider's AS(s)

Inter-provider Border Router: This type of router is for Interconnecting ISPs, this is a BGP speaking router that maintains BGP sessions with other BGP speaking routers in other providers' ASes.

Core Router: A router that resides within the middle or backbone of the LAN network rather than at its periphery.

Wired and Wireless Routers: It is used in Home and small office networking is becoming popular by day by the use of IP wired and wireless router.

✓ **NETWORK SWITCH:**

A network switch is a computer networking device that links network segments or network devices. The term commonly refers to a multi-port network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3) and above are often called layer-3 switches or multilayer switches.



Types of Network Switch:

Managed Switches: A type of network switch in which different types of methods are used to manage the different parts of the network and can able to upgrade the working and the performance of the switch with the help of common methods of management is called as the managed network switch.

Unmanaged Network Switch: Basically these networking switches are designed for those customers that are not able to spend more money because those are less expensive. A type of network switch in which interface is not involved is called as unmanaged network switches. They are designed for the direct use.

Smart Switches: Basically the smart network switches are the important types of managed switches in which the specific management features are discussed. Typically these switches are used for the networking devices such as VLANs. They also increase the working ability of the parts connected by the switches

✓ **HUB:**

An Ethernet hub, active hub, network hub, repeater hub, multiport repeater or hub is a device for connecting multiple Ethernet devices together and making them act as a single network segment. It has multiple input/output (I/O) ports, in which a signal introduced at the input of any port appears at the output of every port except the original incoming. A hub works at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.



Types of Hub:

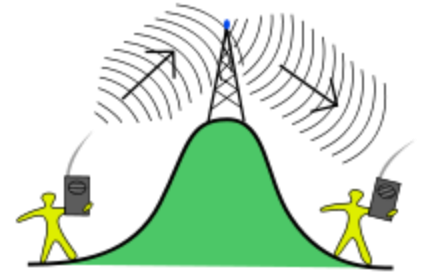
Passive Hub: The first type of the networking hub is the passive hub. Passive hub does not perform any particular function but it just behaves like a bridge between the cables of connection and just receives the information and forwards it with out any change in topology.

Active Hub: Second type of the networking hub is the active hub. This type of hub is quite similar to that of the passive hub but can perform the additional tasks. Active hubs are those hubs that can work as connector between two regions but also has ability to regenerate the information with the help of strong electrical signals. it is also called as the multi port repeater. It helps in the communication and can upgrade the properties of the signals before delivery.

Intelligent Hub: The third and the last type of the hub that can perform the both functions of the active and the passive hub are generally referred to as the intelligent hub. Basically this hub provides the opportunity to increase the speed of networking and also make the performance of the network efficient as compared to other devices. Addition to their specific work intelligent hubs can also perform the different functions that of routing, bridging etc.

✓ **REPEATER:**

A network repeater is a device used to expand the boundaries of a wired or wireless (Wi-Fi) local area network (LAN). A repeater is an electronic device that receives a signal and retransmits it at a higher level or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances. In the past, wired network repeaters were used to join segments of Ethernet cable. The repeaters would amplify the data signals before sending them on to the uplinked segment, thereby countering signal decay that occurs over extended lengths of wire. Modern Ethernet networks use more sophisticated switching devices, leaving the wireless flavor of the network repeater a more popular device for use with wireless LANs (WLANs) at work and home.



Types:

- An optical communications repeater is a piece of equipment that receives an optical signal, converts that signal into an electrical one, regenerates it, and then retransmits it as an optical signal. In contrast, optical amplifiers, which amplify the light beam directly, are often used in transcontinental and submarine communications cables, because the signal loss over such distances would be unacceptable without them.
- Radio repeaters are used in radio communication services.
- A digipeater is a blend meaning "digital repeater", particularly used in amateur radio.

Advantages:

- Makes it easy to expand a network over a large distance.
- Connection between various types of media [e.g. fiber optic, UTF, coaxial cable] is possible.

Disadvantages:

- Traffic cannot be filtered to ease congestion.
- A repeater cannot work across multiple network architectures.

✓ LAN ADAPTERS:

A network interface controller (also known as a network interface card, network adapter, LAN adapter and by similar terms) is a computer hardware component that connects a computer to a computer network.

Early network interface controllers were commonly implemented on expansion cards that plugged into a computer bus; the low cost and ubiquity of the Ethernet standard means that most newer computers have a network interface built into the motherboard.



Types of Network Adapters:

10/100 Ethernet: 10/100 Ethernet cards are networking cards that are used most frequently in the home or small office setting. As the name suggests, they are capable of speeds up to 10 or 100 megabits per second, not to be confused with megabytes per second.

Gigabit Ethernet: Gigabit Ethernet NICs provide network transfer speeds of up to one Gigabit per second. These cards connect to the computer using the same means as previously mentioned; however, they are much more likely to be produced for PCIe slots.

Fiber Optics: Major network infrastructures such as tier 1 and 2 Internet backbones require much more powerful NICs. Fiber optic NICs use fiber optic cabling to reach speeds of 10 gigabits per second currently, with a specification under review to push this limit to 100 gigabits per second.

Wireless NICs: Wireless networking has become very popular in the last few years, as of 2009. Wireless NICs provide the same networking capabilities as their wired counterparts; however, they have their own transfer capabilities.

Wireless Dongles: There is a wireless networking device used by individual machines that have access to a main computer that is connected to a wireless router. This wireless router allows the user to install wireless dongles instead of entire routers with each additional machine on the network.

Experiment-3

Aim: Familiarization with transmission media and tools.

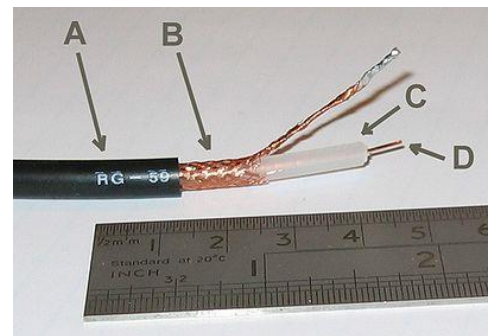
✓ Coaxial Cables:

Coaxial cable or **coax** is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.

Coaxial cable conducts electrical signal using an inner conductor (usually a solid copper, stranded copper or copper plated steel wire) surrounded by an insulating layer and all enclosed by a shield, typically one to four layers of woven metallic braid and metallic tape. The cable is protected by an outer insulating jacket

Applications:

Common applications of coaxial cable include video and CATV distribution, RF and microwave transmission, and computer and instrumentation data connections.



Connector Type:

These cables use an RF type connector. The ends of coaxial cables usually terminate with connectors. Coaxial connectors are designed to maintain a coaxial form across the connection and have the same impedance as the attached cable. Connectors are usually plated with high-conductivity metals such as silver or tarnish-resistant gold.



✓ **Twisted pair cable:**

Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of cancelling out electromagnetic interference (EMI) from external sources; for instance, electromagnetic radiation from unshielded twisted pair (UTP) cables, and crosstalk between neighbouring pairs.



In balanced pair operation, the two wires carry equal and opposite signals and the destination detects the difference between the two. This is known as differential mode transmission. Noise sources introduce signals into the wires by coupling of electric or magnetic fields and tend to couple to both wires equally. The noise thus produces a common-mode signal which is cancelled at the receiver when the difference signal is taken.

Different types include Shielded twisted pair, Screened twisted pair, Shielded foiled twisted pair etc.

Advantages:

- Differential signal introduces electromagnetic radiation from the cable, along with the associated attenuation allowing for greater distance between exchanges. It is a thin, flexible cable that is easy to string between walls.
- More lines can be run through the same wiring ducts.
- Electrical noise going into or coming from the cable can be prevented.
- Cross-talk is minimized

Connectors:

Twisted pair cables use many connectors including RJ-45 and DB 25.

✓ Optical Fiber Cable:

An optical fiber cable is a cable containing one or more optical fibers. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed.

Optical fiber consists of a core and a cladding layer, selected for total internal reflection due to the difference in the refractive index between the two. In Experiment fibers, the cladding is usually coated with a layer of acrylate polymer or polyimide. This coating protects the fiber from damage but does not contribute to its optical waveguide properties.



Optical cables transfer data at the speed of light in glass (slower than vacuum). This is typically around 180,000 to 200,000 km/s, resulting in 5.0 to 5.5 microseconds of latency per km. Typical modern multimode graded-index fibers have 3 dB/km of attenuation loss at 850 nm and 1 dB/km at 1300 nm.

Advantages:

Some advantages include:

- Fast transfer
- No sparking issues
- Immune to electromagnetic interference.

Disadvantages:

- Fragile
- Cost

Connectors:

It uses LC/PC and SC/PC connectors.



✓ **Connectors:**

An electrical connector is an electro-mechanical device for joining electrical circuits as an interface using a mechanical assembly. The connection may be temporary, as for portable equipment, require a tool for assembly and removal, or serve as a permanent electrical joint between two wires or devices.

There are hundreds of types of electrical connectors. Connectors may join two lengths of flexible copper wire or cable, or connect a wire or cable or optical interface to an electrical terminal.

Commonly Used connectors:

Plug and socket connectors:

Plug and socket connectors are usually made up of a male plug (typically pin contacts) and a female receptacle.



8P8C connector:

8P8C is short for "eight positions, eight conductors", and so an 8P8C modular connector (plug or jack) is a modular connector with eight positions, all containing conductors.



USB connectors:

The Universal Serial Bus is a serial bus standard to interface devices, founded in 1996. It is currently widely used among PCs, Apple Macintosh and many other devices. There are several types of USB connectors, and some have been added as the specification has progressed.



✓ **Crimping:**

A crimp connection is achieved with a type of solder less electrical connector.

Crimp connectors are typically used to terminate stranded wire. They fulfill numerous uses, including allowing the wires to be easily terminated to screw terminals, fast-on / quick-disconnect ,wire splices, various combinations of these. Crimp-on terminals are attached by inserting the stripped end of a stranded wire into a portion of the terminal, which is then mechanically deformed / compressed (crimped) tightly around the wire.

Advantages:

- Easier, cheaper, or faster to reproduce reliable connections in large-scale production.
- Fewer dangerous, toxic or harmful processes involved in achieving the connection (soldered connections require aggressive cleaning, high heat, and possibly toxic solders).
- Potentially superior mechanical characteristics due to strain relief and lack of solder wicking.

Crimping Tool:

Crimping pliers are a hand tool used to hold objects firmly, for bending, or physical compression. Generally, pliers consist of a pair of metal first-class levers joined at a fulcrum positioned closer to one end of the levers, creating short jaws on one side of the fulcrum, and longer handles on the other side. This arrangement creates a mechanical advantage, allowing the force of the hand's grip to be amplified and focused on an object with precision. The jaws can also be used to manipulate objects too small or unwieldy to be manipulated with the fingers.



Experiment-4

Aim: Implementation of file and printer sharing.

In computing, a shared resource or network share is a device or piece of information on a computer that can be remotely accessed from another computer, typically via a local area network or an enterprise Intranet, transparently as if it were a resource in the local machine.

Examples are shared file access (also known as *disk sharing* and *folder sharing*), shared printer access (*printer sharing*), shared scanner access, etc. The shared resource is called a *shared disk* (also known as mounted disk), *shared drive volume*, *shared folder*, *shared file*, *shared document*, *shared printer* or *shared scanner*.

The term file sharing traditionally means shared file access, especially in the context of operating systems and LAN and Intranet services, for example in Microsoft Windows documentation.^[1] Though, as Bit Torrent and similar applications became available in the early 2000s, the term file sharing increasingly has become associated with peer-to-peer file sharing over the Internet.

Difference from file transfer

Shared file access should not be confused with file transfer using the file transfer protocol (FTP), or the Bluetooth or IRDA OBJECT EXchange (OBEX) protocol. Shared access involves automatic synchronization of folder information whenever a folder is changed on the server, and may provide server side file searching, while file transfer is a more rudimentary service.

Shared file access is normally considered as a local area network (LAN) service, while FTP is an Internet service.

Shared file access is transparent to the user, as if it was a resource in the local file system, and supports a multi-user environment. This includes concurrency controller locking of a remote file while a user is editing it, and file system permissions.

Microsoft developed **specific file and print features** to meet widespread customer needs:

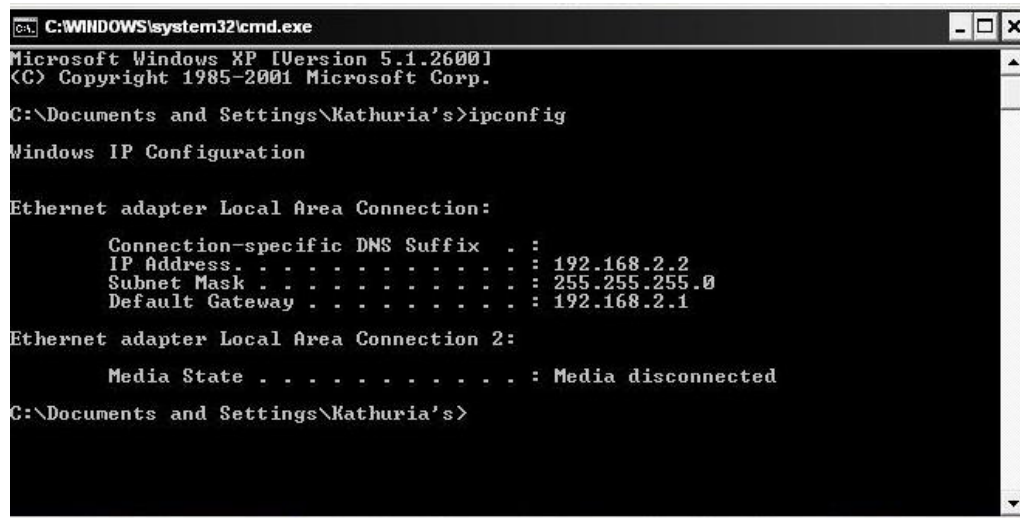
- Reduced cost. Remote Storage migrates infrequently used files to lower-cost secondary storage, yet keeps that data available if needed. Removable Storage helps reduce costs by letting multiple client applications share local libraries and tape or disk drives while ensuring that client applications do not corrupt each other's data.
- Better manageability. The improved NTFS file system, distributed file system (Dfs), and Indexing Service makes it easier to find and access files across expanding networks. New interfaces make operating system services easier to manage; for example, the new printer interface makes it simpler for both administrators and end-users to configure and manage their printing needs.
- Increased availability and reliability. Dfs replication and File Replication service (FRS) synchronization help keep data available to users, even if a server or disk drive fails or a shared folder or file becomes corrupted. Dynamic volumes formatted with NTFS 5 allow fewer reboots when adding disks and creating, extending, or mirroring a volume.
- Scalability. The Windows 2000 NTFS version 5 file system and the Windows 2000 storage subsystems let users efficiently store and retrieve ever-larger quantities of data.

ipconfig

In computing, ipconfig (*internet protocol configuration*) in Microsoft Windows is a console application that displays all current TCP/IP network configuration values and can modify Dynamic Host Configuration Protocol DHCP and Domain Name System DNS settings.

In most cases, the ipconfig command is used with the command-line switch /all. This results in more detailed information than ipconfig alone.

Use of ipconfig at PC 1



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Kathuria's>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

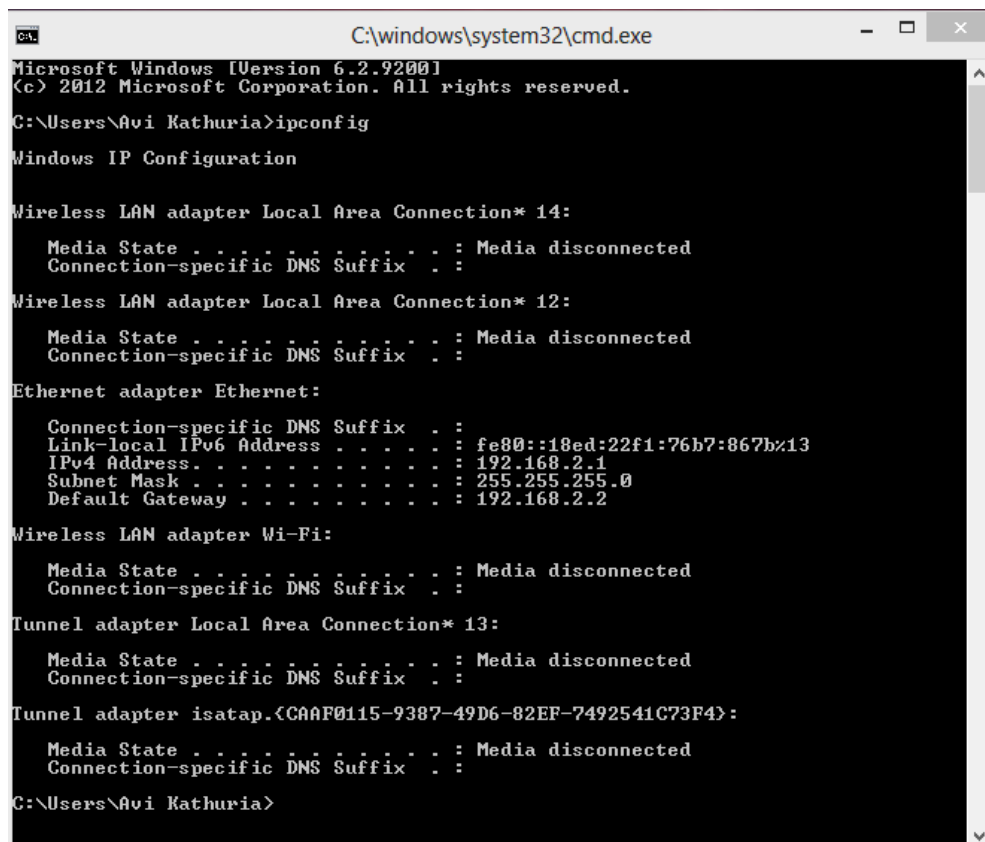
    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.2.2
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.2.1

Ethernet adapter Local Area Connection 2:

    Media State . . . . .             : Media disconnected

C:\Documents and Settings\Kathuria's>
```

Use of ipconfig at PC 2



```
C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Avi Kathuria>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 14:

    Media State . . . . .             : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 12:

    Media State . . . . .             : Media disconnected
    Connection-specific DNS Suffix  . : 

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::18ed:22f1:76b7:867b%13
    IPv4 Address. . . . .             : 192.168.2.1
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.2.2

Wireless LAN adapter Wi-Fi:

    Media State . . . . .             : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 13:

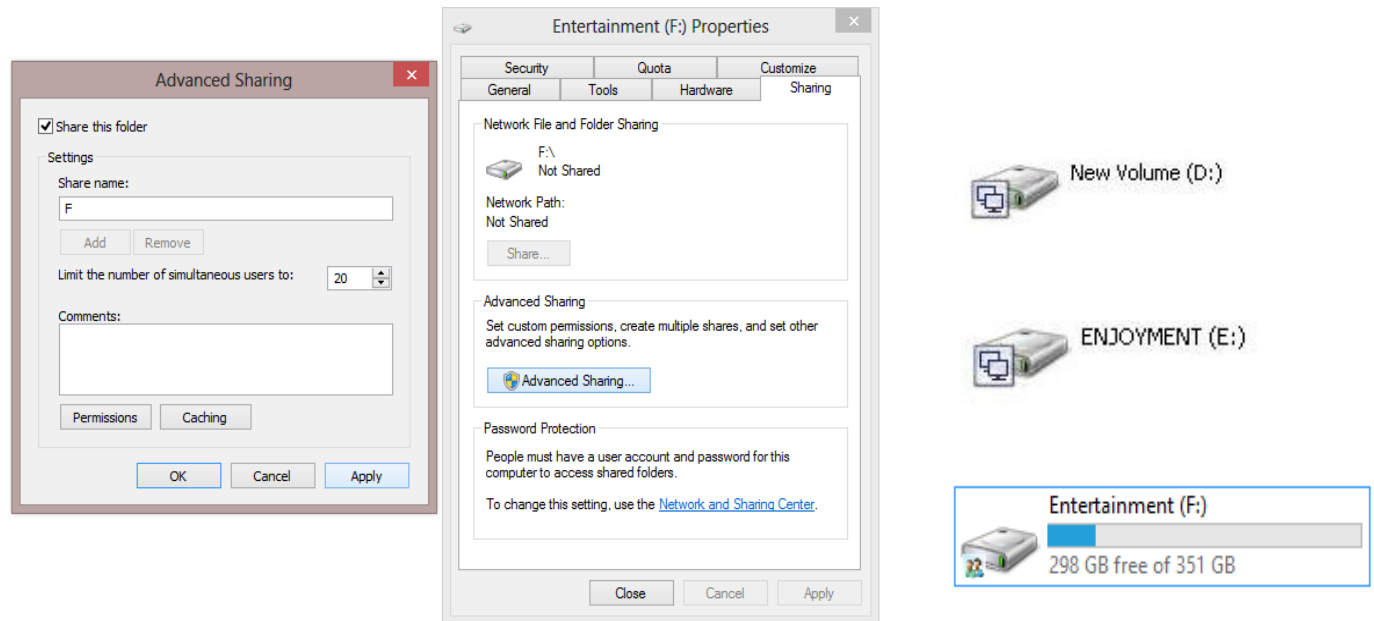
    Media State . . . . .             : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{CAAF0115-9387-49D6-82EF-7492541C73F4}:

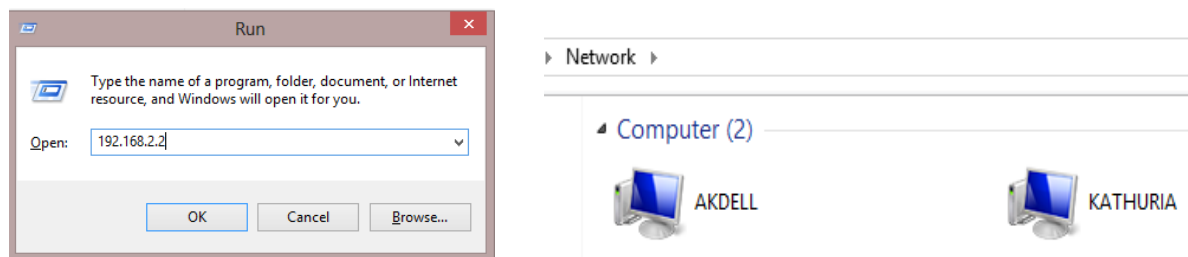
    Media State . . . . .             : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Avi Kathuria>
```

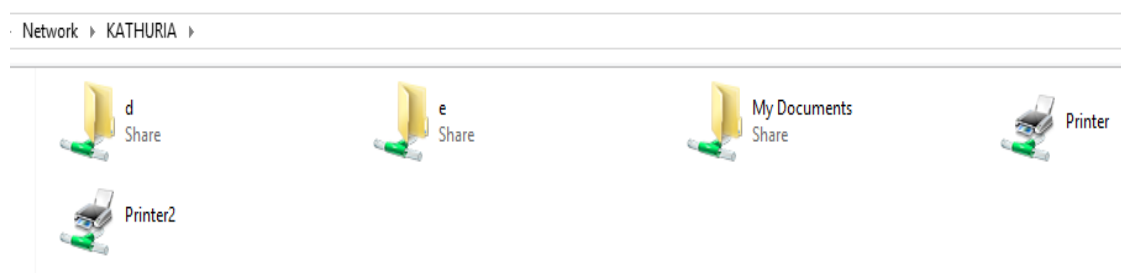

Enable Sharing Mode on Hard drives to share data between systems



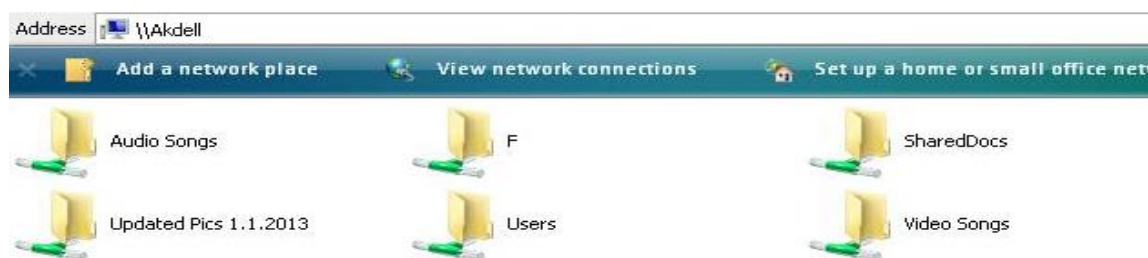
Use of run command line to get into destination ip address and showing linked systems



After Enabling sharing Mode at PC 1 data shared to PC2



Similarly after Enabling sharing Mode at PC 2 data shared to PC1



Experiment-5

Aim: Preparing straight and cross cables.

There are times when you want to transfer your important files and documents from one computer to another. Especially, if you are to manage multiple computers on your home network or a work group, transferring files between them becomes tedious. Though you can use the following alternatives to transfer data.

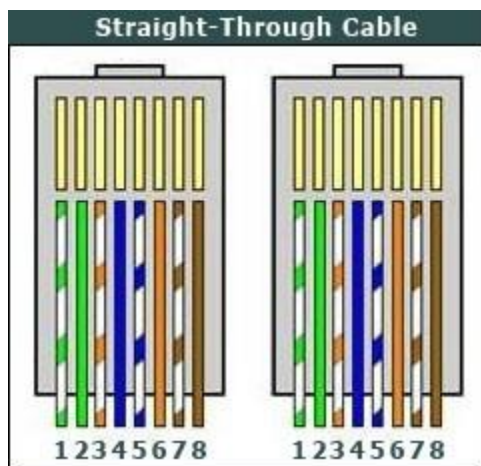
1. The mostly used media to transfer files or documents is removable disk (USB drive). But the drawback of the removable media is that if you want to transfer a large amount of data, you need to divide that in various parts as the total data would not fit in the limited space of your USB drive. It is also slow comparatively with the hard disk.

2. You can use Drop box to sync files across multiple computers. Drop box is a great tool but it is useless without an internet connection.

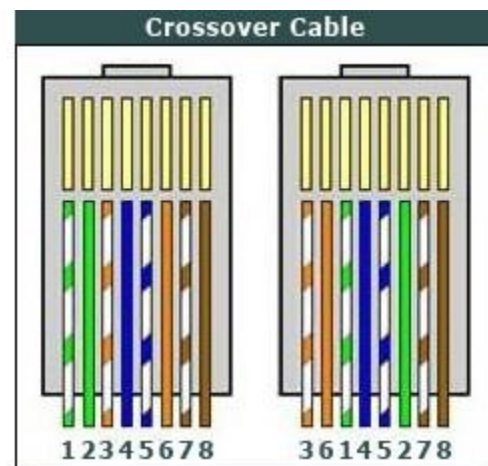
Hence, you should use a fast, reliable and all time available way. One of the best choices to transfer files between two Windows computers is connecting them with an Ethernet cable.

The Ethernet cable is nothing but a simple cable connected with RJ45 clips at both ends. But it comes with two different configurations.

1. Straight-through cable



2. Crossover cable.



You can see the configuration diagram of both types from the above image.

Where the crossover cable can be used only for file transferring, the straight-through cable can be used in various purposes.

Here I will discuss how to connect two Windows computers on LAN though an Ethernet crossover cable and how to transfer files, folders, videos, pictures, images etc. between them.

The steps below are general Ethernet Category 5 (commonly known as Cat 5) cable construction guidelines. For our example, we will be making a Category 5e patch cable, but the same general method will work for making any category of network cables.

1. Unroll the required length of network cable and add a little extra wire, just in case.

If a boot is to be fitted, do so before stripping away the sleeve and ensure the boot faces the correct way.



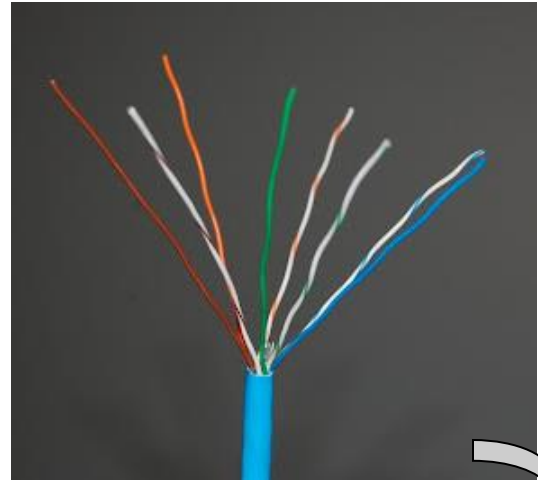
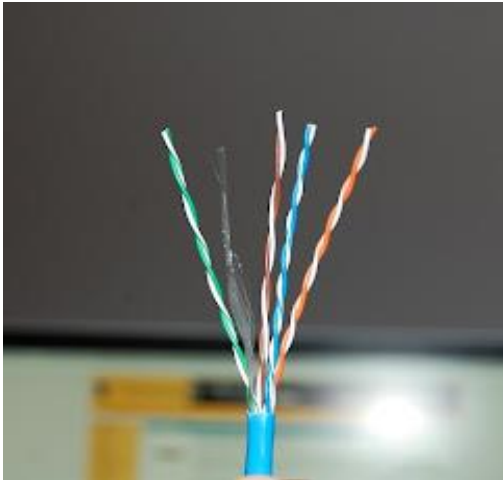
2. Carefully remove the outer jacket of the cable.

Be careful when stripping the jacket as to not nick or cut the internal wiring. One good way to do this is to cut lengthwise with snips or a knife along the side of the cable, away from you, about an inch toward the open end. This reduces the risk of nicking the wires' insulation. Locate the string inside with the wires, or if no string is found, use the wires themselves to unzip the sheath of the cable by holding the sheath in one hand and pulling sideways with the string or wire. Cut away the unzipped sheath and cut the twisted pairs about 1 1/4" (30 mm). You will notice 8 wires twisted in 4 pairs. Each pair will have one wire of a certain color and another wire that is white with a colored stripe matching its partner (this wire is called a tracer).

3. Inspect the newly revealed wires for any cuts or scrapes that expose the copper wire inside.

If you have breached the protective sheath of any wire, you will need to cut the entire segment of wires off and start over at step one. Exposed copper wire will lead to cross-talk, poor performance or no connectivity at all. It is important that the jacket for all network cables remains intact.





4. Untwist the pairs so they will lay flat between your fingers.

The white piece of thread can be cut off even with the jacket and disposed (see Warnings). For easier handling, cut the wires so that they are 3/4" (19 mm) long from the base of the jacket and even in length.

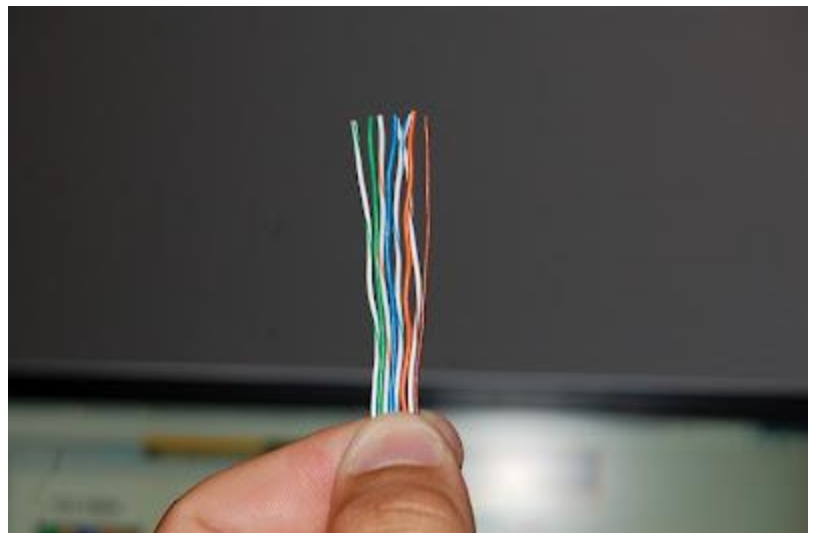
5. Arrange the wires based on the wiring specifications you are following. There are two methods set by the TIA, 568A and 568B. Which one you use will depend on what is being connected. A straight-through cable is used to connect two different-layer devices (e.g. a hub and a PC). Two **like** devices normally require a cross-over cable. The difference between the two is that a straight-through cable has both ends wired identically with 568B, while a cross-over cable has one end wired 568A and the other end wired 568B. For our demonstration in the following steps, we will use 568B, but the instructions can easily be adapted to 568A.

- 568B – Put the wires in the following order, from left to right:

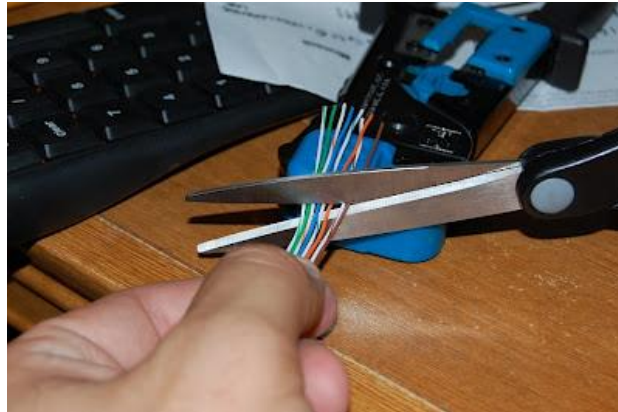
- white orange
- orange
- white green
- blue
- white blue
- green
- white brown
- brown

- 568A – from left to right:

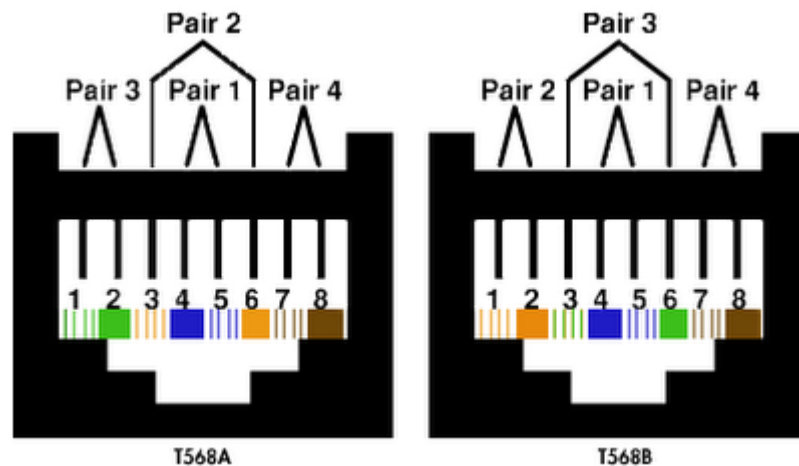
- white/green
- green
- white/orange
- blue
- white/blue
- orange
- white/brown
- brown



With the wires straight and in the correct order, use your scissors to cut off the excess wire, leaving approximately one inch of the wire exposed. Take care to cut the wires straight on the end, as close to a 90 degree cut as possible. This matters greatly when you install the RJ45 on the end.

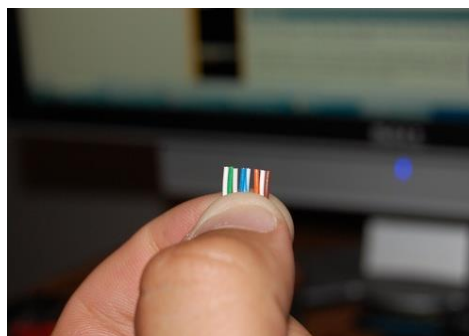


6. You can also use the mnemonic 1-2-3-6/3-6-1-2 to remember which wires are switched.



7. Press all the wires flat and parallel between your thumb and forefinger.

Verify the colors have remained in the correct order. Cut the top of the wires even with one another so that they are 1/2" (12.5 mm) long from the base of the jacket, as the jacket needs to go into the 8P8C connector by about 1/8", meaning that you only have a 1/2" of room for the individual cables. Leaving more than 1/2" untwisted can jeopardize connectivity and quality. Ensure that the cut leaves the wires even and clean; failure to do so may cause the wire not to make contact inside the jack and could lead to wrongly guided cores inside the plug.



8. Keep the wires flat and in order as you push them into the RJ-45 plug with the flat surface of the plug on top.

The white/orange wire should be on the left if you're looking down at the jack. You can tell if all the wires made it into the jack and maintain their positions by looking head-on at the plug. You should be able to see a wire located in each hole, as seen at the bottom right. You may have to use a little effort to push the pairs firmly into the plug. The cabling jacket should also enter the rear of the jack about 1/4" (6 mm) to help secure the cable once the plug is crimped. You may need to stretch the sleeve to the proper length. Verify that the sequence is still correct before crimping.



9. Place the wired plug into the crimping tool.

Carefully place the RJ45 on the end of the cable and push the wires into the module as far as possible. This ensures that the 8 gold prongs inside of the RJ45 cut into the wires and make a good connection. When the RJ45 is in place and the cables all look good, insert the module into your crimps and squeeze the handles together. Many crimps will make a clicking sound when you have applied the correct amount of pressure. This is an easy way to avoid squeezing too hard and risk damaging the RJ45.

10. Final Loop Of The Wire After Cramping:

Once crimped, take a second to look over your creation and marvel at its simple beauty. When admiring, make sure to look closely at two areas. On the top of the RJ45, you should observe all eight ends of the wires sitting against the inside of the RJ45. If this is not the case, you will more than likely need to cut that module off and start back over at step 1. The cold pins inside the RJ45 cut into the wires and make the necessary connection. If the wires are not completely up to the end, the connection might not be made, rendering your cable useless.



You can also look at the side of the RJ45. This will give you a clear view of the outside most wire. In this case, the green and white wire is visible from the end. Another thing that you need to keep an eye on is the sheathing. It needs to be far enough toward the end that the wedge inside the RJ45 comes down and traps it inside the module. This isn't overly important from a functionality perspective but you should always try to be as professional as possible and over time, after many connections and unhooking, your cable should last longer with the sheathing locked firmly in place.



11. Test the cable to ensure that it will function in the field

Mis-wired and incomplete network cables could lead to headaches down the road. In addition, with power-over-Ethernet (PoE) making its way into the market place, crossed wire pairs could lead to physical damage of computers or phone system equipment, making it even more crucial that the pairs are in the correct order. A simple cable tester can quickly verify that information for you. Should you not have a network cable tester on hand, simply test connectivity pin to pin.

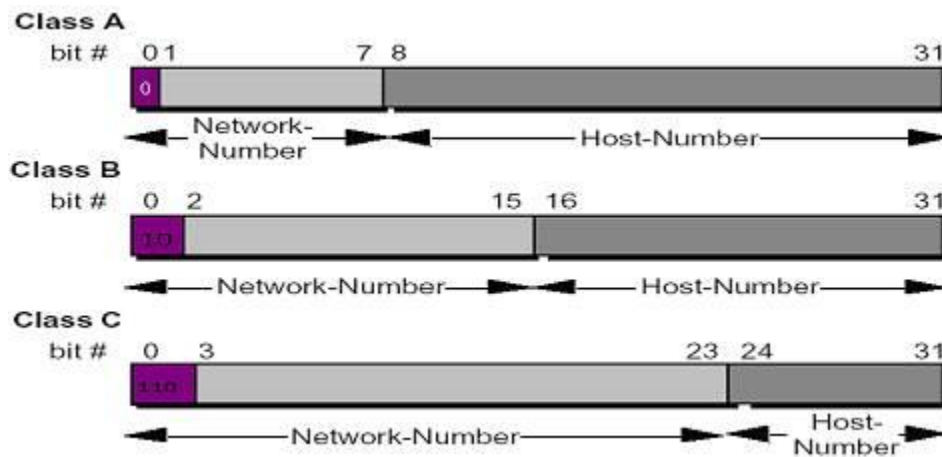


Experiment-6

Aim: Designing and implementing Class A, B, C Networks.

Network Classes

The Internet community originally defined five address classes to accommodate networks of varying sizes. Microsoft TCP/IP supports class A, B, and C addresses assigned to hosts. The class of address defines which bits are used for the network ID and which bits are used for the host ID. It also defines the possible number of networks and the number of hosts per network.



Fig

A *network*, in the context of the discussion of internets, is a collection of systems that have the same network number. There are three classes of internet networks defined for TCP/IP internets as illustrated in Figure 1.

Figure : Network classes

	Example of IP Address	Network Address	Host Address
Class A	45.111.222.101	Network (8 Bits) 45	Host (24 bits) 111.222.101
Class B	140.123.222.101	Network (16 Bits) 140.123	Host (16 Bits) 222.101
Class C	200.123.222.101	Network (24 Bits) 200.123.222	Host (8 Bits) 101

Or, said another way:

For	the network portion is	The first byte can be between	Example
Class A networks	first byte	0 and 127	3.2.5.3
Class B networks	first two bytes	128 and 191	128.7.2.1
Class C networks	first three bytes	192 and 255	195.3.2.1

Class A Networks

Class A networks use the high order byte of the internet address for the network number. The remaining 3 bytes of address information define the host number on the network.

Class A networks always have the high order bit of the network number 0, to distinguish them from other network classes. Thus, there can only be 127 class A networks, but each network can have up to 16,777,215 hosts.

Class B Networks

Class B networks use two bytes for the network number and two bytes for the host number. The two high order bits of a class B network number are "10" to distinguish them from other network classes. Thus, there are up to 16,383 networks of up to 65,535 hosts each.

Class C Networks

Class C networks use three bytes for the network number and one byte for the host number. The two high order bits of the network number are "11" to distinguish the address from other network classes. Thus, there can be up to 4,194,303 networks of up to 255 hosts each.

Class D Networks

Class D addresses are reserved for IP multicast addresses. The four high-order bits in a class D address are always set to binary 1 1 1 0. The remaining bits are for the address that interested hosts recognize. Microsoft supports class D addresses for applications to multicast data to multicast-capable hosts on an internetwork.

Class E Networks

Class E is an experimental address that is reserved for future use. The high-order bits in a class E address are set to 1111

Network Number, Host Number, and Broadcast Address Conventions

By convention, there are actually two fewer internet addresses than the quantities given above. Addresses of all 1-bits (255) or all 0-bits (0) are reserved, so they are not normally available as host or network addresses.

Network Numbers

A network number is an internet address with the host number all 0-bits. For example, the following are all network numbers:

- 7.0.0.0 is a Class A internet network.
- 135.47.0.0 is a Class B internet network.
- 192.47.231.0 is a Class C internet network.

Host Numbers

Host numbers are the converse of network numbers; the high order portion of the address is all 0-bits. Here are some sample host numbers:

- 0.231.47.7 is a host number on a Class A network.
- 0.0.47.7 is a host number on a Class B network.
- 0.0.0.7 is a host number on a Class C network.

Host numbers are rarely used without their accompanying network number.

Broadcast Addresses

Normally, an internet address refers to a single host. The broadcast address refers to all hosts on a network, and is an address with the host portion of the address all 1-bits. Applied to the network numbers in the previous example, we have the following broadcast addresses for each network:

- 7.255.255.255
- 135.47.255.255
- 192.47.231.255

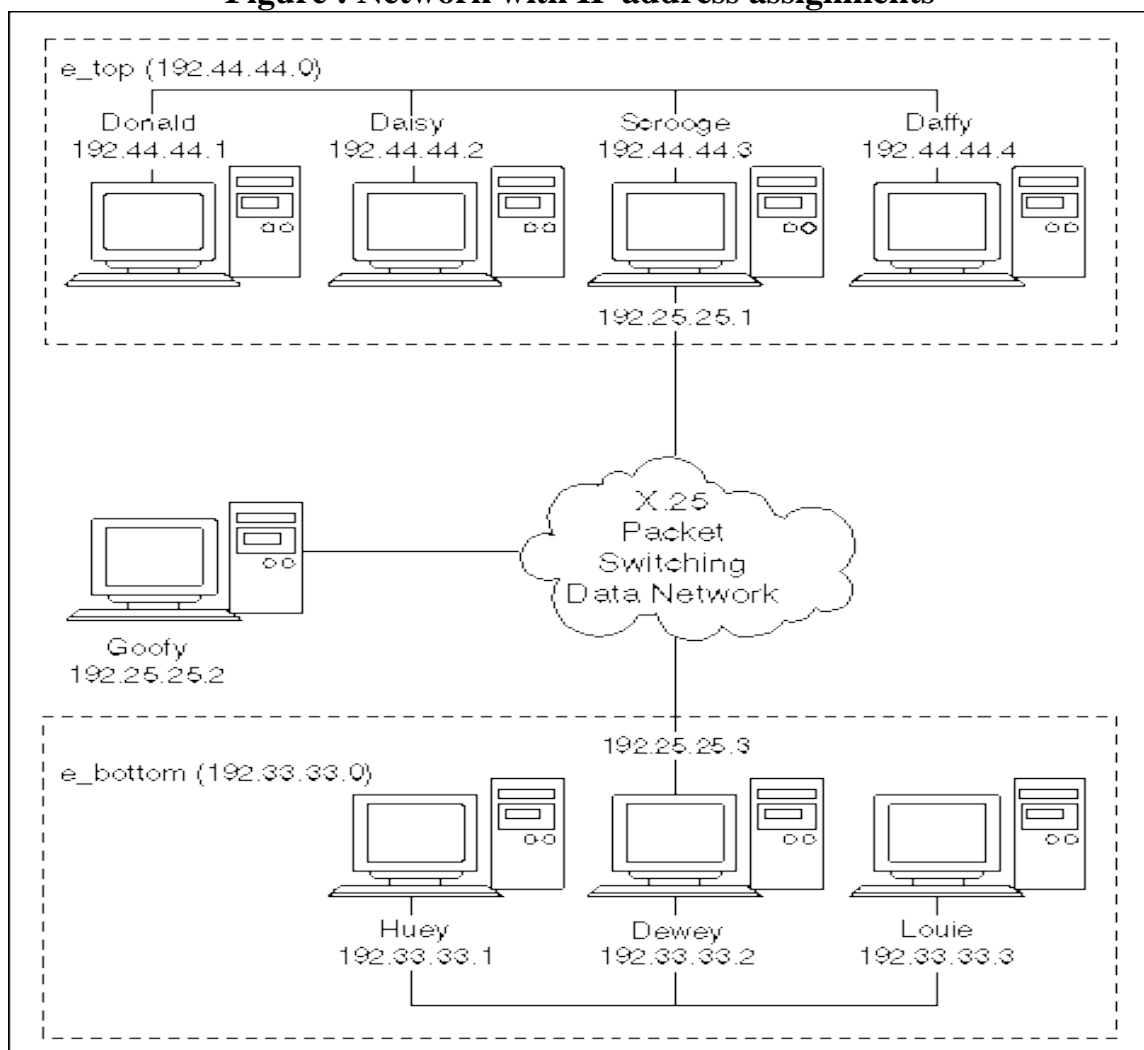
When the network number of the broadcast address is also all 1 (255.255.255.255), the packet applies only to the local network. A broadcast address with a specific network number (such as those in the list above) refers to the network identified, which does not need to be connected directly to the local network.

Implementation

TCP/IP implementations and TCP/IP addressing conventions are the result of experience gained in the design and operation of the Internet. If during your design, you ignore or contravene an Internet convention, your network may not work.

Network name	Network address	Host name	Host address
e_top	192.44.44.0	Donald	192.44.44.1
		Daisy	192.44.44.2
		Scrooge	192.44.44.3
		Daffy	192.44.44.4
wan	192.25.25.0	Wan_Scrooge	192.25.25.1
		Goofy	192.25.25.2
		Wan_Dewey	192.25.25.3
e_bottom	192.33.33.0	Huey	192.33.33.1
		Dewey	192.33.33.2
		Louie	192.33.33.3

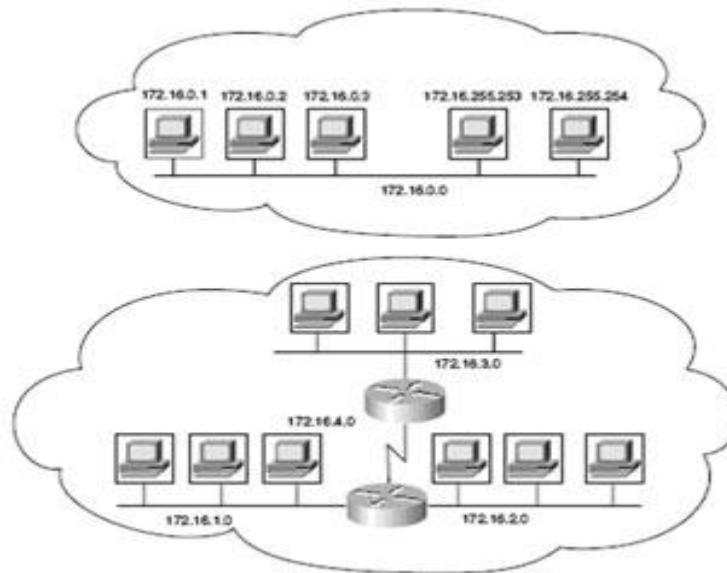
Figure : Network with IP address assignments



Experiment-7

Aim: Subnet planning and its implementation.

Without subnets, the organization operates as a single network. These flat topologies result in short routing tables but, as the network grows, the use of bandwidth becomes inefficient. (All systems on the network receive all the broadcasts on the network.) Network addressing can be made more efficient by breaking the addresses into smaller segments, or subnets. Subnetting provides additional structure to an addressing scheme without altering the addresses. In the figure, the network address 172.16.0.0 is subdivided into four subnets: 172.16.1.0, 172.16.2.0, 172.16.3.0, and 172.16.4.0. If traffic were evenly distributed to each end station, the use of subnetting would reduce the overall traffic seen by each end station by 75 percent.



Subnet Mask

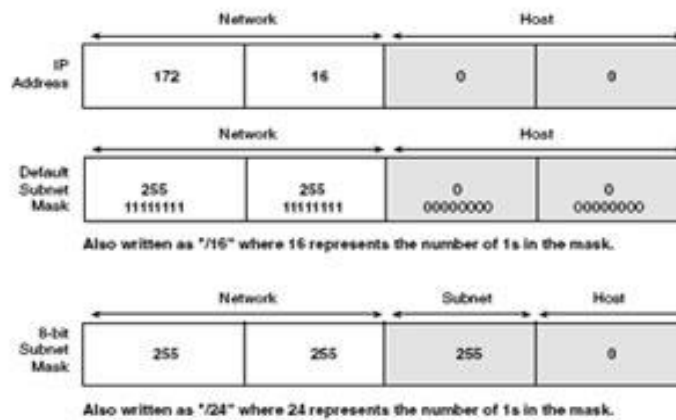
A *subnet mask* is a 32-bit value written as four octets. In the subnet mask, each bit determines how the corresponding bit in the IP address should be interpreted (network, subnet, or host). The subnet mask bits are coded as follows:

- ✓ Binary 1 for the network bits
- ✓ Binary 1 for the subnet bits
- ✓ Binary 0 for the host bits

Although dotted decimal is the most common format, the subnet can be represented in several ways:

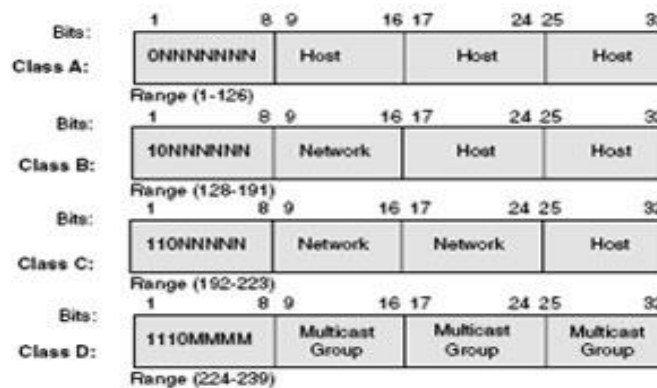
- ✓ **Dotted decimal**—172.16.0.0 255.255.0.0
- ✓ **Bit count**—172.16.0.0/16
- ✓ **Hexadecimal**—172.16.0.0 0xFFFF0000

The ipnetmask-format command can be used to specify the format of network masks for the current session. Dotted decimal is the default.



Default Subnet Masks

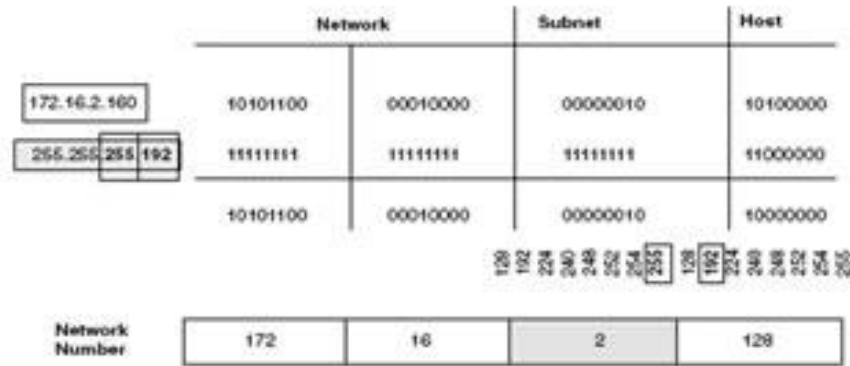
Each address class has a default subnet mask. The default subnet masks only the network portion of the address, the effect of which is no subnetting. With each bit of subnetting beyond the default, you can create $2^n - 2$ subnets. These examples show the effect of adding subnet bits.



Address	Subnet Address	Number of Subnets	Comments
10.5.22.5/8	255.0.0.0	0	This is the default Class A subnet address. The mask includes only the network portion of the address and provides no additional subnets.
10.5.22.5/16	255.255.0.0	254	This Class A subnet address has 16 bits of subnetting, but only the bits in the second octet (those beyond the default) contribute to the subnetting.
155.13.22.11/16	255.255.0.0	0	In this case, 16 bits are also used for subnetting, but because the default for a Class B address is 16 bits, no additional subnets are created.
155.13.10.11/26	255.255.255.192	1022	In this case, there is a total of 26 bits of subnetting, but the Class B address can use only 10 of them to create subnets. The result is the creation of 1024 subnets ($2^{10} - 2$).

How Routers Use Subnet Masks

To determine an address's subnet, a router performs a logical AND operation with the IP address and subnet mask. Recall that the host portion of the subnet mask is all 0s. The result of this operation is that the host portion of the address is removed, and the router bases its decision on only the network portion of the address. In the figure, the host bits are removed, and the network portion of the address is revealed. In this case, a 10-bit subnet address is used, and the network (subnet) number 172.16.2.128 is extracted.



Broadcast Addresses

Broadcast messages are sent to every host on the network. There are three kinds of broadcasts:

- ✓ Directed broadcasts—you can broadcast to all hosts within a subnet and to all subnets within a network. (170.34.2.255 sends a broadcast to all hosts in the 170.34.2.0 subnet.)
- ✓ Hop count is used as the metric for path selection (the maximum is 15).
- ✓ Flooded broadcasts (255.255.255.255)—Local broadcasts within a subnet.
- ✓ You can also broadcast messages to all hosts on all subnets within a single network. (170.34.255.255 sends a broadcast to all subnets in the 170.34.0.0 network.)

Identifying Subnet Addresses

Given an IP address and subnet mask, you can identify the subnet address, broadcast address, first usable address, and last usable address using this method:

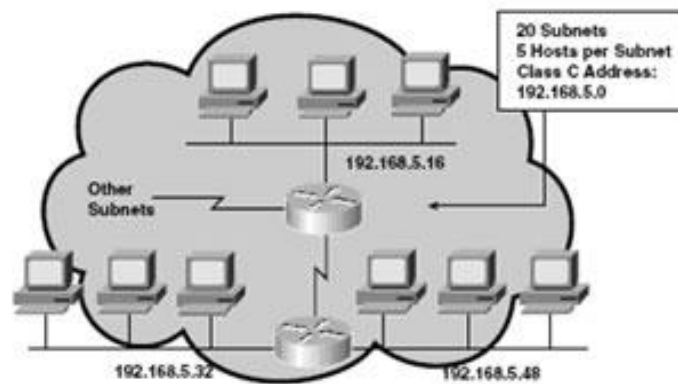
- ✓ Write down the 32-bit address. Directly below that, write down the subnet mask.
- ✓ Draw a vertical line just after the last 1 bit in the subnet mask.
- ✓ Copy the portion of the IP address to the left of the line. Place all 0s for the remaining free spaces to the right. This is the subnet number.
- ✓ Copy the portion of the IP address to the left of the line. Place all 1s for the remaining free spaces to the right. This is the broadcast address.
- ✓ Copy the portion of the IP address to the left of the line. Place all 0s in the remaining free spaces until you reach the last free space. Place a 1 in that free space. This is your first usable address.
- ✓ Copy the portion of the IP address to the left of the line. Place all 1s in the remaining free spaces until you reach the last free space. Place a 0 in that free space. This is your last usable address.

	174	24	4	176	
174.24.4.176	10101110	00011000	00000100	10110000	Host
255.255.255.192	11111111	11111111	11111111	11000000	Mask
174.24.4.128	10101110	00011000	00000100	10000000	Subnet
174.24.4.191	10101110	00011000	00000100	10111111	Broadcast
174.24.4.129	10101110	00011000	00000100	10000001	First
174.24.4.190	10101110	00011000	00000100	10111110	Last

How to Implement Subnet Planning

Subnetting decisions should always be based on growth estimates rather than current needs. To plan a subnet, follow these steps:

- Determine the number of subnets and hosts for each subnet required.
- The address class you are assigned and the numbers of subnets required determine the number of subnetting bits used. For example, with a Class C address and a need for 20 subnets, you will have a 29-bit mask (255.255.255.248). This allows for the Class C default 24-bit mask and 5 bits required for 20 subnets. (The formula $2^n - 2$ yields only 14 subnets for 4 bits, so 5 bits must be used.)
- The remaining bits in the last octet are used for the host field. In this case, each subnet has $2^3 - 2$, or 6 hosts.
- The final host addresses are a combination of the network/subnet plus each host value. The hosts on the 192.168.5.32 subnet would be addressed as 192.168.5.33, 192.168.5.34, 192.168.5.35, and so forth.



Implementing Subnet Planning Summary

- ✓ Breaking up networks into smaller segments (or subnets) improves network efficiency and conserves IP addresses.
- ✓ A 32-bit subnet mask determines the boundary between the subnet host portions of the IP address using 1s and 0s.
- ✓ A subnet defines a broadcast domain in a routed network.
- ✓ Cisco IOS Software supports directed, local network, and subnet broadcasts.
- ✓ Subnet planning should be based on future growth predictions rather than current needs.

Experiment-8

Aim: Study of various LAN topologies and their creation using network devices, cables and computers.

What is a Topology?

- Network topologies describe the ways in which the elements of a network are mapped. They describe the physical and logical arrangement of the network nodes.
- The physical topology of a network refers to the configuration of cables, computers, and other peripherals

Different Types of Topologies

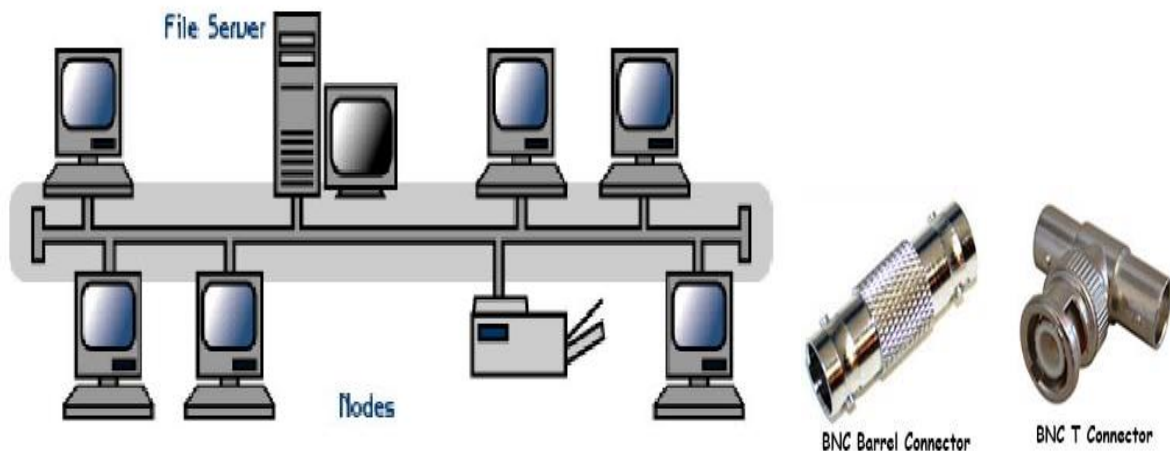
- Bus Topology
- Star Topology
- Ring Topology
- Mesh Topology
- Tree Topology
- Hybrid Topology

Bus Topology

- All the nodes (file servers, workstations, and peripherals) on a bus topology are connected by one single cable.
- A bus topology consists of a main run of cable with a terminator at each end. All nodes (file server, workstations, and peripherals) are connected to the linear cable.
- Popular on LANs because they are inexpensive and easy to install.

Uses a trunk or backbone to which all of the computers on the network connect.

- Systems connect to this backbone using T connectors or taps.
- Coaxial cablings (10Base-2, 10Base5) were popular options years ago.



Advantages of Bus Topology

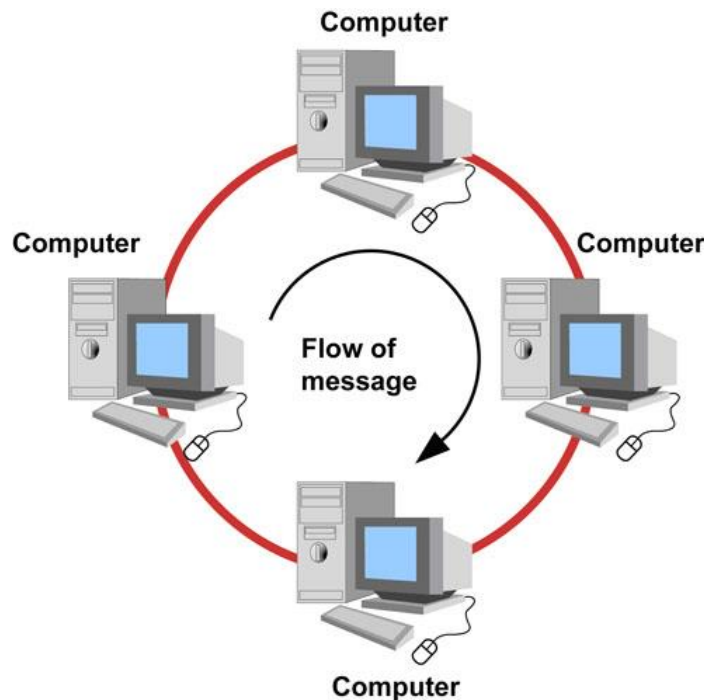
- It is Cheap, easy to handle and implement.
- Require less cable
- It is best suited for small networks.

Disadvantages of Bus Topology

- The cable length is limited. This limits the number of stations that can be connected.
- This network topology can perform well only for a limited number of nodes.
- Difficult to troubleshoot

Ring Topology

- In a ring network, every device has exactly two neighbours for communication purposes.
- All messages travel through a ring in the same direction.
- A failure in any cable or device breaks the loop and can take down the entire network.
- To implement a ring network we use the Token Ring technology
- A token, or small data packet, is continuously passed around the network. When a device needs to transmit, it reserves the token for the next trip around, and then attaches its data packet to it.



Advantage of Ring Topology

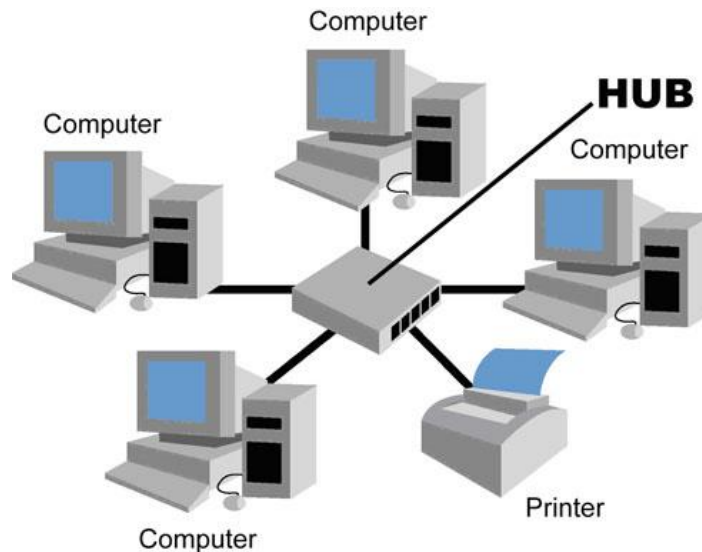
- Very orderly network where every device has access to the token and the opportunity to transmit.
- Easier to Manage than a Bus Network
- Good Communication over long distances
- Handles high volume of traffic
- Cable faults are easily located, making troubleshooting easier

Disadvantages of Ring Topology

- The failure of a single node of the network can cause the entire network to fail.
- The movement or changes made to network nodes affects the performance of the entire network.

Star Topology

- In a star network, each node (file server, workstations, and peripherals) is connected to a central device called a hub.
- The hub takes a signal that comes from any node and passes it along to all the other nodes in the network.
- Data on a star network passes through the hub, switch, or concentrator before continuing to its destination.
- The hub, switch, or concentrator manages and controls all functions of the network.
- The star topology reduces the chance of network failure by connecting all of the systems to a central node.



Advantages of Star Topology

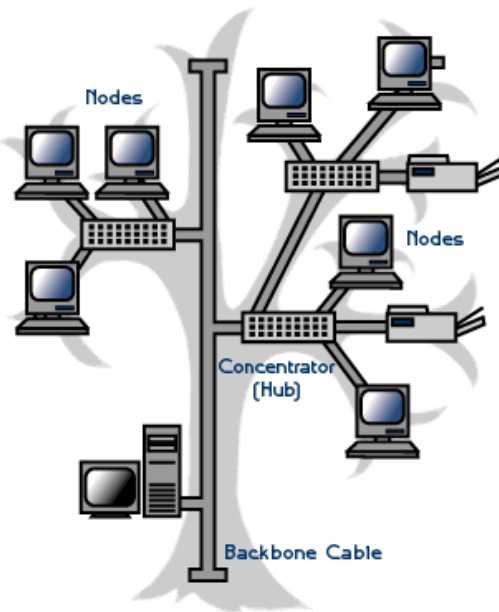
- Easy to manage
- Easy to locate problems (cable/workstations)
- Easier to expand than a bus or ring topology.
- Easy to install and wire.
- Easy to detect faults and to remove parts.

Disadvantages of Star Topology

- Requires more cable length than a linear topology.
- If the hub or concentrator fails, nodes attached are disabled.
- More expensive because of the cost of the concentrators.

Tree Topology

- A tree topology (hierarchical topology) can be viewed as a collection of star networks arranged in a hierarchy.
- This tree has individual peripheral nodes which are required to transmit to and receive from one other only and are not required to act as repeaters or regenerators.
- The tree topology arranges links and nodes into distinct hierarchies in order to allow greater control and easier troubleshooting.
- This is particularly helpful for colleges, universities and schools so that each of the connect to the big network in some way.



Advantages of a Tree Topology

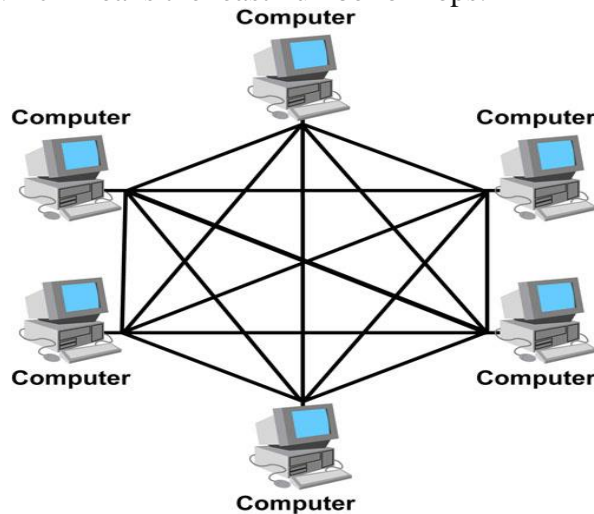
- Point-to-point wiring for individual segments.
- Supported by several hardware and software vendors.
- All the computers have access to the larger and their immediate networks.

Disadvantages of a Tree 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.

Mesh Topology

- In this topology, each node is connected to every other node in the network.
- Implementing the mesh topology is expensive and difficult.
- In this type of network, each node may send message to destination through multiple paths.
- While the data is travelling on the Mesh Network it is automatically configured to reach the destination by taking the shortest route which means the least number of hops.



Advantage of Mesh Topology

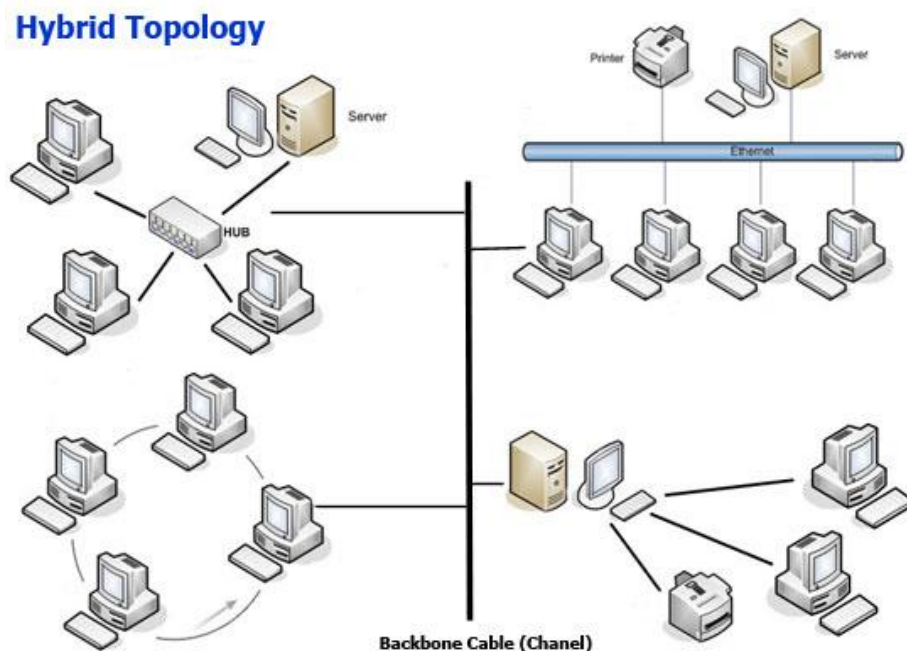
- No traffic problem as there are dedicated links.
- It has multiple links, so if one route is blocked then other routes can be used for data communication.
- Points to point links make fault identification easy.

Disadvantage of Mesh Topology

- There is mesh of wiring which can be difficult to manage.
- Installation is complex as each node is connected to every node.
- Cabling cost is high.

Hybrid Topology

- A combination of any two or more network topologies.
- A hybrid topology always accrues when two different basic network topologies are connected.
- It is a mixture of above mentioned topologies. Usually, a central computer is attached with sub-controllers which in turn participate in a variety of topologies



Advantages of a Hybrid Topology

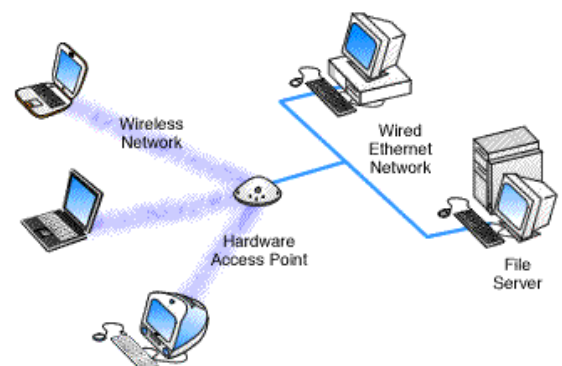
- It is extremely flexible.
- It is very reliable.

Disadvantages of a Hybrid Topology

- Expensive

Wireless networking

- Do not require physical cabling
- Particularly useful for remote access for laptop users
- Eliminate cable faults and cable breaks.
- Signal interference and security issue.



Advantages	Disadvantages
Allows for wireless remote access	Potential security issues associated with wireless transmissions
Network can be expanded without disruption to current users	Limited speed in comparison to other network topologies

Standard	Speed	Physical Topology	Logical Topology	Media	Access Method
802.3	10Mbps		Bus and Star	Coaxial and Twisted pair	CSMA/CD
(802.3u)	100Mbps(Fast Ethernet)	Star	Bus	Twisted pair	CSMA/CD
(802.3z)	1000Mbps	Star	Bus	Twisted pair	CSMA/CD
802.5	4Mbps and 16Mbps	Star	Ring	Twisted pair	Token passing
802.11b	11Mbps	Wireless	Bus	Radio waves	CSMA/CA
FDDI	100Mbps	Dual Ring	Ring	Fiber-optic Twisted pair/CDDI	Token passing

Major Bus Implementation Architectures

- 10Base2
 - 10Base5
 - 10BaseT
 - 100BaseTX
 - 1000BaseT
- Although this represents a logical bus topology, it is implemented physically in the form of a star topology
 - 10Base2 and 10Base5
 - Logical bus and Physical bus
 - 10BaseT
 - Logical bus and Physical star
 - 100BaseTx
 - Logical bus and physical star
 - Fast Ethernet LAN



Thin coaxial cable



T connector



Terminator



Network Interface Card

Network Topology Comparison

Topology	Information Transfer	Setup	Expansion	Troubleshooting	Cost	Cabling Concerns
Star Bus Each computer connects to a central connection device.	All information passes through the central network connection.	Each computer must be close to the central device. 100 meters maximum cable length. Up to 24 computers per network.	Add a new computer by plugging in a new cable from the computer to the connection device.	When one computer goes down, the rest of the network is unaffected. If the connection device goes down, then the network is down.	More expensive of the simple topologies, it requires costly connection device. Usually cheaper than a hybrid network.	Uses twisted pair cable. Requires large amounts of cable. No more than 100 meters from the computer to the connection device.
Bus Single cable connects everything.	One computer at a time sends information. Information goes along the cable and the computer accesses the information off the cable.	Connect the cable from one computer to the next and so on to the end. A terminator is placed at each end of the network.	To add a computer, you must shut down the network and disconnect the cable from the existing computers.	If one computer malfunctions, the entire network goes down.	A cheaper network since there is usually one continuous copper cable.	Single continuous cable connects the devices. Terminator is required at each end of the cable. Uses coaxial or twisted pair cabling.
Ring Single cable configured in a ring.	Information goes in one direction around the ring and passes along the ring until it reaches the correct computer.	Computers are located close to each other. Setup is easy. There is no connector. The ring has no beginning and no end.	Cable between the computers must be broken to add a new computer, so the network is down until the new device is back online.	If there's a break in the cable or an error in the network, information continues to transfer through the rest of the ring until reaching the point of the break. This makes troubleshooting easy.	One of the more expensive topologies due to high cable costs.	Requires more cabling than other topologies. Uses twisted pair.
Hybrid Mesh Combines two or more different structures.	Often used across long distances. Information transfer can happen in different ways, depending on the other topologies.	Often created when expanding an existing network. Can use a variety of connection devices.	Connection devices make combining different networks and different topologies easy.	Troubleshooting is most difficult in this topology because of the variety of technologies.	Expensive, large, and usually complicated.	Cabling depends on the types of networks. Can use twisted pair and coaxial cable. Also incorporates fiber optic cabling over long distances.

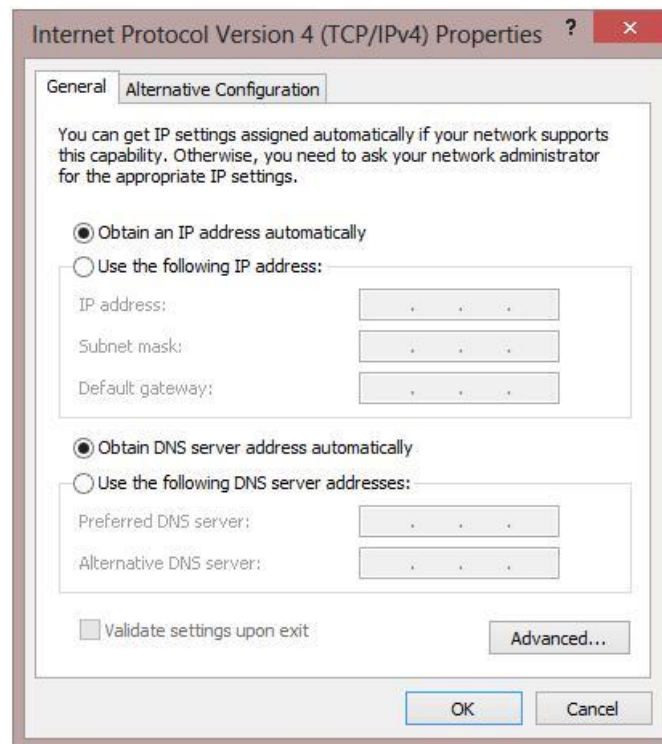
Experiment-9

Aim: Configuration of TCP/IP Protocols in Windows and Linux.

What is IP Address??

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.

An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there. The designers of the Internet Protocol defined an IP address as a 32-bit number.

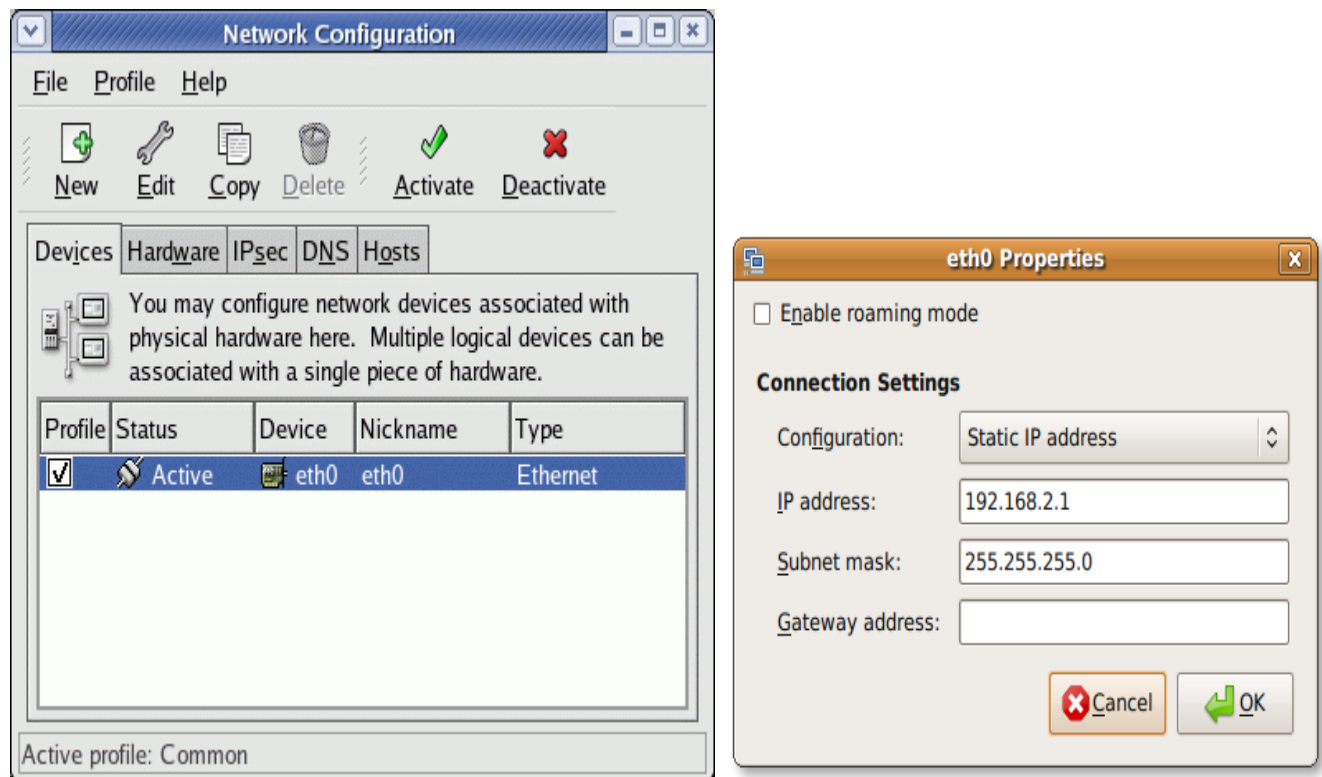


- **Static IP addresses** are generally preferable for such uses as VOIP (Voice over Internet Protocol), online gaming, or any other purpose where users need to make it easy for other computers to locate and connect to them. Static IP addresses are considered somewhat less secure than dynamic IP addresses, since they are easier to track for data mining purposes.
- **Dynamic IP addresses** are temporary and are assigned each time a computer accesses the Internet. They are, in effect, borrowed from a pool of IP addresses that are shared among various computers. Since a limited number of static IP addresses are available, many ISPs reserve a portion of their assigned addresses for sharing among their subscribers in this way. This lowers costs and allows them to service far more subscribers than they otherwise could.

Working with Linux TCP/IP

This article covers the main TCP/IP network configuration files used by Linux to configure various network services of the system such as IP Address, Default Gateway, Name servers - DNS, hostname and much more. Any Linux Administrator must be well aware where these services are configured and to use them. The most of the information provided on this article apply to Redhat Fedora, Enterprise Linux, CentOS, Ubuntu and other similar Linux distributions.

On most Linux systems, you can access the TCP/IP connection details within '**X Windows**' from **Applications > Others > Network Connections**. The same may also be reached through **Application > System Settings > Network > Configure**. This opens up a window, which offers configuration of IP parameters for wired, wireless, mobile broadband, VPN and DSL connections:



The Basic Commands for Networking

The common basic commands used in Linux:

ifconfig - Configures and displays the IP parameters of a network interface

route - Used to set static routes and view the routing table

hostname - Necessary for viewing and setting the hostname of the system

netstat - Flexible command for viewing information about network statistics, current connections, listening ports

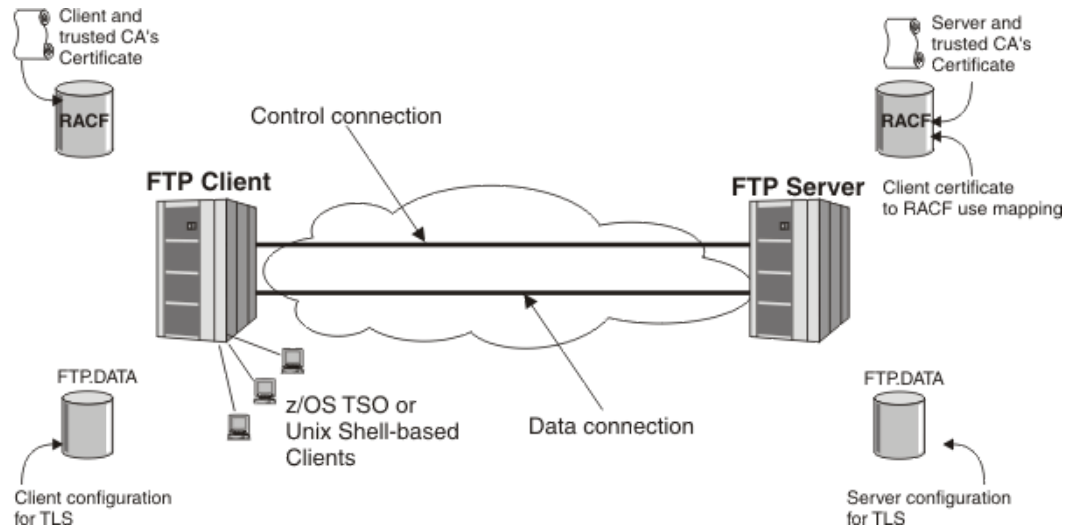
ip - Multi-purpose command for viewing and setting TCP/IP parameters and routes.

tc - Traffic control command, used for classifying, prioritizing, sharing, and limiting both inbound and outbound traffic.

Experiment-10

Aim: Installation of ftp server and client.

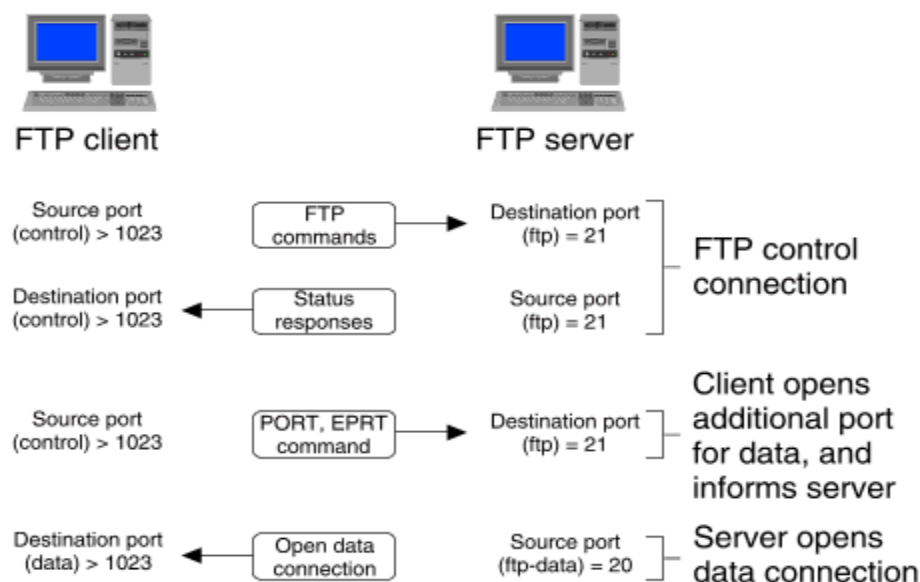
The **File Transfer Protocol (FTP)** is one of the most common means of copying files between servers over the Internet. Most Web-based download sites use the built-in FTP capabilities of Web browsers, and, therefore, most server oriented operating systems usually include an FTP server application as part of the software suite. Linux is no exception.



FTP Overview

FTP relies on a pair of TCP ports to get the job done. It operates using two connection channels:

- ✓ **FTP control channel, TCP Port 21:** All commands you send, as well as the FTP server's responses to those commands, go over the control connection, but any data sent back (such as ls directory lists or actual file data in either direction) will go over the data connection.
- ✓ **FTP data channel, TCP Port 20:** This port is used for all subsequent data transfers between the client and server. In addition to these channels, there are several varieties of FTP.

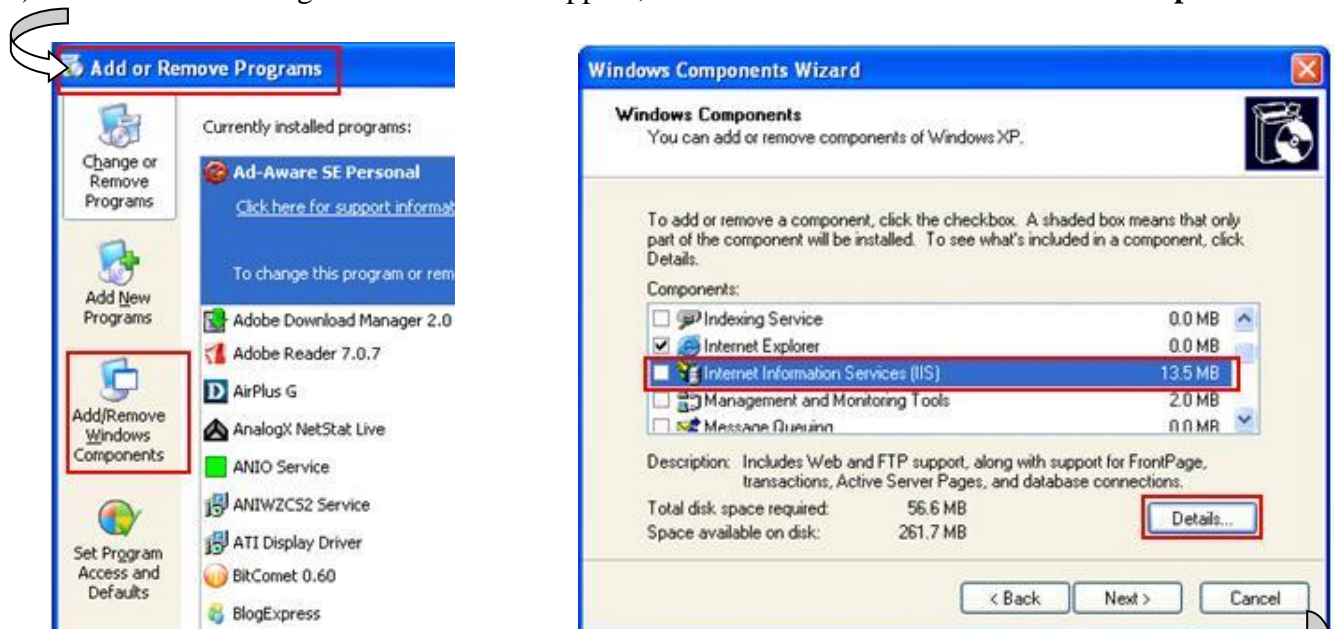


FTP server is good to do file transfer and copying, but the drawback is the communication traffic is sent without encryption, so the FTP login username and password will be seen if somebody sniffs the communication traffic. The better option is to use secure FTP with encryption feature.

Here is **step-by-step instruction** to show you how to enable FTP server in XP Pro:

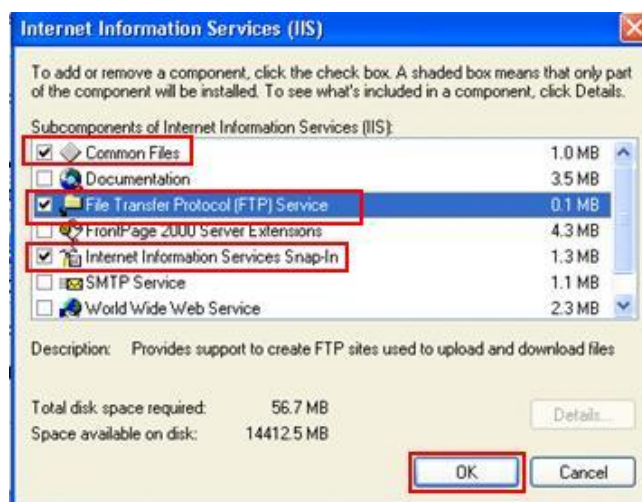
1) Go to **Start** and click **Control Panel**. Control Panel Window will appear, and then double click **Add or Remove Programs**.

2) Add or Remove Programs window will appear, then click **Add/Remove Windows Components**.



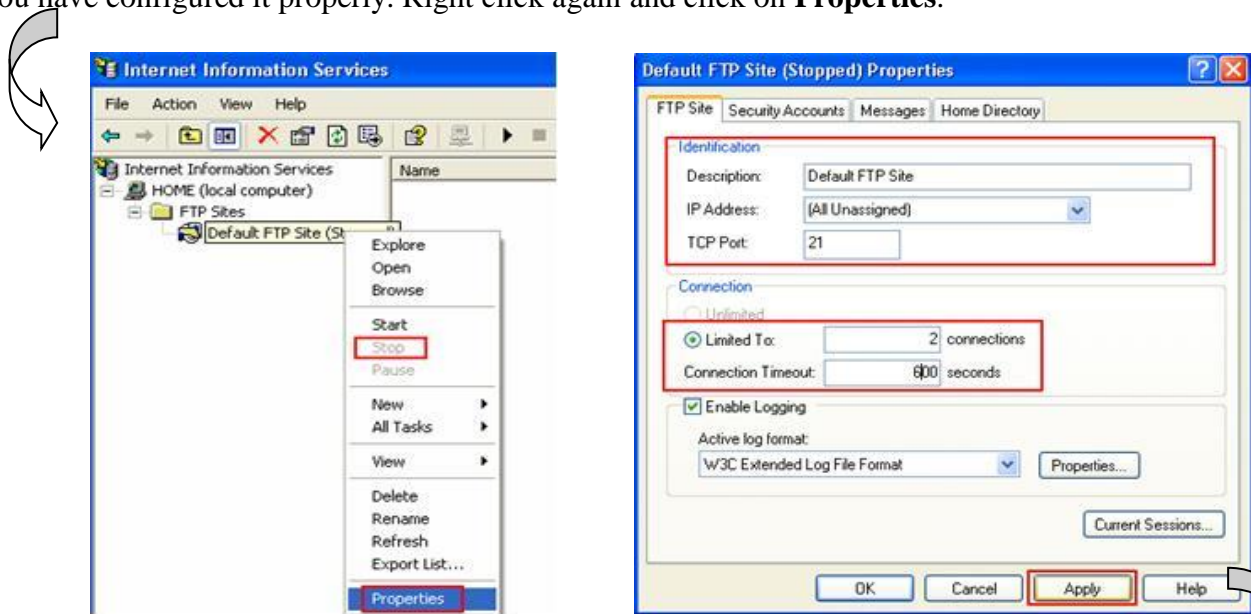
3) In the Windows Components Wizard window, scroll down and select **Internet Information Services (IIS)**, after that click **Details...** button.

4) Internet Information Services window will appear. In order to run FTP server, you need to tick **File Transfer Protocol (FTP) Service**, **Common Files** and **Internet Information Services Snap-In** options. Click **OK** at last and you will be back to previous Windows Components Wizard window; click **Next** to continue and also you may be prompted to insert Windows XP installation CD.



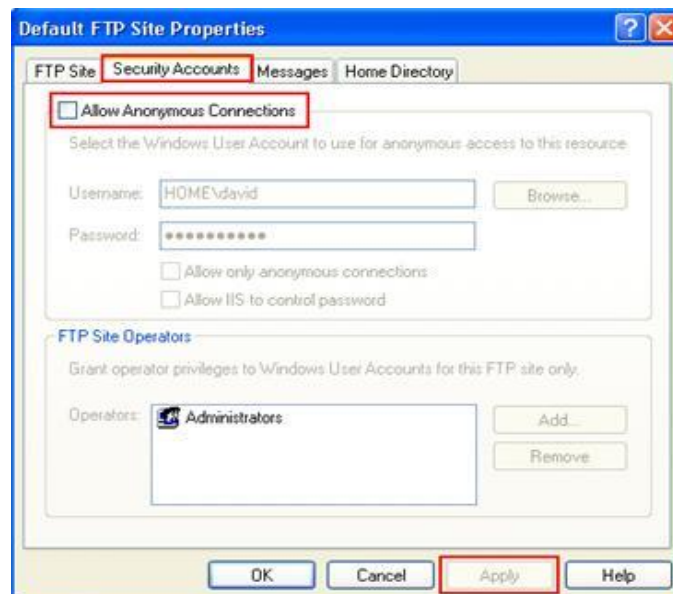
Configuring FTP Server

5) Once you have installed this free FTP server, you need to properly configure it to minimize security risk. Go to your **Control Panel -> Administrative Tools -> open Internet Information Services**. Expand the HOME folder and then right click **Default FTP Sites**, click **Stop** to stop this service until you have configured it properly. Right click again and click on **Properties**.

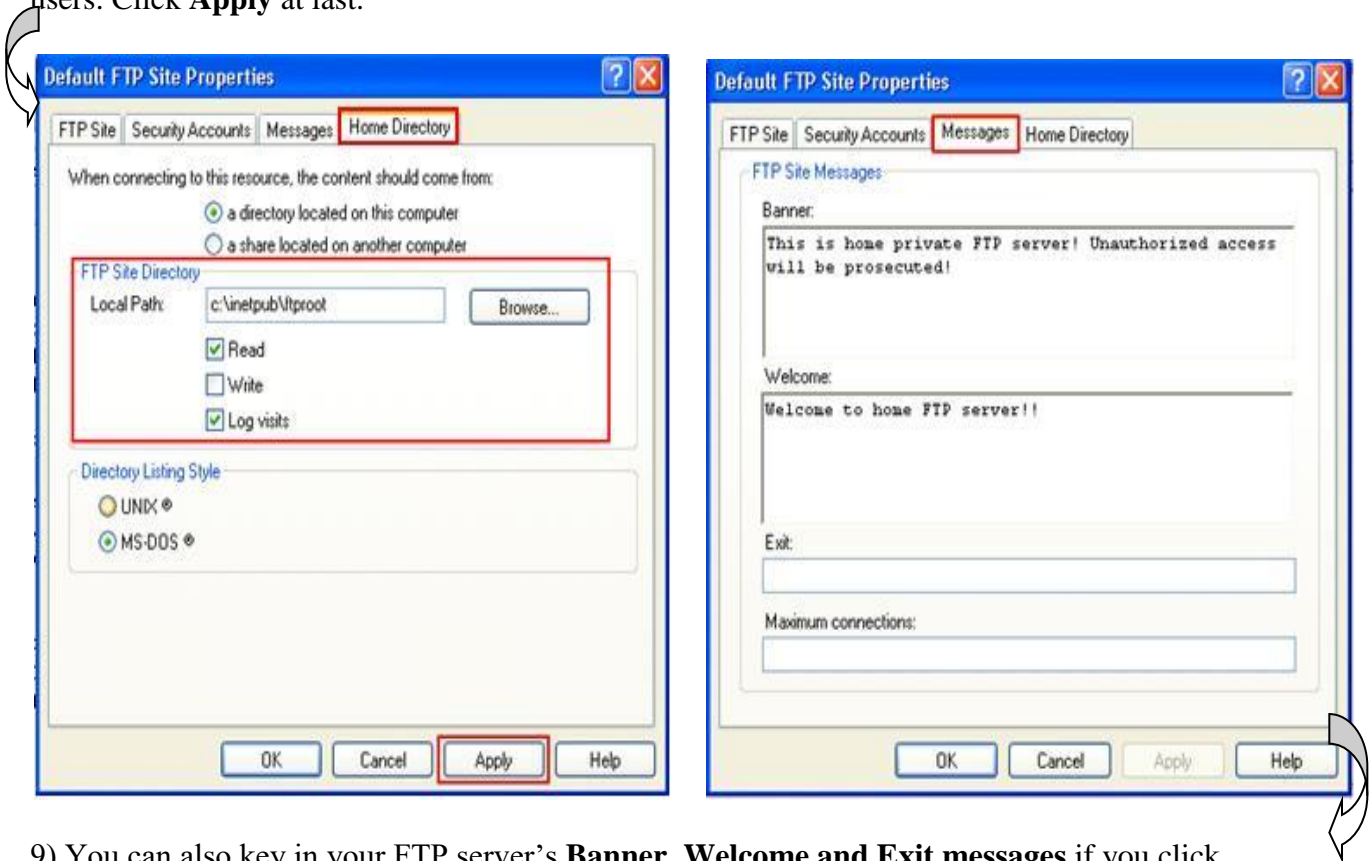


6) Let's go to **FTP Site** tab, here you can configure the **FTP description, IP address and TCP port** if you like, it's optional and so I leave it unchanged. However here I limit to **2 concurrent connections** and **connection timeout** is 600 seconds. You can just decide based on your scenario. Click **Apply** after that.

7) Proceed to click the **Security Accounts** tab, then un-tick **Allow Anonymous Connections** option, so that **only the users on this computer can FTP to this computer by providing username and password**. It would disable anonymous access and better secure you FTP server. Click **Apply** after that.



8) If you click on **Home Directory** tab, you will find out that the FTP home directory is **C:\inetpub\ftproot** (of course you can change it), this is the place you can put the files that you let ftp users to download. Don't tick on **Write** option unless you really want to give the write access to ftp users. Click **Apply** at last.



9) You can also key in your FTP server's **Banner, Welcome and Exit messages** if you click on **Messages** tab.

10) After you have successful configured this free FTP server, don't forget to start the FTP service. And now it's ready to be connected by other FTP users.

Note: If you enable Windows Firewall on this FTP server, you need to enable program exception on FTP port TCP-21. After doing several test, found out Windows Firewall does not support passive FTP well. I would recommend you to use FTP client with active FTP mode to connect to FTP server with Windows Firewall enabled.

Finally, after done with everything, you may access your FTP site through your browser. All you need to do is type `ftp://xxx.xxx.xxx.xxx/` in the URL where "xxx.xxx.xxx.xxx" is the WAN address of your computer.

