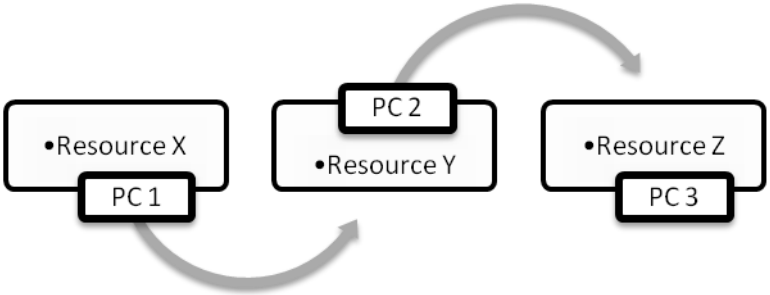
Chapter 1: Introduction

Introduction

- Network is the concept of sharing resources and services
- Network of computer is a group of interconnected system sharing resources using a common communication link.
- Shared resource can be data printer, fax modem services such as email and database.
- To complete a network following are main thing which will be required
  1. Resource to share
  2. Pathway to transfer data (Medium)
  3. A set of rules governing the network (Protocol)

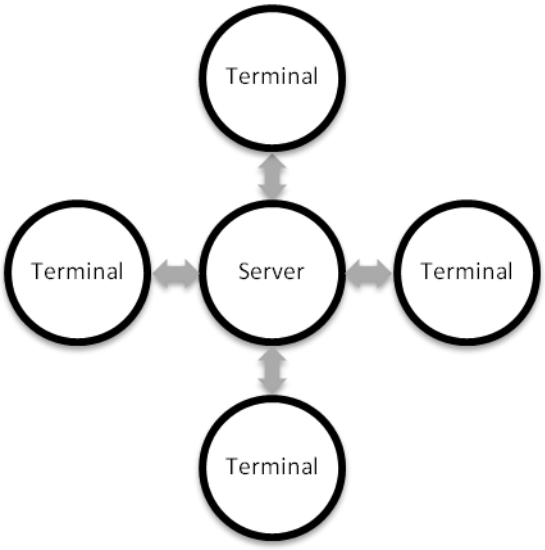


Reason of Network

- Sharing files.
- Sharing printer and other devices.
- Enabling centralized administration and security of resources.
- Supporting network application such as electronic mail and database.

Computing Model

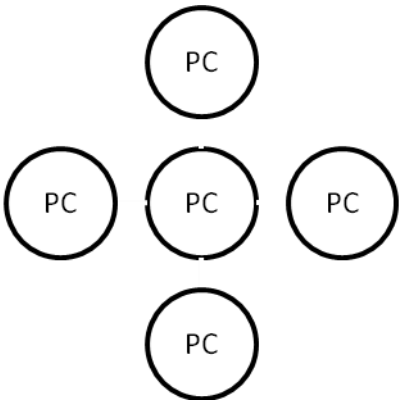
1. **Centralized Computing**
   - In centralized computing dumb terminal are used.
   - Dumb terminal are only for input and output without any independent data storage and processing power.
   - All the processing are done by centralized server i.e. At the single location – Server
   - Today also centralized computing are still being operated around



theworld most often by government and large corporation, such as ATM machine and Railway ticket.

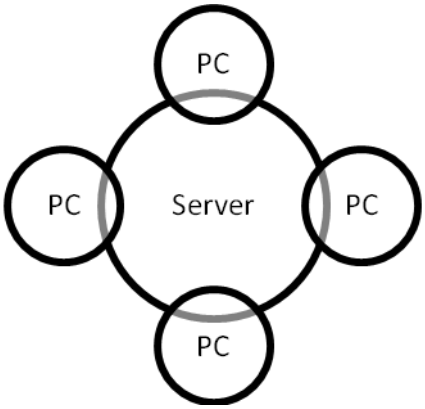
- One of the drawback was that mainframe were not flexible in their placement (Required large size for installation) and did not scale down to the need of small scale organization

2. Distributed Computing



- The personal computer where introduced to the organization and a new model distributed computing emerged.
- Instead of centralized computing at a central device PC make it possible to give each worker an independent individual computer.
- PC could receive input, process the input, generate the output and display the output without aid of another computer
- But the PC is however not a computing has powered of the mainframe computer.
- A centralized computing model is like the BUS, a large powerful vehicle which can transport many people at the once
- Distributed computing model is like a motor-cycle (i.e. PC), can go anywhere without worrying about the other user.
- An advantage of distributed model is that it can provide a small business with their own computational capabilities. Enabling them to perform less complex computing task on smaller inexpensive machine.

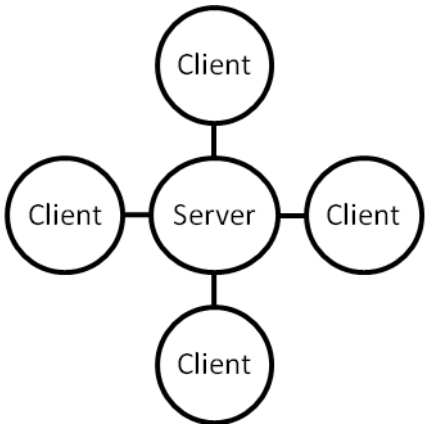
3. Collaborative Computing or Co-Operative Computing



- Co-Operative computing enables computer to distribute the work.
- On the internet web client actively used the resource available on the web server to display image, graphics, videos etc in the browser.
- Another example of co-operative is Microsoft server base product such as Exchange Server or SQL Server
- Many times it is said that computing ratio is 30:70 ratio. 30% work will be done by client and remaining 70% work will be done by the server, when using it.

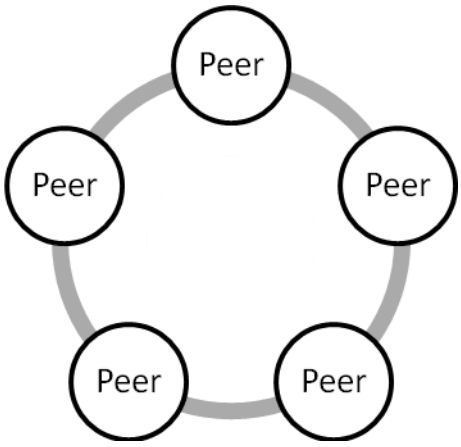
Network Models

1. Client – Server



- A client server network consist of group of user oriented PC called a client, that issue a request to the server.
- A server on the network is responsible to response that request.
- Server is generally high performance system that is made to provide network services to the clients.
- Servers are having more memory, more processing power and more disk space comparing to the client.
- Some example of client server based network is Novell Network and Windows NT.
- In a general server are not often setups to do task that a client machine can do, for example in a Novell, person cannot open a spread sheet directly from the server console.
- In a mainframe computing dumb terminal / online terminal does not process any request, terminal are only for the putting the request and accept the response from the server.

2. Peer to Peer



- In such networking a group of computer operates as equal. Every computer is known as peer.
- Peer share resource such as file, printer etc. just like in server based network.
- The peer given the resource to other is known as server, and peer who is using the resource is known as client.
- In this kind of network any peer can be client and peer can be server depends on resource what they are having.
- Such networks are help full when resource utilization is to be made at the maximum point in a smaller unit of a business.

Network Services

1. **File service**
   - A file service enable network computer to share files to each others, this was the primary reason for a networking of personal computer.
   - The service includes dealing with the storage retrieval or movement of data.
   - Read, write or management of a file is also made possible in the network.
   - Computer providing a file service are referred as file server, there are two kinds of fileserver 'Dedicated server' and 'Non-dedicated server'.
   - Advantages of Dedicate server.
     - Files are stored at a central location, so access of file is easy.
     - As the data storage is central location it can be manage easily.
     - As the file server contains expensive high performance hardware, it can be shared by the large number of users.
     - The dedicated servers are more scalable comparing to others.
   - **Disadvantage of Dedicate server**
     - As the data store in the single server, and a failure of that means no data will be available.
     - As all client connected to the file server to access the data.
     - The average access time might be slower comparing to local data storage in the centralized server.
   - **Advantage of Non-dedicate server**
     - The data storage is at the local disk so failure of any disk will make failure of that particular data only, other data can be access easily.
     - An individual user will experience a faster access time as the data on local disk.
     - No specialized server hardware is required and file service can be directly provided by the standard PC
   - **Disadvantage of Non-dedicate server**
     - To manage the data it is more difficult as a single storage of data does not exist.
     - A file service typically provided by the peer which are not as fast or as flexible as the file server provide the central file storage specially design for that purpose.
     - In the non-dedicated server each and every peer must be upgraded to get high performance as the centralized dedicated servers.

2. **File transfer**
   - Without a network there are limited options available to transfer data between computers.
   - Exchange of file can also be possible with the help of reusable disk such as CD, DVD, Pen drive, etc. this process is known as sneaker net because a physical hand delivery to be made from desk to desk.
   - With the help of file transfer services, high speed data transfer can be made without living there desk.

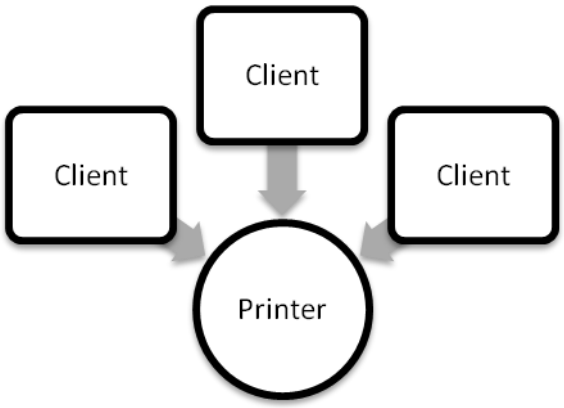
3. **Data migration**
   - It is the technology that automatically moves infrequently moved data from online storage to near line or offline storage.
   - The criteria for moving file the files to offline storage includes owner of the file, file size, last access date and time of file, etc.

Files Older than 60 days | **Files Older than 120 days** | **Files Older than 180 days**

4. **File Archiving**
   - File archiving is also known as the backup.
   - These backup copies serve as the insurance against minor or major system failure.
   - Generally the backup copies contain important system files, application files and data files.
   - It is the responsibility of network administrator to enable file archiving from the centralized or from distributed location.

5. **File update synchronization**
   - The service ensures that all users have resent updated copy of file in network.
   - It will monitor date and time of the file to determine which file where save most recently.
   - In a modern computing environment it is not always visible for all users to get recently update file in real time.
   - File update synchronization becomes more challengeable task when number of users sharing the same file simultaneously.
   - A complex mechanism must be place to make sure that the data is not over written when multiple user are working on it.
   - In some case system might use flags to indicate a conflict of multiple update.

6. Printing service



- After the file service, printing service is the second reason for the installing of the network.
- With the help of this service many user can share same printer, this facility is useful when very expensive device such as color printer and plotter is to be used.
- A printer can be located anywhere on the network even on the work station or directly on the network device such as Hub, Switch, Router, etc.
- The service provide queue based networking so the user can put there printing job in the queue and continue their work as the job is queued.

7. Application service

- The increase the computing power and specialized the capabilities of other computer on network.
- It helps to perform a complex statistical calculation beyond the scope of most desktop computers.
- Such statistical application might need to run on a mainframe computer or on minicomputer.
- The client PC sent the calculation request to the statistical server and server will return the result to that particular client.
- This is the only way through which expensive licensed software and required power processing can be shared in the network to all client.

8. Database service

- The service is specially design in a separate client and server component such application are frequently called as client server database.
- In such services the client application manage data input from the user generation of a screen display, some of the reporting and data retrieval request send to the database server.
- The database server manages the database file. Add, delete and modify the records in the database query the database and generate result required by the client and result is send back to that client.
- With the help of this service a multiple client can request to the server and server can response all client in the same time.
- Such database software can perform following tasks

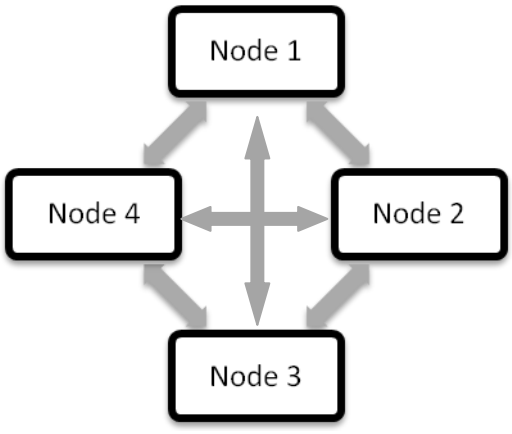
- Provides database security.
- Can service large number of client by reducing the amount of time of any client send to access the database
- A data can be distributed across the multiple database servers.
- The distributed server can be master driven update server or locally driven update server.
- In master driven update server, server will receive all update and it will responsible to update other database servers.
- In locally driven update server, normal server will receive all update and it is responsible to update other server including the master server.

9. Security service

- It is the one of the most important elements invoke a network.
- With the help of security service a various kind of security can be provided such as records of company, file on the server, which user can access a data, who can use the printer, what the specific time, where user can login and what up to what period.
- A security service often deals with user account database, which often contains user information. Mainly login name, passwords and various other user information.
- Some service added to a network can utilize the security system of the running operating system. For example Microsoft Exchange Server.
- But other service or a application such as Lotus Notes is having its own independent security system. It will not use the current available system of running OS.

Topologies

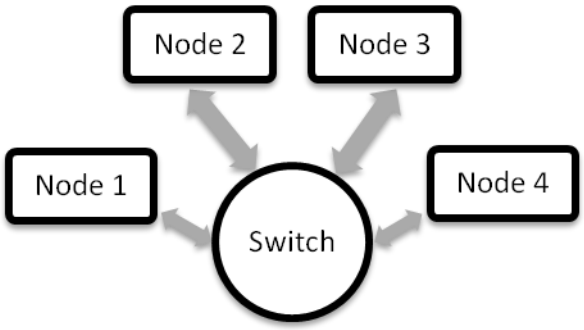
1. Mesh



- In the mesh topology every device has a dedicated point to point link to every other device.
- The term dedicated means that the link carries the traffic only between the two devices.
- The full connected mesh network always has n (n-1)/2 a physical channel to link every other device.
- The advantage of mesh topology can be as follows
  - The use of dedicated links generated that each connection can carry their own data so no traffic problem will exist.
  - It is the robust network if one link fails it does not harm a entire network.

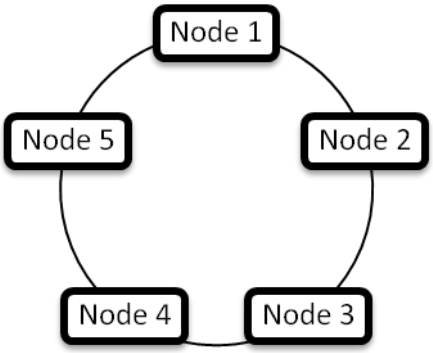
- Another advantage is privacy and security as the message travel in the dedicated lines. It prevents the access of data from other users.

- The disadvantages of mesh topology are as under
  - High amount of cabling is required than any other topology.
  - As more cabling is required the installation of cable is not easy to make fit in current shell.
  - More hardware is also required as each machine is having n-1 input output ports.
  - Upgrading the network is very hard as add one more device means more n-1 cables and I/O ports will be needed.



2. Star

- Each device has dedicated point to point link only to the central controller generally known as switch.
- As devices are not directly connected to one another, the exchange of message or data would be made through a central device switch.
- Sender will pass message or data to central device, which will then relay that message to another connected device i.e. receiver.
- The advantage of star topology are as follows
  - Less expensive comparing to the mess topology as less cabling and only one input output port is required.
  - It is also robust as the mesh topology; if one link fails then all other links will remain active because the internal design of switch is same as mesh topology.
  - It is also helpful in identification of the fault as long as switch is working it can also be used for monitoring the link.
  - The network can also be easily upgraded by adding extra switch in the network and inter connecting them.



3. Ring

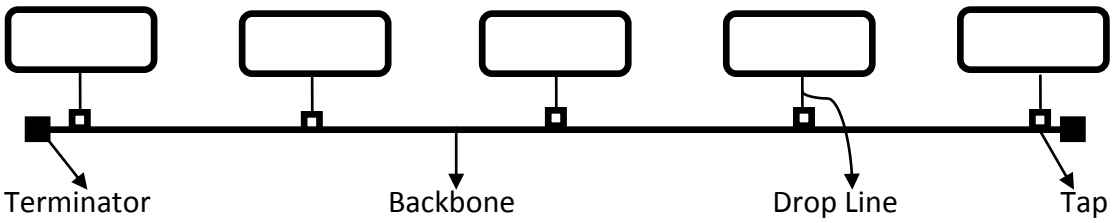
- A dedicated point to point connection is made only with neighbor device on each side of it.
- A signal, message or data will move in only one direction from device to device until it reaches to

its destination.

- Each device will regenerate signal (repeater[i]) and pass it to another device.
- The advantage of ring topology are as follows
  - Fault isolation is simplified as signal is circulating at all time if one device does not receive the signal within the specify period of time.
- The disadvantage of ring topology are as follows
  - The break in the ring, such as any system is down can disable whole network but this can be solved using dual ring.

4. Bus

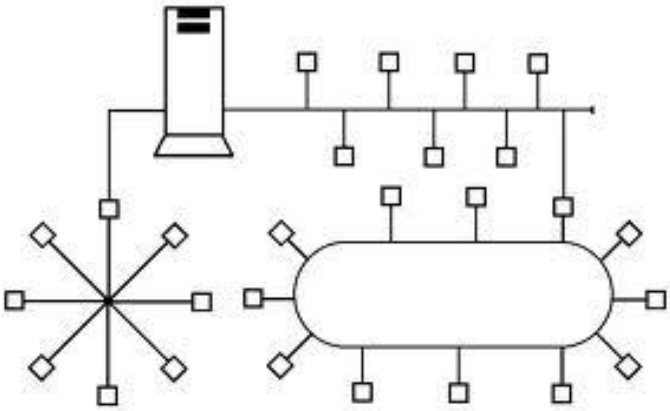
- One cable act as back bone to all devices in the network.
- Every device is connected to the bus cable by drop lines and tapes.
- The drop lines are connection running between device and main cable.
- Tape is the connection that either slice into the main cable or puncher into the main cable to connect with.
- A special connector called a terminator must be place at the end of backbone cable to prevent signal from reflecting back and causing the interference.
- The advantage of bus topology are as follows
  - The topology is having easy installation, comparing to star and mesh topologies.
  - It also required less able compare to star and mesh as only one backbone main cable much be stretched through the entire network.
- The disadvantage of bus topology are as follows
  - It is very hard to reconnection of any device or solving fault.
  - To add any new device will bring down whole network for that time period.
  - Any fault in main cable will bring down whole network.



5. 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.).
- 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 multistation 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).



- Advantages of Hybrid Network Topology
  - Reliable: Unlike other networks, fault detection and troubleshooting is easy in this type of topology. The part in which fault is detected can be isolated from the rest of network and required corrective measures can be taken, WITHOUT affecting the functioning of rest of the network.
  - Scalable: It's easy to increase the size of network by adding new components, without disturbing existing architecture.
  - Flexible: Hybrid Network can be designed according to the requirements of the organization and by optimizing the available resources. Special care can be given to nodes where traffic is high as well as where chances of fault are high.
  - Effective: Hybrid topology is the combination of two or more topologies, so we can design it in such a way that strengths of constituent topologies are maximized while there weaknesses are neutralized. For example we saw Ring Topology has good data reliability (achieved by use of tokens) and Star topology has high tolerance capability (as each node is not directly connected to other but through central device), so these two can be used effectively in hybrid star-ring topology.
- Disadvantages of Hybrid Topology
  - Complexity of Design: One of the biggest drawbacks of hybrid topology is its design. It's not easy to design this type of architecture and it's a tough job for designers. Configuration and installation process needs to be very efficient.
  - Costly Hub: The hubs used to connect two distinct networks, are very expensive. These hubs are different from usual hubs as they need to be intelligent enough to work with different architectures and should be function even if a part of network is down.

- Costly Infrastructure: As hybrid architectures are usually larger in scale, they require a lot of cables; cooling systems, sophisticate network devices, etc.

Types of Network

- There are three main primary categories of network: Local Area Network, Metropolitan Area Network and Wide Area Network.
- Into which category a network falls is determined by its size, ownership, distance it covers and its physical architecture.

1. Local Area Network

- LAN is usually privately owned and links the devices in a single office, building or campus.
- Depending on the need of an organization and the types of technology used, LAN can be even of two PCs and Printer in some office or home.
- LANs are designed to allow resource to be shared between personal computers or workstation.
- One of computer may be given a large capacity disk drive and may become a server to the other clients. Software can be stored on this central server and used as needed by whole group.
- In addition to size LAN are distinguished from other types of networks by their transmission media and topology. Generally LAN uses only one type of transmission medium and common topology star.
- Traditionally LAN have data rates in 4 to 16 megabits per second(Mbps), however today's LAN have speed up to 100Mbps to 1Gbps (Gigabits per seconds).

2. Metropolitan Area Network

- MAN is designed to extend over an entire city. It may be single network such as cable television network or it may be means of connecting a number of LANs into a larger network so that resource may be shared to LAN to LAN.
- MAN may be wholly owned and operated by a private company, or it may be service provided by a public company such as local telephone company.

3. Wide Area Network

- It provides long distance transmission of data, voice, image and video information over large geographic areas that may comprise a country, continent or even whole world
- It contrasts to LANs which depends on their own hardware for transmission.
- WAN may utilize public, leased or private communication equipment usually in combination and therefore span an unlimited number of miles

WAN that is wholly owned and used by a single company is often referred to as enterprise network.

Access Methods

- An access method is set of rules governing how the network nodes share the transmission medium.
- Network comes in few standards forms of architecture and each form is complete system of compatible hardware, protocol, transmission media and topology.
- Several factors set the various network topologies and one of the most important things is selection of access method.
- Access method decided how to share information between different device by sharing same transmission medium
- There are three main types of access methods that are Polling, Token Passing and Contention.

1. Polling

- In polling one device is responsible for polling to check that other device are ready for transmission or to receive the data or not.
- Polling based system require a device called a controller or a master device to check other devices on network.
- This access method is not widely used on the network because the polling itself can cause a fair amount of traffic in the network.
- A common example of polling is when computer call's printer for the print job.

2. CSMA/CD

- CSMA/CD (Carrier Sense Multiple Access/Collision Detection) is the protocol used in Ethernet networks to ensure that only one network node is transmitting on the network wire at any one time.
- CSMA/CD is a type of contention protocol.
- CSMA/CD is a set of rules determining how network devices respond when two devices attempt to use a data channel simultaneously (called a collision). Standard Ethernet networks use CSMS/CD to physically monitor the traffic on the line at participating stations. If no transmission is taking place at the time, the particular station can transmit.
- If two stations attempt to transmit simultaneously, this causes a collision, which is detected by all participating stations. After a random time interval, the stations that collided attempt to transmit again.
- If another collision occurs, the time intervals from which the random waiting time is selected are increased step by step. This is known as exponential back off.

- **Carrier Sense** means that every Ethernet device listens to the Ethernet wire before it attempts to transmit. If the Ethernet device senses that another device is transmitting, it will wait to transmit.
- **Multiple Access** à means that more than one Ethernet device can be sensing (listening and waiting to transmit) at a time.
- **Collision Detection** à means that when multiple Ethernet devices accidentally transmit at the same time, they are able to detect this error.

3. CSMA/CA

- CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is a protocol for carrier transmission in 802.11 networks. Unlike CSMA/CD (Carrier Sense Multiple Access/Collision Detect) which deals with transmissions after a collision has occurred, CSMA/CA acts to prevent collisions before they happen.
- In CSMA/CA, as soon as a node receives a packet that is to be sent, it checks to be sure the channel is clear (no other node is transmitting at the time). If the channel is clear, then the packet is sent.
- If the channel is not clear, the node waits for a randomly chosen period of time, and then checks again to see if the channel is clear. This period of time is called the backoff factor, and is counted down by a backoff counter. If the channel is clear when the backoff counter reaches zero, the node transmits the packet. If the channel is not clear when the backoff counter reaches zero, the backoff factor is set again, and the process is repeated.
- CSMA CD takes effect after a collision while CSMA CA takes effect before a collision.
- CSMA CA reduces the possibility of a collision while CSMA CD only minimizes the recovery/time.
- CSMA CD is typically used in wired networks while CSMA CA is used in wireless networks.

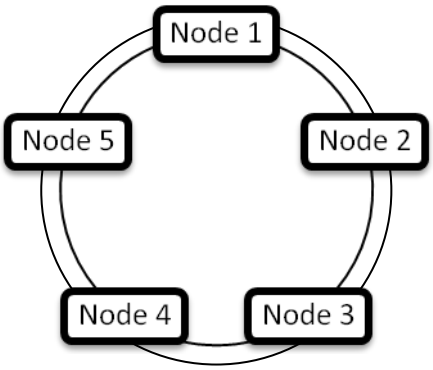
4. Token Passing

- The token passing access method is a non-contention method that works verydifferently from the contention methods.
- In token passing, when a host want to transmit data, it should hold the token, which is an empty packet. The token is circling the network in a very high speed.
- If any workstation wants to send data, it should wait for the token. When the token has reached the workstation, the workstation can take the token from the network, fill it with data, mark the token as being used and place the token back to the network.
- In a Token Ring network, the token goes around the ring; in a token bus network, it goes down the line of the bus. If a computer has data to transmit, it must wait until the token reaches it; then that computer can capture the token and transmit data.

Advance Network Topologies

1. FDDI

- Fiber Distributed Data Interface (FDDI) is an expensive LAN technology that employs a pair of fiber-optic rings.
- One is primary ring and the second ring is used to replace the primary ring in the case of a network failure. Fiber Distributed Data Interface (FDDI) uses fiber-optic cable and is wired in a ring topology and Fiber Distributed Data Interface (FDDI) uses token passing as its media-access method and can operate at high speeds.



- The Fiber Distributed Data Interface (FDDI) provides high-speed network backbones that can be used to connect and extend LANs.
- Like token ring, FDDI also has error-detection and correction capabilities. In a normally operating Fiber Distributed Data Interface (FDDI) ring, the token passes by each network device fast. If the token is not seen within the maximum amount of time that it takes to circulate the largest ring, it indicates a network problem.
- Fiber-optic cable such as the cable used with Fiber Distributed Data Interface (FDDI) can support very large volumes of data over large distances.
- Fiber Distributed Data Interface (FDDI) is an expensive technology to set up because the network devices require a special network card and also fiber-optic cabling is required, which is expensive than twisted-pair cable. Because most Fiber Distributed Data Interface (FDDI) installations use a redundant second ring, more cabling is required.

2. CDDI

- For a local area network (LAN), CDDI (Copper Distributed Data Interface) is a standard for data transmission based on FDDI (Fiber Distributed Data Interface) that uses shielded twisted-pair (STP) or unshielded twisted pair (UTP) copper wire instead of fiber optic lines.
- CDDI supports a dual-ring capacity of 200 Mbps. CDDI's maximum distance is up to 200 meters, which is much shorter than FDDI.
- CDDI is defined by the American National Standards Committee X3-T9.5 and conforms to the Open Systems Interconnection (OSI) model of functional layering.
- CDDI is officially named the Twisted-Pair Physical Medium Dependent (TP-PMD) standard and is also referred to as Twisted Pair Distributed Data Interface (TP-DDI).

3. Ethernet

- Ethernet is the most widely used network topology. You can choose between bus and star topologies, as well as coax, twisted-pair, or fiber optic cabling.
- With the right connective equipment, multiple Ethernet-based LANs can be linked together. In fact, with the right equipment and software, even Token Ring, AppleTalk®, and wireless LANs can be connected to Ethernet.
- Ethernet uses CSMA/CD (Carrier Sense Multiple Access with Collision Detection). In this method, multiple workstations access a transmission medium (multiple access) by listening until no signals are detected (carrier sense).
- Then they transmit and check to see if more than one signal is present (collision detection). Each station attempts to transmit when it "believes" the network is free. If there is a collision, each station attempts to retransmit after a preset delay, which is different for each workstation.
- When a collision is detected, a "jam" signal is propagated to all nodes. Each station that detects the collision will wait some period of time and then try again.
- The two possible topologies for Ethernet are bus and star.
- The bus is the simplest (and the traditional) topology. Standard Ethernet (10BASE5) and Thin Ethernet (10BASE2), both based on coax cable systems, use the bus. In this one-cable LAN, all workstations are connected in succession (a "bus" arrangement) on a single cable.
- In a star topology, all attached workstations are wired directly to a central hub that establishes, maintains, and breaks connections between them (in the event of an error). Twisted-Pair Ethernet (10BASE-T), based on unshielded twisted pair, and Fiber Optic Ethernet (FOIRL and 10BASE-FL), based on fiber optic cable, use the star.
- **Standard Ethernet (Coax): 10BASE5**
  - The maximum length of a segment is 500 meters.
  - A maximum of 2 IRL (InterRepeater Links) is allowed between devices; the maximum length of cable is 2.5 km.
  - Devices attach to the backbone via transceivers.
  - The minimum distance between transceivers is 2.5 meters.The maximum length of a transceiver cable is 50 meters.
  - Up to 100 transceiver connections can be attached to a single segment.
  - Only transceivers without SQE ("heartbeat") test enabled should be used with repeaters.
  - Both ends of each segment should be terminated with a 50-ohm resistor.
  - One end of each segment should be grounded to earth.
- **Thin Net Ethernet (Coax): 10BASE2**
  - The maximum length of a segment is 185 meters.

- A maximum of 2 IRL (InterRepeater Links) is allowed between devices; the maximum length of cable is 925 meters.
- Typically, devices use Ethernet network interface cards (NICs) with built-in BNC transceivers, so connections can be made directly to the Thin Net cable.
- Devices are connected to the cable with T-connectors, which must be plugged directly into the card. No cable is allowed between the T and the card. Workstations are daisy chained with an "in-and-out" cabling system.
- The minimum distance between T-connectors is 0.5 meters.
- If the interface card does not have its own built-in BNC transceiver, a BNC transceiver and transceiver cable are required. The maximum length of a transceiver cable is 50 meters.
- Up to 30 connections can be attached to a single segment.
- Both ends of each segment should be terminated with a 50-ohm resistor. One end of each segment should be grounded to earth.

Twisted-Pair Ethernet (Unshielded Twisted Pair): 10BASE-T, UTP

- There are two versions of Ethernet over unshielded twisted pair: 10BASE-T (the standard) and its predecessor UTP.
- 10BASE-T and UTP segments can coexist on the same network via a transceiver and transceiver cable or converter when each hub is attached to a common segment.
- The cable used is 22 to 26 AWG unshielded twisted pair (standard telephone wire), at least Category 2 with two twists per foot. Category 3 or 4 is preferred. Category 5 supports 100BASE-T (Fast Ethernet) and is recommended for all new installations.
- Workstations are connected to a central concentrator ("hub") in a star configuration. Concentrators can be attached to a fiber optic or coax network and can be daisy chained to form larger networks.
- A hub usually also has an AUI port for standard Ethernet connections.
- The maximum segment distance from concentrator to node is 100 meters.
- The maximum number of devices per segment is two: the hub port and the 10BASE-T or UTP device.
- Ethernet network interface cards (NICs) are available with built-in 10BASE-T transceivers.Devices with standard AUI ports may be attached with a twisted-pair transceiver.
- Twisted pair is the most economical cable type, since it may already be installed, and it is the easiest to work with. But it's not recommended for installations with a great deal of EMI/RFI interference (for example, in industrial environments).

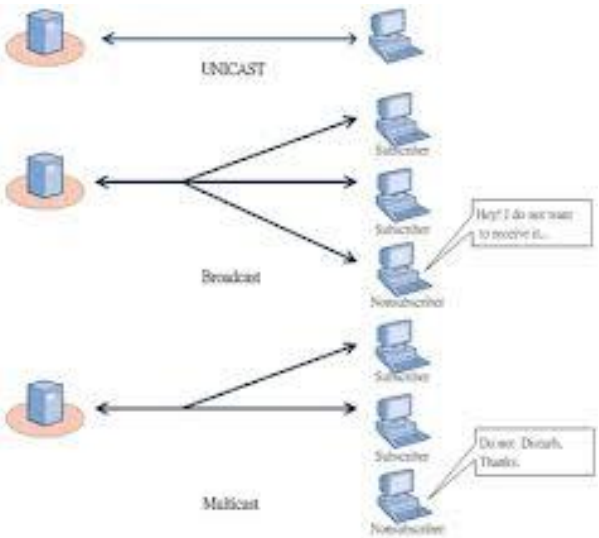
Fiber Optic Ethernet: FOIRL or 10BASE-FL

- There are two versions of Ethernet over fiber optic cable, one for the older FOIRL (Fiber Optic InterRepeater Link) and one for the more recent 10BASE-FL standards.
- FOIRL and 10BASE-FL fiber optic Ethernet differ only in how far each will transmit (the maximum length of a segment). For FOIRL it is 1 km; for 10BASE-FL it is 2 km.
- The maximum number of devices per segment is two: the hub port and the 10BASE-FL device.
- Fiber optic cable provides the best signal quality as well as the greatest point-to-point distance and is completely free of EMI/RFI interference.
- Fiber optic cable runs point to point only-it cannot be tapped or daisy chained. A fiber optic hub or multiport repeater is required to carry the signal to multiple devices (for FOIRL, a FOIRL multiport repeater and transceivers).
- Since fiber optic cable does not carry electrical charges, there are no electrical cable problems. And it's immune to electronic eavesdropping. When outdoor-quality fiber optic cable is used to link buildings, grounding problems and voltage spikes are eliminated.

Communication Methods

1. Unicasting

- Unicast is the term used to describe communication where a piece of information is sent from one point to another point. In this case there is just one sender, and one receiver.
- Unicast transmission, in which a packet is sent from a single source to a specified destination, is still the predominant form of transmission on LANs and within the Internet.



2. Multicast

- Multicast is the term used to describe communication where a piece of information is sent from one or more points to a set of other points. In this case there is may be one or more senders, and the information is distributed to a set of receivers (there may be no receiversor any other number of receivers).

3. Broadcast

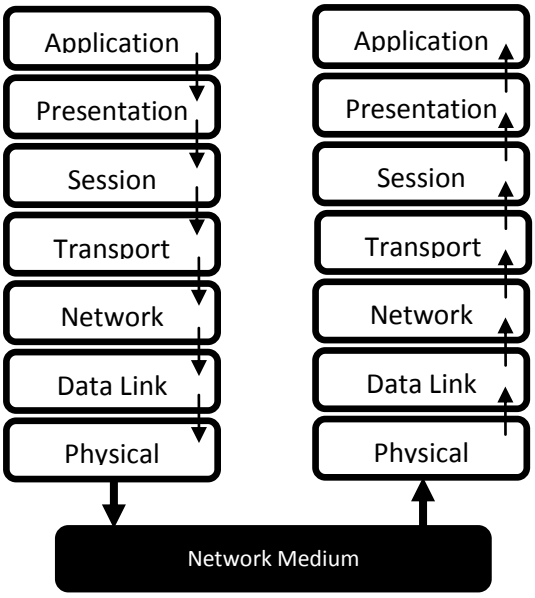
- Broadcast is the term used to describe communication where a piece of information is sent from one point to all other points. In this case there is just one sender, but the information is sent to all connected receivers.

Network Standards

1. **De-Facto standard**
   - De-Facto standard arise through widespread commercial and education use.
   - This standard often is proprietary and usually remains unpublished and unavailable to the outside vendors' i.e. common users.
   - Unpublished and unavailable standard is also known as closed system.
   - Publish and available standard on the other hand are known as open system.
   - The example of proprietary or closed system is IBM system network architecture and Novell's NetWare.

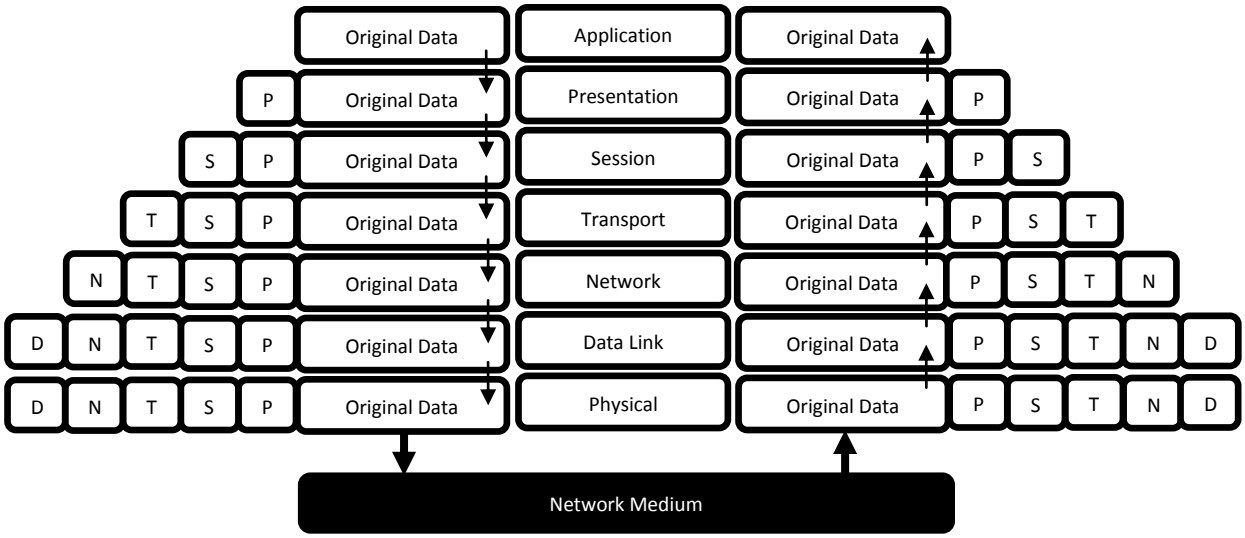
2. **De-Jure standard**
   - De Jure standards are nonproprietary, which means that no single company creates them or owns the rights to them.
   - De Jure is developed with the intent of enhancing connectivity and interoperability by making specification public; so that independent manufacturer can build such specification. TCP/IP is an example of nonproprietary De Juire standard.

OSI Reference Model



- The most commonly used model is open system inter connection.
- The OSI model released in 1984 by international standard organization (ISO)
- OSI model is the blue print for vendors while developing a protocol.
- OSI model having different 7 layers, each having their special work to complete the process of communication.
- Layer 1 the physical layer or hardware layer consist of protocols that control communication of network media.
- Layer 7 the application layer interface the network services with the application of the computer. The service can be file service, printing service, etc.
- The other layers data link layer, network layer, transportation layer, session layer and presentation layer.
- When information is passed with the OSI model on a computer, each protocol layer add its own information to message which is being send.

- The information takes the form of header added to beginning of original message. The sending of a message always goes down in OSI model, hence the header are added top to bottom.
- When the message is received by destination computer every layer's information will be removed one after another.
- The header are removed in reverse order i.e. header which is added last will be removed first, and first added header will be removed last.
- The information of layer pass vertically, but the information between the computer communicate horizontal because each layer of sender computer will talks to it respective layer of receiving computer.
- Note should be made that the physical layer does not add any header information because the layer deals with providing a transmission routes between the computers.



1. **Physical Layer**
   - OSI physical layer does not define the media which should be used. The layer is concern with all aspect of transmitting or receiving data or network media
   - The layer is not responsible for saying whether a cable should be made a silver, copper or gold.
   - A layer is concern with transmitting and receiving bits.
   - This layer defines several key characteristics of the physical network, including the Following
     - Physical structure of the network (physical topology)
     - Mechanical and electrical specifications for using the medium (not the medium itself)
     - Bit transmission encoding and timing

2. **Data Link Layer**

- In the network communication the main thing involved is transferring the bits from one machine to another.
- Dozens of steps must be performing before transferring message to one device to another.
- The real message is not consist of a single bit but group of bits known as frame received from upper layer.
- It is the responsibility of data link layer to disassemble the frames into the bits from sender side and reassemble bits into frame at receiver side.
- The other function of data link layer is addressing, error control and flow control for a single link between the network devices.
- **The Data Link layer into two sub layers:**
  - Media Access Control (MAC). The MAC sub layer controls the means by which multiple devices share the same media channel. This includes contention methods and other media access details. The MAC layer also provides addressing information for communication between network devices.
  - Logical Link Control (LLC). The LLC sub layer establishes and maintains links between communicating devices.

3. Network layer

- The data link layer deals with communication between the devices on the same network.
- The network layer handle the communication between devices, which are logically on the different network but are connected as the inter network.
- As the inter network can be off large size and may be constructed with the different types of network. The network layer will guide the packet by using the routing algorithm after reading their destination address.

4. Transportation Layer

- The layer ensures the reliable delivery of message to the destination device.
- The term reliable does not mean that the error never occurs instead it means that if error occurs they are detected.
- If error such as lost of data are detected the transformation layer either request the retransmission or notifies upper layer protocol so that they can take corrective action
- The main function of the transportation layer is to break large message in to segments suitable for network delivery.

Activities of transportation layer

- Repacking: When the large message divided into segment for the transportation, the transportation layer must be package the segments when they are receive before reassembling the original message.
- Error Control: When segments are lost during the transmission or when segment have duplicate ID the transportation layer initiate error recovery. The transportation layer also detects corrupted segments by managing end to end error control technique.
- End to End flow control: The transportation layer manage end to end flow control by using acknowledgment between two connected devices. If no acknowledgement receive or negative acknowledgment is detected the transportation layer can request the retransmission of most recent segment.

5. Session Layer

- The layer manage dialog between two computers by establishing, managing and terminating communication.
- There are three types of communication which are as follows.

Types of Session

- Simple dialog: It is responsible for one way data transfer only, for example a fire alarm which send a alarm message to the fire station but cannot receive any message from fire station
- Half Duplex dialog: This dialog handles two way transmissions but only one way at a time. When one device completes transmission then only another can transmit the message.
- Full Duplex dialog: It permits two way transmissions by providing a separate communication channel to the both side. The sending and receiving of the message can be done at parallel.

6. Presentation Layer

- The presentation layer deals with the syntax, or grammatical rules, needed for communication between two computers.
- The presentation layer converts system specific data from the application layer into a common, machine independent format that will support a more standardized design for lower protocol layers.
- On the receiving end, the presentation layer converts the machine independent data from the network into the format required for the local system.
- The conversion could use following
  - Bit order translation
  - Byte order translation
  - Character code translation

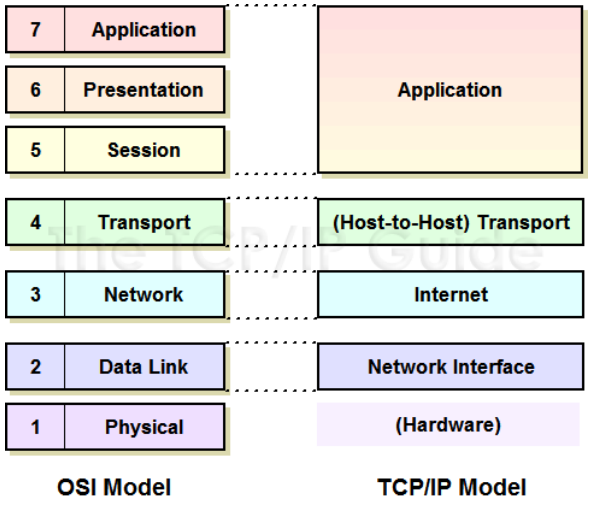
- File syntax translation

7. Application Layer

- The application layer of the OSI reference model is concerned with providing services on the network, including file services, printing services, email services, database service, etc
- Common misunderstanding is that the application layer is responsible for running user application such as word processors.
- The application layer provides an interface whereby applications can communicate with the network.
- The application layer also advertises the available services to network

TCP/IP Model

- The Internet Protocol Suite, TCP/IP, is a suite of protocols used for communication over the internet. The TCP/IP model was created after the OSI 7 layer model for two major reasons.
- First, the foundation of the Internet was built using the TCP/IP suite and through the spread of the World Wide Web and Internet, TCP/IP has been preferred.
- Second, a project researched by the Department of Defense (DOD) consisted of creating the TCP/IP protocols.
- The DOD's goal was to bring international standards which could not be met by the OSI model. Since the DOD was the largest software consumer and they preferred the TCP/IP suite, most vendors used this model rather than the OSI.



- The TCP/IP model, similar to the OSI model, is comprised of layers. The OSI has seven layers and the TCP/IP model has four or five layers depending on different preferences.
- TCP/IP stands for Transmission Control Protocol/Internet Protocol
- TCP/IP defines how electronic devices (like computer) should be connected to internet and how data should be transmitted between them.
- TCP is known as fixed connection, communication between application
- If one application wants to communicate with another, its sends a communication request. TCP will set up 'full-duplex' communication between two application

- The 'full-duplex' communication will occupy separate communication line between the two computer until it is closed by one of the two application
- IP is connection less, communication between computers
- IP does not occupy the communication line between two computers, each line can be used by multiple computers at the same time
- With the help of IP message divide into small independents 'packets' and sent between computers via internet.
- IP is responsible for routing each packets to the correct destination
- TCP/IP is a large collection of different communication protocols based upon the two original protocols TCP and IP are having following other protocols

1. **Application**
   - This layer is comparable to the application, presentation, and session layers of the OSI model all combined into one.
   - It provides a way for applications to have access to networked services. This layer also contains the high level protocols. The main issue with this layer is the ability to use both TCP and UDP protocols.
   - For example TFTP uses UDP because usually on a LAN the physical links are short enough to ensure quick and reliable packet delivery without many errors.
   - SMTP instead uses TCP because of the error checking capabilities. Since we consider our email important information we would like to ensure a safe delivery.

2. **Transport**
   - This layer acts as the delivery service used by the application layer. Again the two protocols used are TCP and UDP.
   - The choice is made based on the application's transmission reliability requirements. The transport layer also handles all error detection and recovery.
   - It uses checksums, acknowledgements, and timeouts to control transmissions and end to end verification. Unlike the OSI model, TCP/IP treats reliability as an end-to-end problem.

3. **Internet**
   - The routing and delivery of data is the responsibility of this layer and is the key component of this architecture.
   - It allows communication across networks of the same and different types and carries out translations to deal with dissimilar data addressing schemes. It injects packets into any network and delivers them to the destination independently to one another.

- Because the path through the network is not predetermined, the packets may be received out of order.
- The upper layers are responsible for the reordering of the data. This layer can be compared to the network layer of the OSI model. IP and ARP6 are the major protocols used at this layer.

4. Network access

- This is a combination of the Data Link and Physical layers of the OSI model which consists of the actual hardware.
- This includes wires, network interface cards, etc. Other related details within this layer are connectors, signal strength, and wavelength along with various others. It will use the required LAN operating algorithms, such as Carrier Sense Multiple Access with Collision Detect (CMSA/CD) or Token Passing etc. and is responsible for placing the data within a frame.
- The frame format is dependent on the system being used, for example Ethernet LAN, Frame relay (packet switching protocol for connecting devices on a Wide Area Network.), etc. The frame is the package that holds the data, in the same way as an envelope holds a letter.
- The frame holds the hardware address of the host and checking algorithms for data integrity. This layer has actually not been specified in details because it depends on which technology is being used such as Ethernet. So freedom is given to this layer as far as implementation is concerned.

TCP/IP Protocol suite

1. TCP (Transmission Control Protocol)

- TCP is used for transmission of data from an application to network
- TCP is responsible for breaking data down into IP packets before they are sent and for assembling the packets when they arrive

2. IP (Internet Protocol)

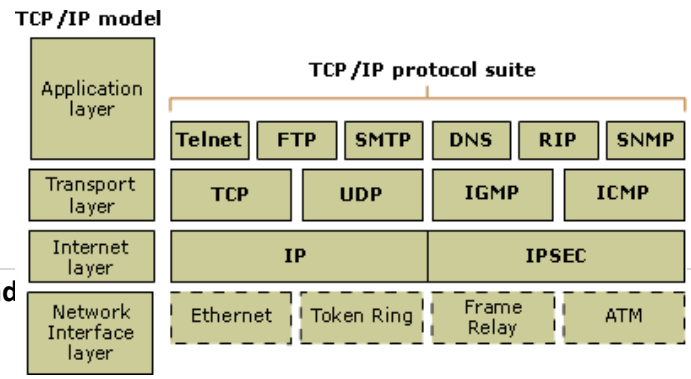
- IP takes care of the communication with other computers
- IP is responsible for sending and receiving data packets over internal

3. HTTP (Hyper Text Transfer Protocol)

- HTTP takes care of the communication between a web server and web browser
- HTTP is used for sending requests from web – client (browser) to web – server, returning web content (web page) from the server back to clients

4. HTTPS (Secure HTTP)

- HTTPs takes care of secure communication



between web server and web browser

- HTTPs typically handles credit card transaction and other sensitive data

5. **SSL (Secure Sockets Layer)**
   - SSL protocols is used for encryption of data for secure data transmission
6. **SMTP (Simple Mail Transfer Protocol)**
   - SMTP is used for transmission email
7. **MIME (Multi Purpose Internet Mail Extension)**
   - MIME protocol lets SMTP transmits multimedia files including voice, audio, and binary data across TCP/IP network
8. **IMAP (Internet Message Access Protocol)**
   - IMAP is used for storing and retrieving emails
9. **POP (Post Office Protocol)**
   - POP is used for downloading emails from an email server to personal computers
10. **FTP (File Transfer Protocol)**
    - FTP take care of transmission of files between computers
11. **NTP (Network Time Protocol)**
    - NTP is used to synchronize time of clock between computers
12. **DHCP (Dynamic Host Configuration Protocol)**
    - DHCP is used for allocation of dynamic IP address to computers in a network
13. **SNMP (Simple Network Management Protocol)**
    - SNMP is used for administration of computers networks
14. **LDAP (Lightweight Directory Access Protocol)**
    - LDAP is used for collection information about users and email address from internet
15. **ICMP (Internet Control Message Protocol)**
    - ICMP handles error and care of error in network
16. **ARP (Address Resolution Protocol)**
    - ARP is used by IP to find the hardware address of computer network card based on IP address
17. **RARP (Reverse Address Resolution Protocol)**
    - RARP is used by IP to find IP address based on hardware address of computer network card.
18. **BOOTP (Boot Protocol)**
    - BOOTP is used for booting (starting) computers from network
19. **PPTP (Point to Point Tunneling Protocol)**
    - PPTP is used for setting up a connection (tunnel) between private networks.

File & Printer Sharing

- File and printer sharing is the part of Microsoft networking that enables you to share files and local printers with other users on small networks.
- If this service is enabled on your Windows computer and you are connected to a Local Area Network (LAN) you are allowing others to connect to your computer and access your files and printer.
- While you can setup passwords to protect your files and printers when using this service, you should know that passwords can provide a false sense of security.
- It is possible for someone to guess your password, or run a program to try all possible passwords.
- If a user on the network gains access to your computer, they may have access to all of your personal information stored on your hard drive.
- Also, with remote access a malicious individual can use your computer to spread viruses or even become a launching pad for attacks on other computers or networks.

Get this working under Windows XP

1. Open the control panel. You will find this by clicking on start, then settings, and then control panel. Click on the icon that says “Network and Internet Connections”
2. Once you are in there. Click on the icon that says “Network Connections”
3. Now you will find your network cards listed here. You will need to right click on the card you want to enable file sharing. Select the properties menu
4. Go to the advanced tab, and click on settings
5. Go to the exceptions menu and make sure file and printer sharing is checked.
6. Click OK. We still have one more step. Microsoft has a feature called “Simple File Sharing”. It should be really called “Broken File Sharing” With this turned on, you cannot access shares unless you give everyone permission. To do this stay in the “Network Connections” Folder click on the tools menu, and select “Folder Options…”
7. Go to the view tab. Scroll down and make sure “Use simple file sharing” is unchecked.
8. Click OK. Sharing is now on
9. One other important note. Make sure you have set a password, or you will always get an access denied message when trying to connect to a remote machine.

Get this working under Windows 7 & 8

1. Click the Start button, type Control Panel, and press Enter.
2. Double-click the Network and Sharing Center icon and then click Change Advanced Sharing Settings.
    a. This step opens the Advanced Sharing Settings page, which lists network settings for each network you’re connected to.
    b. For a home computer running Windows 7: Two networks are listed: Home or Work, and Public.

   c. In Windows 8: The Home or Work network is called Private.
   d. For a computer connected to a domain network: A third network named Domain is listed.
3. Click the down arrow next to the network you want to enable file and printer sharing for.
   a. For a home computer: Click the down arrow next to Home or Work (Windows 7) or Private (Windows 8).
   b. For a computer connected to a domain network: Click the down arrow next to Domain.
4. The figure shows the settings for a Domain network. The settings for a Home or Work network are the same.
5. Do not enable file or printer sharing for the Public network. Enabling file or printer sharing on a public network exposes your computer's data to other users on the same public network.
6. Select the Turn on File and Printer Sharing option.
7. Click the Save Changes button.
8. This action saves your changes and closes the Advanced Sharing Settings page.

Mapping Drive

- Drive mapping is how operating systems, such as Microsoft Windows, associate a local drive letter (A through Z) with a shared storage area to another computer over a network.
- After a drive has been mapped, a software application on a client's computer can read and write files from the shared storage area by accessing that drive, just as if that drive represented a local physical hard disk drive.

Get this working under Windows XP

1. Open Windows Explorer or My Computer from the Windows Start Menu.
2. From the Tools menu, click Map Network Drive…. A new Map Network Drive window opens.
3. In the Map Network Drive window, choose an available drive letter from the dropdown list located next to the "Drive:" option. Any drives already mapped will have a shared folder name displayed inside the dropdown list, next to the drive letter.
4. Type the name of the folder to map. This name must follow UNC. Alternatively, click the Browse… button to find the correct folder by browsing available network shares.
5. Click the "Reconnect at login" checkbox if this network drive should be mapped permanently. Otherwise, this drive wills un-map when the user logs out of this computer.

6. If the remote computer that contains the shared folder requires a different username and password to log in, click the "different user name" hyperlink to enter this information.
7. Click Finish.
8. If the drive letter was previously mapped to a different location, a message box will appear asking to replace the current connection with the new one. Click Yes to disconnect and un-map the old mapped drive.
9. If the Finish operation succeeds, the network drive will be mapped. If the network drive cannot be mapped, ensure the folder name is spelled correctly, that this folder was correctly set up for sharing on the remote computer, that (if necessary) the correct username and password have been entered, and that the computer network connections are functioning properly.

Get this working under Windows 7

1. Open the Computer window by choosing Computer.
2. Click the Map Network Drive button on the toolbar to open the Map Network Drive dialog box.
3. To be able to map a network folder to a local drive, the folder must be shared and you must have network permission to access it on the other computer.
4. Select an unused drive letter for the network folder in the Drive drop-down list.
5. In the Folder text box, enter the network share pathname. When you're done, click OK.
6. You can type the path like the \\server\share example shown, or you can click the Browse button and locate the shared network folder. If you want to select a previously mapped folder, you can select it from the drop-down list of previously entered pathnames.
7. (Optional) Select the Reconnect at Logon check box to tell Windows to map this same drive every time you start the computer.
8. Also, if you're not an administrator, select the Connect Using Different Credentials check box. Then ask an administrator on your network to enter their username and password in the Windows Security dialog box that appears before you click OK.
9. Click the Finish button.
10. When you click Finish, Windows creates the network drive and automatically opens it in Windows Explorer. After that, you can access any of the folder's subfolders and files by simply opening the network drive in the Computer window.

Disk Quota

- A disk quota is a limit set by a system administrator that restricts certain aspects of file system usage on modern operating systems. The function of using disk quotas is to allocate limited disk space in a reasonable way.

- There are two basic types of disk quotas. The first, known as a usage quota or block quota, limits the amount of disk space that can be used. The second, known as a file quota or inode quota, limits the number of files and directories that can be created.
- In addition, administrators usually define a warning level, or soft quota, at which users are informed they are nearing their limit that is less than the effective limit, or hard quota. There may also be a small grace interval, which allows users to temporarily violate their quotas by certain amounts if necessary.

Get this working under Windows 7

1. Open the Computer window, right click or press and hold on the NTFS formatted hard disk (ex: my F drive) that you want to disable all quota limits on for all users, and click/tap on Properties.
2. Click/tap on the Quota tab, and click/tap on the Show Quota Settings button.
3. If prompted by UAC, click/tap on Yes (Windows 7/8) or Continue.Check the Enable quota management box, and click/tap on Apply.
4. Click/tap on OK.
5. If you would like to deny disk space to users exceeding quota limit, then checkthis box. NOTE: Checking this box will prevent a user from being able to save anything to the selected hard disk (step 1) when they exceed their quota limit.

Encryption

- Encryption is the conversion of data into a form, called a ciphertext that cannot be easily understood by unauthorized people.
- Decryption is the process of converting encrypted data back into its original form, so it can be understood.
- The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a code, can be employed to keep the enemy from obtaining the contents of transmissions.
- Technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII.
- Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.
- In order to easily recover the contents of an encrypted signal, the correct decryption key is required.
- The key is an algorithm that undoes the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to break the cipher.

- The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key.
- Network encryption (sometimes called network layer or network level encryption) is a network security process that applies crypto services at the network transfer layer - above the data link level, but below the application level.
- The network transfer layers are layers 3 and 4 of the Open Systems Interconnection (OSI) reference model, the layers responsible for connectivity and routing between two end points.
- Using the existing network services and application software, network encryption is invisible to the end user and operates independently of any other encryption processes used.
- Data is encrypted only while in transit, existing as plaintext on the originating and receiving hosts.
- Network encryption is implemented through Internet Protocol Security (IPSec), a set of open Internet Engineering Task Force (IETF) standards that, used in conjunction, create a framework for private communication over IP networks.
- IPSec works through the network architecture, which means that end users and applications don't need to be altered in any way. Encrypted packets appear to be identical to unencrypted packets and are easily routed through any IP network.

Compression

- Compression is the reduction in size of data in order to save space or transmission time. For data transmission, compression can be performed on just the data content or on the entire transmission unit (including header data) depending on a number of factors.
- Content compression can be as simple as removing all extra space characters, inserting a single repeat character to indicate a string of repeated characters, and substituting smaller bit strings for frequently occurring characters.
- This kind of compression can reduce a text file to 50% of its original size. Compression is performed by a program that uses a formula or algorithm to determine how to compress or decompress data.
- Graphic image file formats are usually designed to compress information as much as possible (since these can tend to become very large files). Graphic image compression can be either lossy (some information is permanently lost) or lossless (all information can be restored).
- When you send or receive information on the Internet, larger text files, either singly or with others as part of an archive file, may be transmitted in a zip, gzip, or other compressed format.

NetMeeting

- Microsoft introduced the NetMeeting application to allow for VoIP communications and video conferencing. NetMeeting used the H.323 protocol for video conferencing.
- It also allowed for application and desktop sharing, remote desktop sharing and transfer of files between client computers.
- NetMeeting was available for use starting with later versions of Internet Explorer 3 and Windows 95 OSR2 and continued up through Windows XP.
- NetMeeting was one of the most popular applications for video conferencing, until free video conferencing capabilities began to be introduced in applications like Yahoo! Messenger and MSN Messenger.
- Microsoft changed course at this point and focused on Windows Messenger and Microsoft Office Live Meeting for its offering of video conferencing capabilities.

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. An icon will be displayed on the desktop. (During startup, if Windows XP Firewall attempts to block NetMeeting, click Unblock.

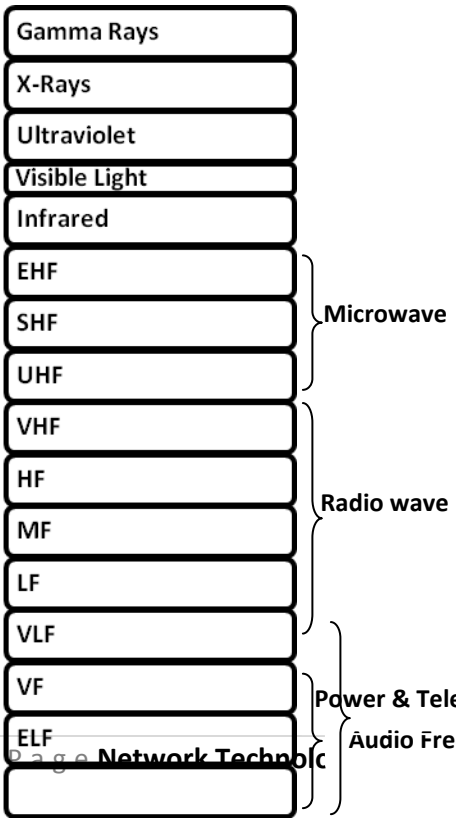
Chapter 2: Transmission Media

Introduction

- Transmission media enable computer to send and receive message but, as it human communication, do not guarantee that the message will be under stood.
- One broad classification of this transmission media is known as bounded media or cable media. This include cable type such as coaxial cable, shielded twisted pair cable unshielded twisted-pair cable, and fiber-optic cable.
- Another type of media is known as boundless media, these media include all forms of wireless communication.

Transmission Frequencies

- Transmission media make possible the transmission of the electronic signals from one computer to another.These electronic signals express data value in the form of binary (on/off) impulses which are the basic for all computer information represented as 1's or 0's.
- All signal transmitted between computer consist of some form of electromagnetic waveform, ranging from radio to frequencies through microwave and infrared light.
- Different media are used to transmit the signals, depending on the Frequency of the EM wave form. Illustrates the range of electromagnetic wave forms known as the electromagnetic spectrum and their associated Frequencies



- EHF- Extremely High Frequency
- SHF-Super High Frequency
- UHF-Ultra High
- UHF-Very High Frequency
- HF-High Frequency
- MF-Medium Frequency
- LF-Low Frequency
- VLF-Very Low Frequency
- VF-Voice Frequency
- ELF-Extremely Low Frequency

Transmission Media Characteristics

1. Bandwidth

- Bandwidth describes the maximum data transfer rate of a network or Internet connection. It measures how much data can be sent over a specific connection in a given amount of time.
- For example, a gigabit Ethernet connection has a bandwidth of 1,000 Mbps, (125 megabytes per second). An Internet connection via cable modem may provide 25 Mbps of bandwidth.
- While bandwidth is used to describe network speeds, it does not measure how fast bits of data move from one location to another.
- Since data packets travel over electronic or fiber-optic cables, the speed of each bit transferred is negligible (unimportant). Instead, bandwidth measures how much data can flow through a specific connection at one time.

2. Band Usage (Baseband&Broadband)

- The two ways to allocate the capacity of transmission media are baseband& broadband transmission.
- Baseband devotes the entire capacity of the medium to one communication channel.Broadband enable two or more communication channels to share the band width of the communication medium.
- Where as in other cases for example TV cable is television signal can share the band width of the cable because each signal is modulated using a separate given frequency.
- This technique of dividing bandwidth into frequency bands is called Frequency Division Multiplexing (FDM) and works only with analogy signals, another technique called Time Division Multiplexing (TDM) support digital signals.

3. Attenuation

- Attenuation[ii] is measure to see new much a signal getting weaker as it travels through a medium.Attenuation is a factor why cable designs must specify limits in the length of cable runs.
- When signal strength falls below certain limits, the electronic equipment that receives the signal from the voice present in all electronic transmissions.
- The best example is radio signal.You can lock the signal on your radio but generally it still contain move voice that sound from radio station.

4. Electro Magnetic Interface(EMI)

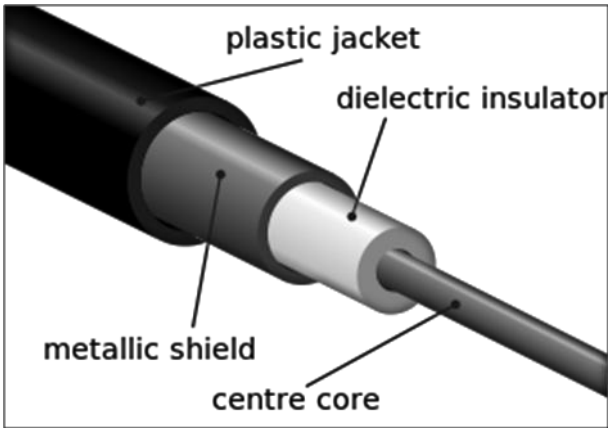
- EMI consists of outside electromagnetic noise that distorts[iii] the signal in a medium.

- Crosstalk is a special kind of interference caused by adjacent wires.Crosstalk is cure when the signal from one wire is picked up by another wire.
- You may have experienced this when talking on a telephone and hearing another conversation going on in the background.
- Crosstalk is a particularly significant problem with computer network because large number of cables oftenlocated close together

Transmission Cable (Guided Media)

1. Coaxial Cable

- Coaxial cables were the first cable type used in LANs. The cable is most frequency referred to as a "coax"
- The components of a coaxial cable are center conductor it is made up of solid copper wire and outer conductor it is the tube surrounding the center conductor.

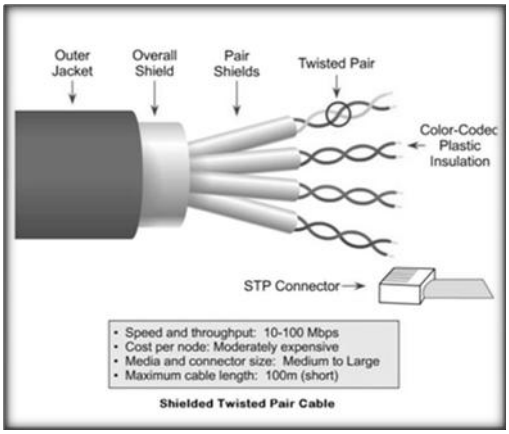


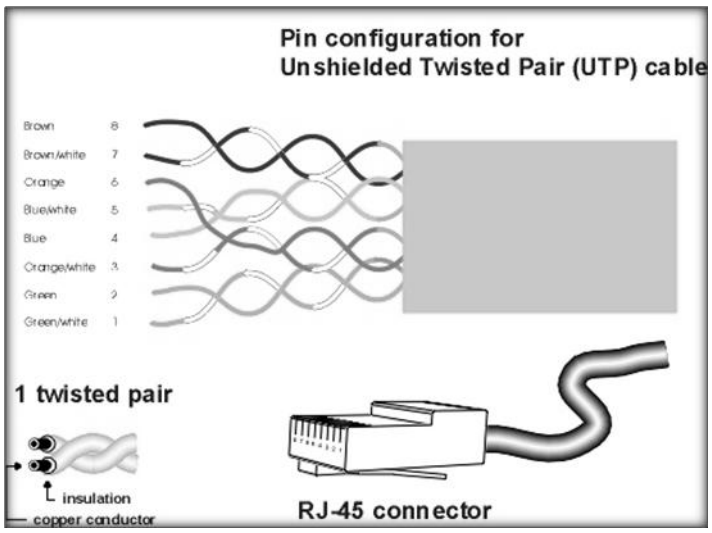
- Coaxial cables are available of two types, Thinnet and Thicknet.
- Thinnest is a light and flexible cabling medium that is inexpensive and easy to install.
- It is approximately 0.25 inches (6mm) in thickness and having 50 ohm impedance. It can transmit a signal for 185 meter (610 feet).
- Thicknet is relative more expensive comparing to the think net.
- It is approximately of 0.5 inches (13 mm). It can transmit the data up to 500 meters (1650feet). It is generally used to connect two or more think net network.

2. Twisted Pair cable

- Cable is widely used in computer networking because of several reasons.
- The twisted pair cable is inexpensive to install and offers lowest cost per foot then any cable. The best example of twisted pair cable is the telephone cable.
- It consists of two standard copper wire twisted together. The twisting of cable reduces the EMI & also controls the tendency of the wire to cause EMI in each other.
- Twisted cable are also available of two types, Shielded twisted pair cable (STP) and Unshielded twisted pair cable (UTP)
- Twisted cable consist of one or more twisted pairs of cable enclosed in a foil wrap & woven copper shield.

- In the early LAN shielded twisted pair cable was widely used because of the shield performs double duty. It will reduce the tendency of cable to radiate EMI and reduce the cable sensitivity to outside interference.
- UTP does not incorporate a braided shield into its structure.
- The characteristic of UTP are similar to the STP but the difference is in attenuation and EMI.
- Server twisted pair can be bundled together in a signal cable, these pairs are typically color-coded.
- UTP are having different categories considering the transfer rate.
- Category (CAT) 1 and 2, generally used for voice data transmission at low data rate approximately at 4MBPS.
- CAT 3, generally used for data transmission at low rate, approx at 10MBPS
- CAT 4 can transmit the data at 16 mbps.
- CAT 5 transmits the data at 100MBPS which consist of 4 twisted pair cable. Current widely used in LAN.
- CAT 6 can transmit the data at 1GBPS; it is being replaced by CAT 5.
- The connector used for CAT 5 & CAT 6is RJ45 having 8 pins for computer networking and RS 11 having 2 pins used for telephone networking.

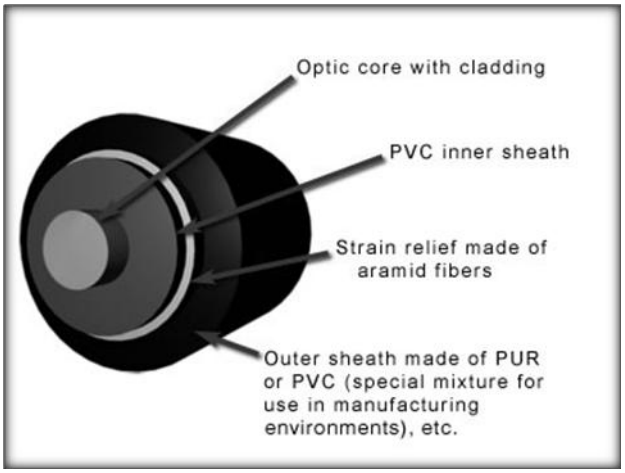




3. Fiber Optic Cable

- Fiber optic cable is the ideal cable for data transmission
- The cable accommodates extremely high bandwidths, and also presents no problems with EMI and supports durable cables & cable runs as long as several kilometers.
- The center conductor is consists of highly refined glass or plastic deigned to transmit light signals with very little loss.
- A glass core support a longer cabling distance, but a plastic core is typically easier to work with.

- The fiber is coated with a cladding or a gel that reflect signal back into the fiber to reduce signal loss.



Cable Type	Cost	Installation	Capacity	Range	EMI
Coaxial Thinnet	<STP	Inexpensive & easy	Avg.10Mbps	185m	< sensitive than UTP
Coaxial Thicknet	>STP <Fiber	Easy	Avg. 10Mbps	500m	< sensitive than UTP
STP	>UTP < Thicknet	Fairly easy	16Mbps to 500Mbps	100m	< sensitive than UTP
UTP	Lowest	Inexpensive & easy	10Mbps to 100Mbps	100m	Most sensitive
Fiber Optic	Highest	Expensive & difficult	100Mbps	10's of Kilometer	Insensitive

Wireless Media (Unguided Media)

- Wireless media may require when space for cabling is not available or inconvenient. These include open lobbies, inaccessible parts of buildings, older buildings, historical buildings where renovation is prohibited and outdoor installations.
- People who move around a lot within their work environment i.e. network admission, sales man, etc.
- Temporary installation for only temporary department which will be relocated very soon.
- Satellite offices or branches, ships in the ocean, or teams in remote field that need to be connected to a main office or location.

1. **Infrared Transmission**
   - We use an infrared communication system time we control our television with a remote control.
   - The remote control transmits pulses of infrared light that carry coded instruction to a receiver into 4 verity

- **Broadband optical telephone:** this method uses broadband technology. Data transfer rates in this high-end option are competitive with those for a cable-based network.
- **Line-of-signal infrared:** Transmission must occur over a clear line of signal path between transmitter and receiver.
- **Reflective infrared:** It will transmit toward a common, central until they finally reach the receiver.
- **Scatter infrared:** Transmission reflects of floors, wall and Calling until they finally reach the receiver. Because of the imprecise trajectory, data transfer rates are slow. The maximum reliable is around 100 feet.

2. **Laser**
   - High-power laser transmitter can transmit data for several thousand (1000 yard) when line-of-signal communication is possible.
   - On a LAN laser light technology is similar to infrared technology.

3. **Narrow-band radio transmission**
   - In narrow-band radio communication occult at a signal radio frequency.
   - The range of narrow-band radio is grater then that of infrared, effectively enabling mobile computing over a limited area.
   - The receiver and transmitter are not required to place in a direct line of site.
   - The signal can bounce off walls buildings, and even the atmosphere, but heavy wall, such as steel or concrete can block the signal.
4. **Microwave**
   - Microwave technology has applications in all three of the wireless networking scenarios: LAN, extended LAN, and mobile networking.
   - Microwave communication can take two forms: terrestrial (ground) links and satellite links. The frequencies and technologies employed by these two forms are similar.
   - **Terrestrial Microwave**:
     - Terrestrial microwave communication employs Earth-based transmitters and receivers.
     - The frequencies used are in the lowgigahertz range, which limits all communications to line-of-sight.
     - You probably have seen terrestrial microwave equipment in the form of telephone relay towers, which are placed every few miles to relay telephone signals cross-country.
     - Microwave transmissions typically use a parabolic antenna that produces a narrow, highly directional signal. Terrestrial microwave systems operate in the low-gigahertz range, typically at 4–6 GHz and 21–23 GHz, and costs are highly variable depending on requirements.

- Long-distance microwave systems can be quite expensive but might be less costly than alternatives.
- Properly designed systems are not affected by attenuation under normal operational conditions—rain and fog, however, can cause attenuation of higher frequencies.
- Microwave systems are highly susceptible to atmospheric interference and also can be vulnerable to electronic eavesdropping.

- **Satellite Microwave**:
  - Satellite microwave systems relay transmissions through communication satellites that operate in geosynchronous orbits 22,300 miles above the earth.
  - Satellites orbiting at this distance remain located above a fixed point on earth. Earth stations use parabolic antennas (satellite dishes) to communicate with satellites.
  - These satellites then can retransmit signals in broad or narrow beams, depending on the locations set to receive the signals. When the destination is on the opposite side of the earth, for example, the first satellite cannot transmit directly to the receiver and thus must relay the signal through another satellite.
  - As no cables are required, satellite microwave communication is possible with most remote sites and with mobile devices, which enables transmission with ships at sea and motor vehicles. The time required for a signal to arrive at its destination is called propagation delay.
  - The delays encountered with satellite transmissions range from 0.5 to 5 seconds. Unfortunately, satellite communication is extremely expensive. Building and launching a satellite can cost easily in excess of a billion dollars.
  - Satellite links operate in the low-gigahertz range, typically at 11–14 GHz. Costs are extremely high and usually are distributed across many users by selling communication services.

5. Bluetooth

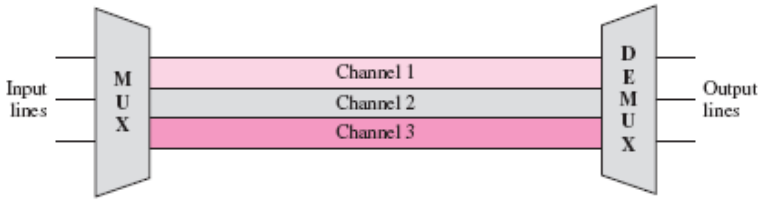
- Bluetooth is a specification (IEEE 802.15.1) for the use of low-power radio communications to link phones, computers and other network devices over short distances without wires.
- The name Bluetooth is borrowed from Harald Bluetooth, a king in Denmark more than 1,000 years ago.
- Bluetooth technology was designed primarily to support simple wireless networking of personal consumer devices and peripherals, including cell phones, PDAs, and wireless headsets.

- Wireless signals transmitted with Bluetooth cover short distances, typically up to 30 feet (10 meters). Bluetooth devices generally communicate at less than 1 Mbps.
- Bluetooth networks feature a dynamic topology called a *piconet* or *PAN*. Piconets contain a minimum of two and a maximum of eight Bluetooth peer devices.
- Devices communicate using protocols that are part of the Bluetooth Specification. Definitions for multiple versions of the Bluetooth specification exist including versions 1.1, 1.2 and 2.0.
- Bluetooth technology is not a suitable Wi-Fi replacement. Compared to Wi-Fi, Bluetooth networking is much slower, a bit more limited in range, and supports many fewer devices.

Multiplexing

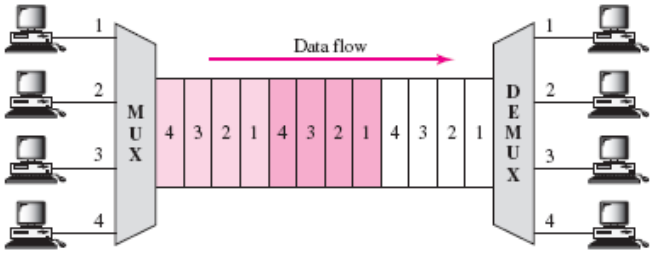
- It enables broadband media to support multiple data channels i.e. single media can pass multiple data at same time
- It helps when media costly, bandwidth is idle, when large amount of data to sent from low capacity channels.
- Demultiplexing is separating two or more signals that have been combined into one signal.
- Demultiplexing is the extraction of the original channels on the Receiver side. A device that performs the Demultiplexing process is called a Demultiplexer (DEMUX).

1. FDM



- In this any signal will convert to analog. Each analog signal can be modulated by separate frequency called 'carrier frequency' which helps to recover the original signal on opposite end
- One advantage of FDM is that, it supports bidirectional signaling on the same time i.e. transmission of data can be done from both side of cable at the same time

2. TDM



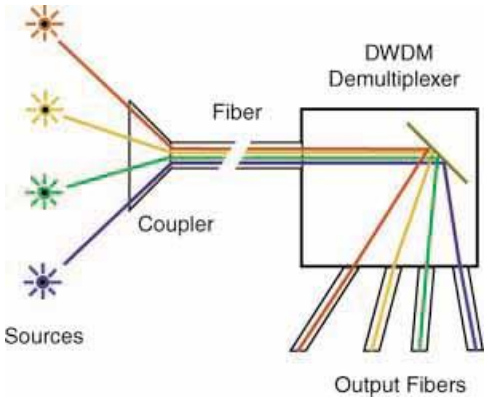
- Time division multiplexing divides a channel into time slots that are allocated to data streams to be transmitted. It will transmits the multiplexed signal in baseband mode
- TDM equipments utilize fixed time division and allocate time to channel.
- If channel is free then full utilized is not done as the time division are programmed into configuration of multiplexer this often known as synchronous TDM
- For fully utilization of medium, if channel is free then statistical time division multiplexing can be use (StatTDM)
- StatTDM allocates time slots based on traffic demand on the individual channels i.e. if data to be passed then time slots will be given else not.

3. CDM

- Code division multiplexing (CDM) is a networking technique in which multiple data signals are combined for simultaneous transmission over a common frequencyband.

- When CDM is used to allow multiple users to share a single communications channel, the technology is called code division multiple access (CDMA).
- CDMA uses spread spectrum, a technology that was developed in World War II to prevent enemies from intercepting and jamming transmissions. In spread spectrum, a data signal is sent over a range of frequencies in an assigned frequency spectrum.
- A pseudo-random spreading code is used to multiplex the base signal. Multiplexing with a spreading code increases the bandwidth required for the signal, spreading it out over the available spectrum. The receiving device is aware of the spreading code and uses it to demultiplex the signal.
- CDMA provides a certain amount of built-in security, as the transmissions of multiple users are mixed together within the frequency spectrum. The spreading code is required to decode a specific transmission.

4. WDM

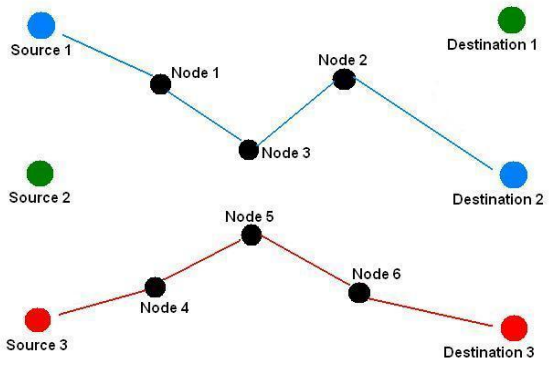


- In fiber-optic communications, wavelength-division multiplexing (WDM) is a technology which multiplexes a number of optical carrier signals onto a single optical fiber by using different wavelengths (i.e. colors) of laser light.
- This technique enables bidirectional communications over one strand of fiber, as well as multiplication of capacity.
- Wavelength-division multiplexing (WDM) is a method of combining multiple signals on laser beams at various infared (IR) wavelengths for transmission along fiber optic media.
- Each laser is modulated by an independent set of signals. Wavelength-sensitive filters, the IR analog of visible-light color filters, are used at the receiving end.
- WDM is similar to frequency-division multiplexing (FDM). But instead of taking place at radio frequencies (RF), WDM is done in the IR portion of the electromagnetic spectrum.
- Each IR channel carries several RF signals combined by means of FDM or time-division multiplexing (TDM). Each multiplexed IR channel is separated, or demultiplexed, into the original signals at the destination.
- Using FDM or TDM in each IR channel in combination with WDM or several IR channels, data in different formats and at different speeds can be transmitted simultaneously on a single fiber.

Switching Techniques

- Switching techniques are mechanism for moving data from one network segment to another.Switching technique is of three types circuit switching, message switching and packet switching.

1. Circuit Switching

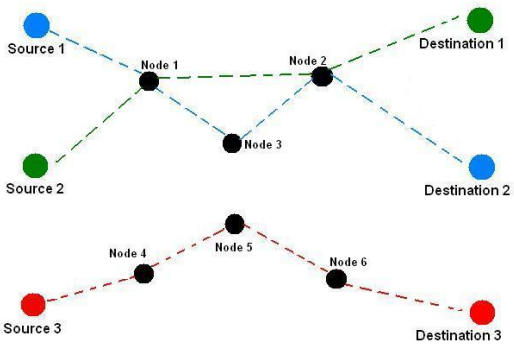


- Circuit switching establishes dedicated path for the transmission until the transmission is completed.
- It much works as the telephone system.The transmission line is freed, when connection is hang off till then no other can use that line even no transmission is made
- Secondly to select any dedicated path it is time consuming. As line cannot be shared with other bandwidth might be inefficiently utilized

2. Message Switching

- In the message switching each message treats as an independent entity.
- Every time when new message to be send, it will find the new path and will transfer the complete message from that.
- When message transmission is completed its dedicated line is freed for other.
- Another advantage is that switches can store message until a channel becomes available, which reduces sensitivity over network congestion
- Message priorities can also be set to manage network traffic.

3. Packet Switching



- In packet switching message are divided into smaller pieces called packets.
- Each packets store source and destination address information so that individual packets can be routed through the network independently.Every packet can select its own path to transfer data.
- As message divide into packet, provides speedy transmission as various path can be taken for single message transmission.Packet switching is of two types datagram switching and virtual circuit switching.

Hubs

- Hubs are known as wiring concentrators which provides central attachment point for network cabling. Hubs comes in three types : Passive, Active and Switching

1. **Passive**
   - It is oldest technique for network cabling as it does not contain any electronic components.
   - No data correction, no repeating of signal, no routing algorithm was done by this kind of hubs
   - They work like an on/off electric switch from where all signals are transmitted and received.If switch is on transmission is done. If off then no transmission
2. **Active Hub**
   - Active is having electronic components that can amplify the signal that flow between devices on network.
   - The main advantage can be its is robust for network and distance between devices can be increased
   - Active hub also act as repeater so separate repeater is not required. But they are much expensive then passive hubs
3. **Intelligent Hubs**
   - Switches are known as intelligent hubs
   - It is intelligent because of tow reason, first that administrator can order that hub to shutdown connection (terminate connection) which generate network error repeatedly
   - Secondly it also works like bridge i.e. it will transfer the data only to port at which receiving device is connected not to all. It will maintain routing table same like a bridge
   - Also it provide much better speed compare to passive and active hub as data not to transferred to all ports.

NIC (Network Interface Card)

- Most important device in network is NIC. Each computer on network must have at least one NIC installed.
- NIC provides connectivity between PC and network physical medium (cable)
- Most of new motherboard are having network interface integrated with motherboard, older computers may not have integrated so it is to be installed separately
- They also handle an important data conversion function. Data travels in parallel on PCI bus system, but network medium demands serial transmission
- NIC also have ability of supplying basic addressing system that can be used to get data from one computer to another on network

- The hardware or MAC address is burned into ROM chip on NIC, this is referred as MAC address because media access control layer is actually sub layer of OSI's data link layer.
- Basic NIC types are gigabit Ethernet interface, controller interface, serial interface, dialer interface, loopback interface, tunnel interface and ATM interface.

Modems

- Standard telephone lines can transmit signals in analog. Computer transmits signals in digital.
- Modem can transmit digital computer signals over telephone lines by converting them to analog form.
- Converting signals from digital to analog is called modulation. Recovering analog to digital for original signal is call demodulation
- So the modem word derives from modulation/ demodulation
- A **Digital Subscriber Line (DSL) modem** is a device used to connect a computer or router to a telephone line which provides the digital subscriber line service for connectivity to the Internet, which is often called DSL broadband.
- The term DSL modem is technically used to describe a modem which connects to a single computer, through a USB port or is installed in a computer PCI slot. The more common DSL router which combines the function of a DSL modem and a home router is a standalone device which can be connected to multiple computers through multiple Ethernet ports or an integral wireless access point. Also called a residential gateway, a DSL router usually manages the connection and sharing of the DSL service in a home or small office network.
- Short for **Asymmetric Digital Subscriber Line**, ADSL is a type of DSL broadband communications technology used for connecting to the Internet. ADSL allows more data to be sent over existing copper telephone lines (POTS), when compared to traditional modem lines. A special filter, called a micro filter, is installed on a subscriber's telephone line to allow both ADSL and regular voice (telephone) services to be used at the same time. ADSL requires a special ADSL modem and subscribers must be in close geographical locations to the provider's central office to receive ADSL service. Typically this distance is within a radius of 2 to 2.5 miles. ADSL supports data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).

Repeater

- The purpose of repeater to extend the range of network cable
- The repeater will repeat the signal from one point to another point with higher strength of signals.

- It operates at physical layer in OSI model. It does not require sender and receiver address to transmit the signal
- The main limitation of repeater is that is merely repeats the signal, filter or correction of data is not done.
- If data is corrupted that also will be regenerated even broadcast storm caused by malfunctioning adapter will be repeated.
- Although they cannot connect network having different data frame format also not able to connect even if data frame is same but cabling is dissimilar.
- Main thing to be remember is propagation delay i.e. time taken by signal to reach farthest point on network.
- If propagation delay is more than normal time no signal are encountered then network error condition is assumed
- The main and only advantage of repeater is that it is inexpensive and easy for installation.

Switches

- **Unmanaged switches**: This is the most basic type of switch. It provides basic connectivity between networked devices, such as PCs, servers and storage, at a low cost. However, these are set-it-and-forget-it switches that aren't capable of changing settings or functions. They tend to be easy to use and best for simple connectivity.
- **Web-managed switches**: These switches, also called smart switches, are for networks with up to 200 computers. They have a graphical user interface with easy-to-understand controls and are managed via a web browser. They provide a lot of guidance to users and are designed for those who have no advanced network training. They can support a limited number of VLANs.
- **Fully managed switches**: These switches also have a GUI and use a web browser, but they also have a command line interface, which allows network engineers to create scripts to program and manage multiple switches. Fully managed switches have a full suite of capabilities including link aggregation, traffic prioritization and security features that can be used to shape the behavior of traffic on the network.

Bridge

- Bridge controls the data flow direction, whereas repeater transfer every data it receive whether receiving device is available or not on opposite side.
- Bridge comes in two main forms transparent or learning bridge another is source routing bridge.

1. **Transparent Or Learning Bridge**
   - These types of bridge are transparent to the device sending the packet
   - The bridge will learn over a period of time which device exists on each side of it.

- This is done by reading data link information of each packet passing through it.
- The bridge will analyze the MAC address of packet and build the table of device of each side.

2. **Source Routing Bridge**
   - This kind of bridge divide busy network into smaller segments.
   - Source routing bridge is used in token ring network.Bridge also read the information of packet and decide whether to pass the data in token ring or not.
   - If network accounting and sales are department, which are overloaded, then we can divide logically segment that network into two networks
   - Only when accounting and sales want to communicate bridge will allow the packet to be sent.

Router

- Bridges are suitable for relatively simple network, but bridges have certain limitations which are advantages of router.
- Bridge will transfer packet to every device on that segment, only correct receiver will able to accept that packet.
- In many case the bridge might start transfer the packet in loop which increase the network traffic.
- Bridge cannot find fastest route to pass the packet over the multiple interconnected segment.
- Bridge fails to transfer the packet on different cabling network as bridge work on data link information i.e. physical device.
- The above limitation of bridge is removed in router and they are advantage of it.
- Routers are generally used for wide area network, having different cabling, platform, and multiple segment of network virtually or physical.
- Static router do not determine path, instead administrator have to configure the routing table specifying potential routes for packets.
- In dynamic router, router itself has capability to determine routes and to find optimum path among redundant routes based on packet information and information received from other router.

Layer 3 Switch

- A Layer 3 switch is a high-performance device for network routing. Layer 3 switches actually differ very little from routers. A Layer 3 switch can support the same routing protocols as network routers do.
- Both inspect incoming packets and make dynamic routing decisions based on the source and destination addresses inside. Both types of boxes share a similar appearance.
- Layer 3 switches were conceived as a technology to improve on the performance of routers used in large local area networks (LANs) like corporate intranets.

- The key difference between Layer 3 switches and routers lies in the hardware technology used to build the unit.
- The hardware inside a Layer 3 switch merges that of traditional switches and routers, replacing some of a router's software logic with hardware to offer better performance in some situations.

Brouter

- A brouter (pronounced BRAU-tuhr or sometimes BEE-rau-tuhr) is a network bridge and a router combined in a single product.
- A bridge is a device that connects one local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring).
- If a data unit on one LAN is intended for a destination on an interconnected LAN, the bridge forwards the data unit to that LAN; otherwise, it passes it along on the same LAN.
- A bridge usually offers only one path to a given interconnected LAN. A router connects a network to one or more other networks that are usually part of a wide area network (WAN) and may offer a number of paths out to destinations on those networks.
- A router therefore needs to have more information than a bridge about the interconnected networks. It consults a routing table for this information.
- Since a given outgoing data unit or packet from a computer may be intended for an address on the local network, on an interconnected LAN, or the wide area network, it makes sense to have a single unit that examines all data units and forwards them appropriately.

Gateway

- A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node.
- Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.
- In the network for an enterprise, a computer server acting as a gateway node is often also acting as a proxy server and a firewall server.
- A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.
- A gateway is a node that allows you to gain entrance into a network and vice versa. On the Internet the node which is the stopping point can be a gateway or a host node.

- A computer that controls the traffic your network or your ISP (Internet Service Provider) receives is a node. In most homes a gateway is the device provided by the Internet Service Provider that connects users to the internet.
- When a computer server serves as a Gateway node, the gateway node also operates as a firewall and a proxy server. A firewall is a system created to prevent unauthorized admission into a private network.
- A proxy server is located right between a client application such as a web browser and the real server. The proxy server sees if the client applications requests can be carried out by the real server.

Chapter 3: Network Protocols

Packets

- Packets is one unit of binary data capable of being routed through a computer network
- To improve communication performance and reliability each message sent between two network devices is often sub divided into packets by underlying hardware and software
- Packets are constructed in some standard packet format. Packets formats generally include a header, body containing the message data (also known as pay load) and sometimes a footer (also known as trailer)
- Packet header lists the destination of packets and often indicates the length of message data.
- Packet footer contains data that signifies the end of packet, such as a special sequence of bits known as magic number
- Both packet header and footer may contain error checking information.
- The receiving device is responsible for re-assembling individual packets into the original message, by stripping off the headers and footers and concatenating packets in correct sequence.

Protocols

- A network protocol defines rules and conventions for communication between network devices.
- Packets for computer networking all generally use packet switching techniques to send and receives message in the form of packets.
- Network protocols include mechanisms for devices to identify and make connections with each other as well as formatting rules that how data packed into packets.
- Some protocols also support message acknowledgements and data compression.
- Hundreds of different computer network protocols have been developed each one with specific purpose and environments.

There are two types of Internet Protocol (IP) traffic. They are **TCP** or **Transmission Control Protocol** and **UDP** or **User Datagram Protocol**. TCP is connection oriented – once a connection is established, data can be sent bidirectional. UDP is a simpler, connectionless Internet protocol. Multiple messages are sent as packets in chunks using UDP.

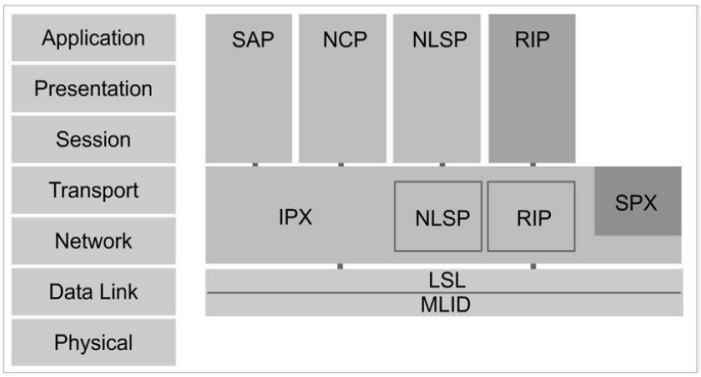
	TCP	**UDP**
Acronym for	Transmission Control Protocol	User Datagram Protocol or Universal Datagram Protocol
Connection	TCP is a connection-oriented	UDP is a connectionless protocol.

	TCP	UDP
	protocol.	
Function	As a message makes its way across the internet from one computer to another. This is connection based.	UDP is also a protocol used in message transport or transfer. This is not connection based which means that one program can send a load of packets to another and that would be the end of the relationship.
Usage	TCP is suited for applications that require high reliability, and transmission time is relatively less critical.	UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.
Examples	HTTP, HTTPs, FTP, SMTP, Telnet	DNS, DHCP, TFTP, SNMP, RIP, VOIP.
Ordering of data packets	TCP rearranges data packets in the order specified.	UDP has no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer.
Speed of transfer	The speed for TCP is slower than UDP.	UDP is faster because there is no error-checking for packets.
Reliability	There is absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent.	There is no guarantee that the messages or packets sent would reach at all.
Header Size	TCP header size is 20 bytes	UDP Header size is 8 bytes.
Common Header Fields	Source port, Destination port, Check Sum	Source port, Destination port, Check Sum
Weight	TCP is heavy-weight. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP is lightweight. There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP.
Data Flow Control	TCP does Flow Control. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP does not have an option for flow control
Error Checking	TCP does error checking	UDP does error checking, but no recovery options.
Acknowledgement	Acknowledgement segments	No Acknowledgment
Handshake	SYN, SYN-ACK, ACK	No handshake (connectionless protocol)

	TCP	UDP
Checksum	No checksum	to detect errors

IPX/SPX

- Internet Packet Exchange / Sequenced Packet Exchange is proprietary protocol stack developed by Novell and based on Xerox Network System (XNS) protocol
- IPX and SPX are derived from XNS, IDP and SPP protocols. IPX is network layer protocols (Layer 3 of OSI Model) while SPX is transport layer protocol (layer 4 of OSI Model).
- IPX and SPX both provide connection services similar to TCP/IP. IPX protocol having similarities of IP and SPX having similarities to TCP
- IPX/SPX was primarily designed for Local Area Network (LAN) and was very efficient protocol for that purpose
- But TCP/IP become De-Facto standard protocol, due to that it provide superior performance in Wide Area Network (WAN) and TCP/IP is a more mature protocol designed specifically with this purpose in mind
- Addressing in IPX/SPX is much similar to TCP/IP. IPX/SPX also have two distinct addresses a host address and network address
- The host address based on hardware address of network adapter card used by device attaching to network (LAN Card).
- These address are hexadecimal in nature
- Network address, logical address is assigned by the administrator of the cable segment when a server or router is installed
- Network address is generally is of eight character hexadecimal address
- Example 55-66-00-e4-7a:e8022000 another example 44-45-53-54-00:00beee00
- First part is host address before colon sign, second part is network address after colon sign



IPX/SPX Protocol Suite Mapped to OSI Reference Model

- Service Advertisement Protocol (SAP): This protocol is used by various servers, such as file and print servers, to publicize their IPX addresses and services.
- Netware Core Protocol (NCP): This protocol is used to make server functions, such as file and print sharing, available to clients.
- Internetwork Packet Exchange (IPX): This protocol provides fast but connectionless communication service. For this purpose, it uses datagram, which are not

acknowledged. In addition to providing logical addressing on the network, IPX also provides routing services.

- Sequential Packet Exchange (SPX): This protocol is connection-oriented and guarantees the error-free delivery of data packets.
- Netware Link Service Protocol (NLSP): This protocol works with the IPX protocol to find the appropriate route between communicating networks.
- Routing Information Protocol (RIP): This protocol provides routing-related information to the Network layer.
- Link Support Layer (LSL): This protocol provides the interface between network cards and upper layer protocols.
- Multiple Link Interface Driver (MLID): This protocol enables the integration of network cards with upper layer protocols.

AppleTalk

- AppleTalk is a protocol suite developed by Apple computer in early 1980 for Macintosh[iv] computer
- It is routable protocol and its design is followed by TCP/IP protocol. It is a multi-layered protocol that provides internetwork routing, files and printer service, naming service and data communication services.
- AppleTalk has two version AppleTalk Phase 1 and AppleTalk Phase 2
- AppleTalk Phase 1 cannot contain more than 135 Hosts/Servers; AppleTalk Phase 2 cannot contain more than 253 Hosts/Servers.
- The data in AppleTalk can be transmitted at the speed of 230 kbps
- The network devices can be 1000 feet apart from each others
- The PCS has to support AppleTalk hardware and software in order to communicate with the Macintosh Computer
- There are two main protocol Name Binding Protocol (NBP) and AppleTalk Address Resolution Protocol (AARP)
- AppleTalk address Consist of four number i.e. two byte network number and one byte socket number and one byte node number
- In 2009 it moved to unsupported status after the Macintosh OS X 10.6

NetBIOS Name

- NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a local area network (LAN).
- It was created by IBM for its early PC Network, was adopted by Microsoft, and has since become a de facto industry standard.
- NetBIOS is a software protocol for providing computer communication services on local networks. Microsoft Windows uses NetBIOS on Ethernet or Token Ring networks.
- Software applications on a NetBIOS network locate each other via their *NetBIOS names*.

- A NetBIOS name is up to 15 characters long and in Windows, separate from the computer name.
- It can include alpha numeric characters also with little symbol special character such as! @ # $ % ^ & () - _ ‘ { }
- The name should be unique throughout the network. And should be such that the user should be easily remembered.
- Applications on other computers access NetBIOS names over UDP port 137. The Windows Internet Naming Service (WINS) provides name resolution services for NetBIOS.
- Two applications start a *NetBIOS session* when one (the client) sends a command to "Call" another (the server) over TCP port 139 on a remote computer.
- Both sides issue "Send" and "Receive" commands to deliver messages in both directions. The "Hang-Up" command terminates a NetBIOS session.
- NetBIOS also supports connectionless communications via UDP datagrams. Applications listen on UDP port 138 to receive *NetBIOS datagrams*.

L2CAP

- Bluetooth use a variety of protocols.
- Bluetooth protocols are divided into to two types ‘controller stack’ and ‘host stack’.
- Controller stack is generally implemented in a low cost silicon device containing Bluetooth radio and a microprocessor.
- Host stack is generally implemented as a part of an operating system, or a installable package on operating system.
- Small device such as Bluetooth headsets host stack and controller stack can be run on the same microprocessor (known as host less system)
- Logical link control and application protocol is under host stack.
- The Logical Link Control and Adaptation Layer Protocol (L2CAP) is layered over the Baseband Protocol and resides in the data link layer.
- L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions.
- L2CAP permits higher level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length.

RFCOMM

- Radio Frequency Communication comes under host stack of Bluetooth.
- It is simple set of transport protocol made on top of the L2CAP protocol.
- It provides up to 60 simultaneous connections to a Bluetooth device at a time.

- RFCOMM sometime called serial port emulation, it provides simple reliable data stream to user similar to TCP

Routing

In internetworking, the process of moving a packet of data from source to destination. Routing is usually performed by a dedicated device called a router. Routing is a key feature of the Internet because it enables messages to pass from one computer to another and eventually reach the target machine. Each intermediary computer performs routing by passing along the message to the next computer. Part of this process involves analyzing a *routing table* to determine the best path.

Routing is often confused with *bridging,* which performs a similar function. The principal difference between the two is that bridging occurs at a lower level and is therefore more of a hardware function whereas routing occurs at a higher level where the software component is more important. And because routing occurs at a higher level, it can perform more complex analysis to determine the optimal path for the packet.

Types of Routing

- **Static routing**, the alternative to dynamic routing, is the process in which the system network administrator would manually configure network routers with all the information necessary for successful packet forwarding. The administrator constructs the routing table in every router by putting in the entries for every network that could be a destination. Static routes to network destinations are unchangeable.
- **Dynamic routing** is a networking technique that provides optimal data routing. Unlike static routing, dynamic routing enables routers to select paths according to real-time logical network layout changes. In dynamic routing, the routing protocol operating on the router is responsible for the creation, maintenance and updating of the dynamic routing table. In static routing, all these jobs are manually done by the system administrator.Dynamic routing uses multiple algorithms and protocols. The most popular are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).
- **A default route** of a computer that is participating in computer networking is the packet forwarding rule (route) taking effect when no other route can be determined for a given Internet Protocol (IP) destination address. All packets for destinations not established in the routing table are sent via the default route. This route generally points to another router, which treats the packet the same way: If a route matches, the packet is forwarded accordingly; otherwise the packet is forwarded to the default route of that router. The process repeats until a packet is delivered to the destination. Each router traversal counts as one hop in the distance calculation for the transmission path.

Routing Protocols

Exterior Routing Protocol

- **BGP (Border Gateway Protocol)** is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems. BGP is often the protocol used between gateway hosts on the Internet. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen.Hosts using BGP communicate using the Transmission Control Protocol (TCP) and send updated router table information only when one host has detected a change. Only the affected part of the routing table is sent.

Interior Routing Protocol

- **Distance Vector Routing** is a simple *routing protocol* used in packet-switched networks that utilizes distance to decide the *bestpacket* forwarding path. Distance is typically represented by the *hop* count**.**
  - The **Routing Information Protocol** (**RIP**) is one of the oldest distance-vector routing protocols, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance, in other words the route is considered unreachable.
  - **IGRP Interior Gateway Routing Protocol** is a distance-vector routing protocol, which means that each router sends all or a portion of its routing table in a routing message update at regular intervals to each of its neighboring routers. A router chooses the best path between a source and a destination. Since each path can comprise many links, the system needs a way to compare the links in order to find the best path. A system such as RIP uses only one criteria -- hops -- to determine the best path. IGRP uses five criteria to determine the best path: the link's speed, delay, packet size, loading and reliability. Network administrators can set the weighting factors for each of these metrics.
  - Enhanced Interior Gateway Routing Protocol an evolved version of IGRP that addresses the demands of large-scale internetworks and the changes in network technology that have been developed since the implementation of IGRP. Routers that already use IGRP can use EIGRP because the metrics for both protocols are directly translatable, i.e., they are as easily comparable as if they were routes that originated in their own autonomous systems. A router running EIGRP stores copies of all its neighbors' routing tables so that it can quickly adapt to alternate routes. If no appropriate route exists, EIGRP queries its neighbors to discover an alternate route. These queries propagate until an alternate route is found. Unlike some earlier routing protocols that would send an entire table to neighboring routers when one routing table

entry changed, EIGRP notifies the neighbors of only the specific change in the table.

- **The Link State Routing Protocol** is performed by every *switching node* in the network (i.e., nodes that are prepared to forward packets; in the Internet, these are called routers). The basic concept of link-state routing is that every node constructs a *map* of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical *path* from it to every possible destination in the network. The collection of best paths will then form the node's routing table.
  - **Open Shortest Path First**, an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Routers use link-state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links, and it also sends the complete routing structure (topography). The advantage of shortest path first algorithms is that they results in smaller more frequent updates everywhere. They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity (when routers continuously increment the hop count to a particular network). This makes for a stable network. The disadvantage of shortest path first algorithms is that they require a lot of CPU power and memory. In the end, the advantages outweigh the disadvantages.
  - The IS-IS (Intermediate System - Intermediate System) protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors. The topology information is flooded throughout the AS, so that every router within the AS has a complete picture of the topology of the AS. This picture is then used to calculate end-to-end paths through the AS, normally using a variant of the Dijkstra algorithm. Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.

Chapter 4: IP Addressing

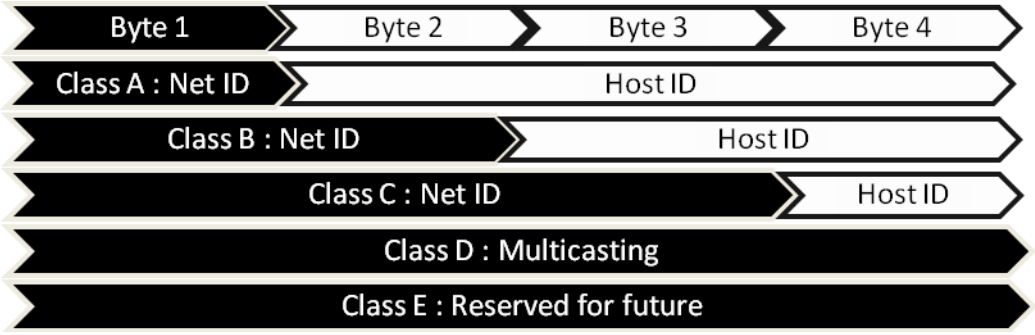
IP Addressing

- Short for Internet Protocol address. An IP address identifies a computer that is connected to the internet or a network. An IP address usually consists of four groups of number separated by dots such as 192.168.0.0
- A 32 bit address must be unique in network to access it. Each byte is having 8 bit i.e. IP address is store 4 bytes memory
- These addresses are actually broken down into three main distinct classes. They are known as Class A, Class B, Class C

IP Address Classes

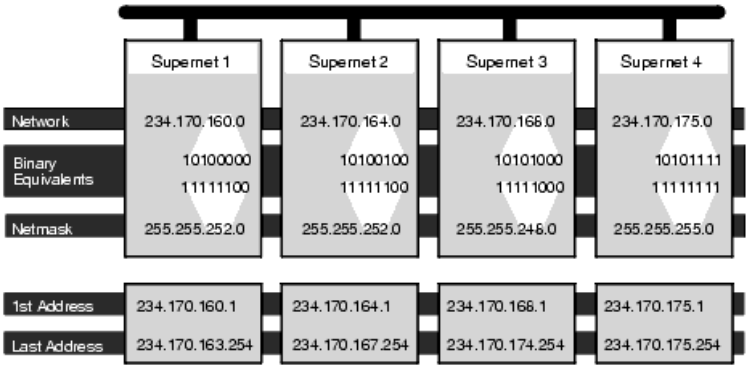
1. **Class A**
   - IP address ranges from 1.0.0.1 through 126.255.255.254
   - First byte indicates the network, last three byte indicates the host ID on network
   - Supports 16 million hosts on each of 127 networks.
2. **Class B**
   - IP address ranges from 128.0.0.1 to 191.255.254.254
   - 127.0.0.1 to 127.255.255.254 is reserved
   - First two octet indicates network last two octal indicates the host ID on network
   - Supports 65,000 hosts on each of 16,000 networks.
3. **Class C**
   - IP address ranges from 192.0.0.1 through 223.255.255.254
   - First three octet represents network and last octet represents the host ID on network
   - Supports 254 hosts on each of 2 million networks.

- There are two more class that are Class D and Class E. Class D and Class E not allocated to hosts.
- Class D addresses are used for multicasting and Class E addresses are not available for general use, they are reserved for future purpose**.**



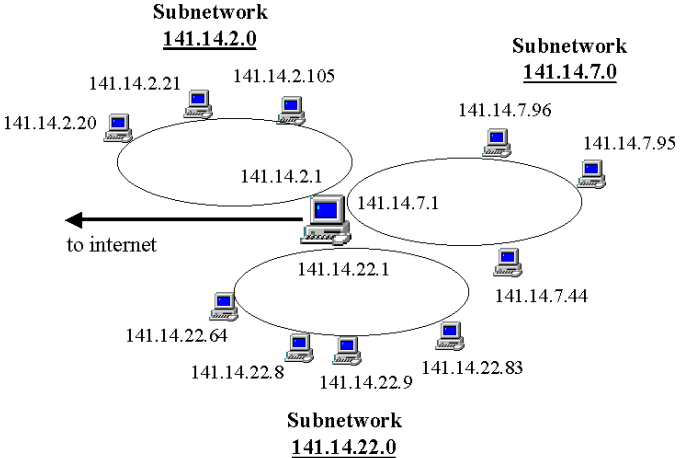
Supernetting

A supernet is created by combining several Internet Protocol (IP) networks or subnets into one network with a single classless interdomain routing (CIDR) prefix. The new combined network has the same routing prefix as the collection of the prefixes of the subnets. The procedure used to create a supernet is commonly called supernetting, route aggregation or route summarization. Supernetting enables organizations to modify their network size and minimize the extensive requirement of network routing devices by combining several independent routes. It also helps to conserve address space and helps the router to effectively store routing information and minimize processing overheads while matching the routes. Supernetting supports the CIDR address coding scheme, allowing routing table entries to be reduced.



Subnetting

Subnetting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets). An IP address includes a network segment and a host segment. Subnets are designed by accepting bits from the IP address's host part and using these bits to assign a number of smaller sub-networks inside the original network. Subnetting allows an organization to add sub-networks without the need to acquire a new network number via the Internet service provider (ISP). Subnetting helps to reduce the network traffic and conceals network complexity. Subnetting is essential when a single network number has to be allocated over numerous segments of a local



area network (LAN). Subnets were initially designed for solving the shortage of IP addresses over the Internet.

Basic Structure of IPv6

- The current version of IP is IPv4, evolved since 1970, and not been substantially changed since 1981.
- When the Internet Engineering Task Force (IETF) published the definitive specification of IP (RFC 971) it proved as robust, easily implemented and interoperable.
- But today things provided by IPv4 was not enough such as..
- IPv4 has two level address structure (Net ID) and (Host ID) categorized into five classes A, B, C, D & E. The address space is now inefficient.
- The internet must accommodate real time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resource not provided in IPv4.
- Internet must accommodate encryption and authentication of data for some application. Originally no security mechanism provided by IPv4
- To overcome these deficiencies IPv6 also known as Internetworking protocol, next generation (IPng) was proposed and is now a standard
- It is modified to accommodate the unforeseen growth of internet
- The format and length of IP address where changed along with the packet format
- IPv6 address has eight groups of hexadecimal characters (0-9 , A-F) separated by colons
- Example of IPv6 3ffe:ffff:0000:2f3b:0299:00ff:fe28:9c59
- The leading zero in section can be suppressed 3ffe:ffff:0:2f3b:299:ff:fe28:9c59
- All zero can also be suppressed 3ffe:ffff::2f3b:299:ff:fe28:9c59
- Following are main difference between IPv4 and IPv6

IPv4	IPv6
In IPv4 source and destination address are 32 bit	In IPv6 source and destination address are 128bits
IPsec[v] is optional in v4	IPsec is require in v6
Fragmentation is done by both routers and sending host in v4	Fragmentation is done only by sending host not by routers in v6
Headers includes checksum in v4	No checksum stored in headers in v6
Headers includes various options in v4	All optional data moved to IPv6 extension header
Must be configured either manually and through DHCP in v4	Does not require manual configuration or DHCP in v6

Installation of IPv6

- To install IPv6 using network connection.Click Start Menu

- Either click Control Panel and then double click on Network Connection or point setting, click on Control Panel and then double click on Network Connection
- Right click any local area connection and then click properties
- Click Install. In the select Network Component type dialog box, click protocol and then click Add.In the select Network Protocol dialog box click Microsoft TCP/IP version 6

Uninstall of IPv6

- Click Start Menu
- Either click Control Panel and then double click on Network Connection or point setting, click on Control Panel and then double click on Network Connection
- Right click any Local Area Connection and then click properties
- Click Microsoft TCP/IP version 6 in the list of installed components and then click uninstall.Restart computer

Install of IPv6 using Command Prompt

- To open Command Prompt click Start Menu →Click Run and type 'cmd' without quotation marks and click Ok
- At Command Prompt type 'netsh interface ipv6 install' without quotation marks and then press Enter

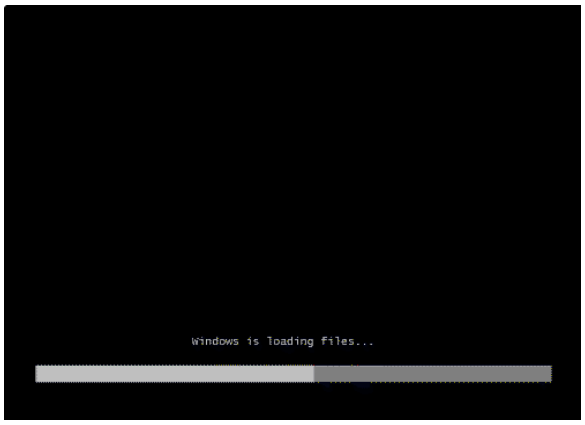
Uninstall of IPv6 using Command Prompt

- At Command Prompt type 'netsh interface ipv6 uninstall' without quotation marks and then press Enter.

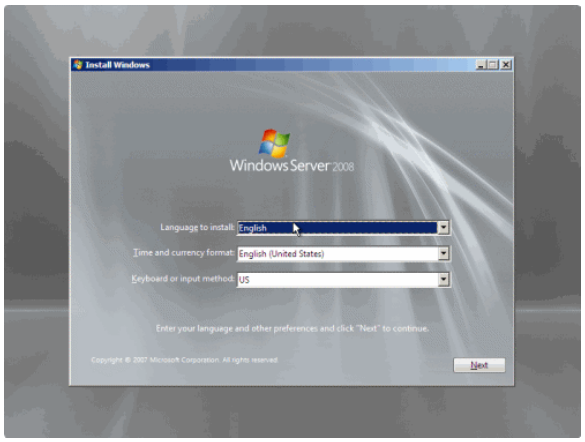
Windows 2008 Server Installation

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.

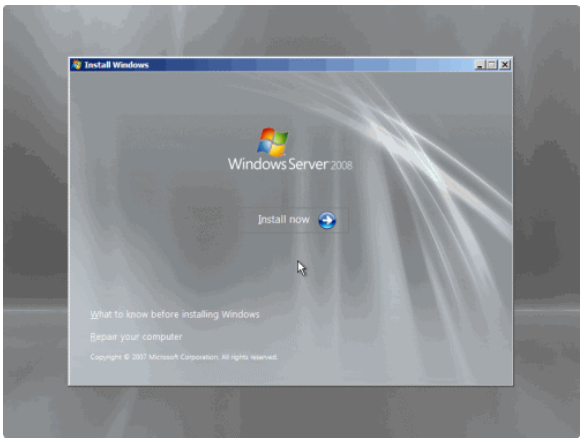
2. **Reboot** the computer.



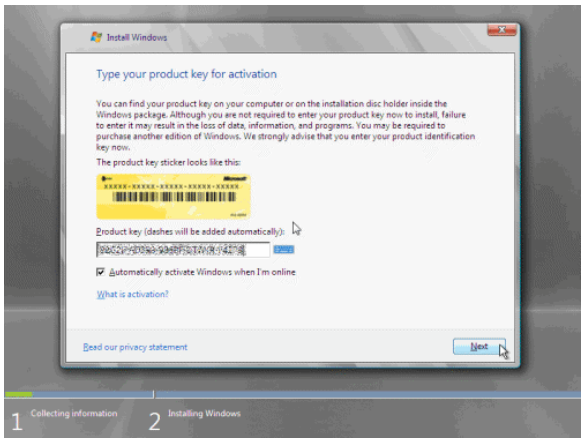
3. When prompted for an **installation language** and other regional options, make your selection and press **Next**.



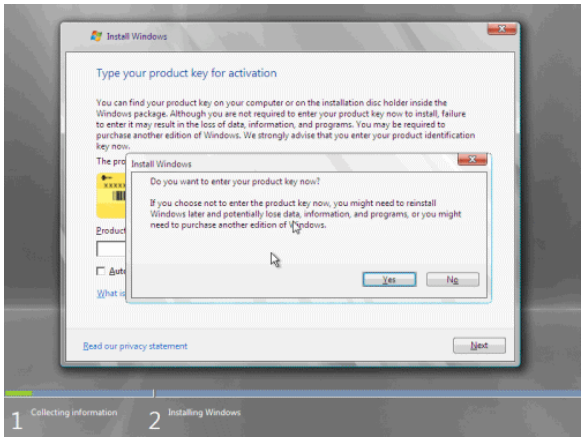
4. Next, press **Install Now** to begin the installation process.



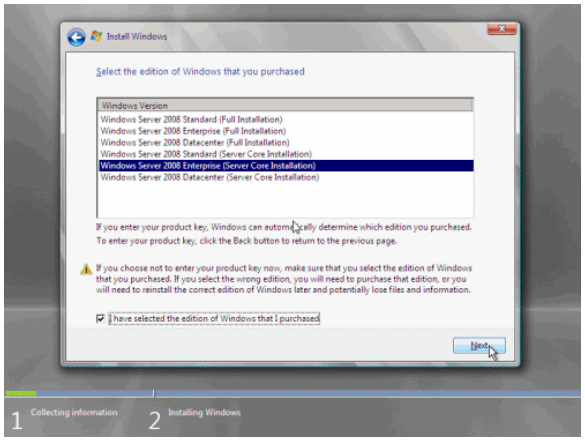
5. Product activation is now also identical with that found in Windows Vista. Enter your **Product ID** in the next window, and if you want to automatically activate Windows the moment the installation finishes, click **Next**.



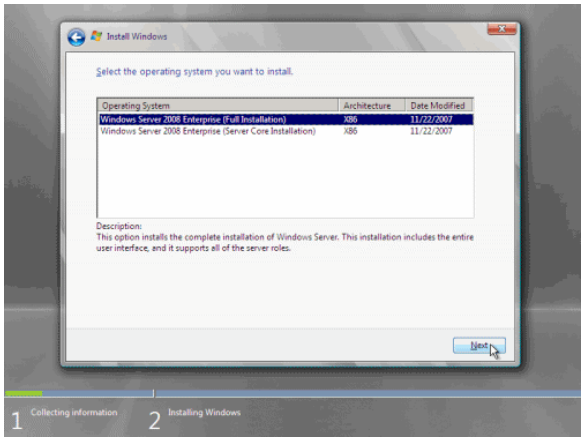
If you do not have the Product ID available right now, you can leave the box empty, and click Next. You will need to provide the Product ID later, after the server installation is over. Press No.



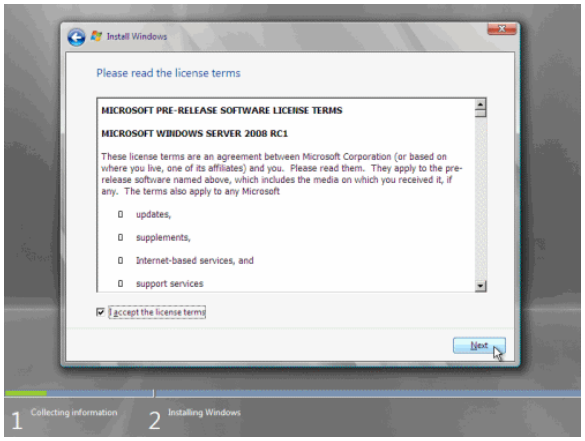
6. Because you did not provide the correct ID, the installation process cannot determine what kind of Windows Server 2008 license you own, and therefore you will be prompted to **select your correct version** in the next screen, assuming you are telling the truth and will provide the correct ID to prove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



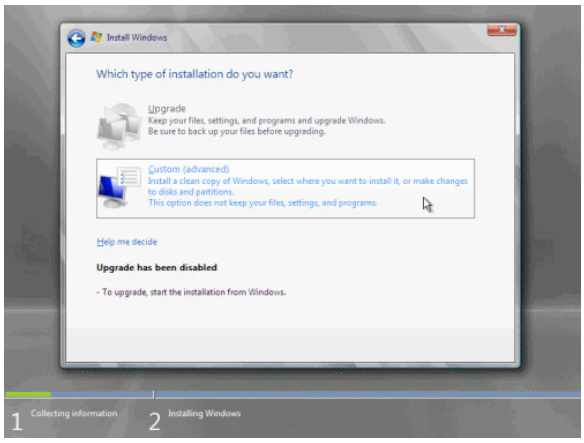
7. If you did provide the right Product ID, select the **Full version** of the right Windows version you're prompted, and click **Next**.



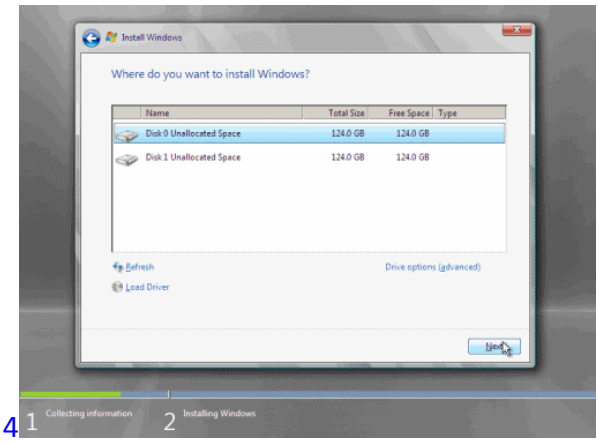
8. Read and accept the license terms by clicking to select the **checkbox** and pressing **Next**.



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**.



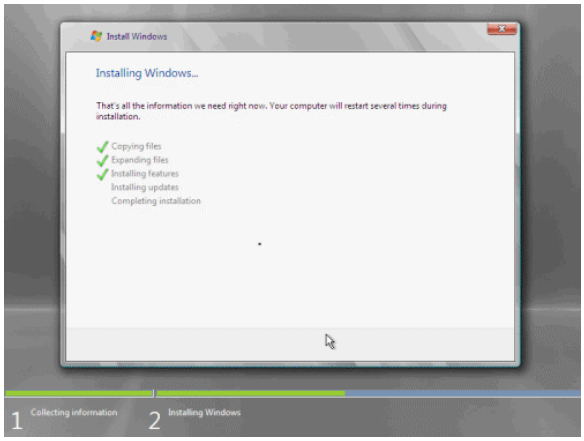
4

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're installing in a Virtual Machine environment, make sure you read the "Installing the Virtual SCSI Controller Driver for Virtual Server 2005 on Windows Server 2008"

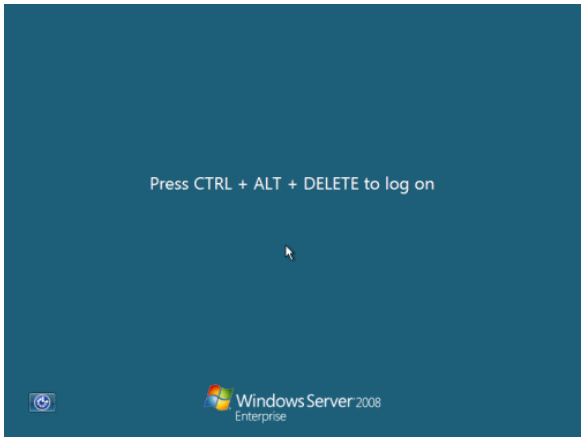
If you must, you can also click Drive Options and manually create a partition on the destination hard disk.

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.

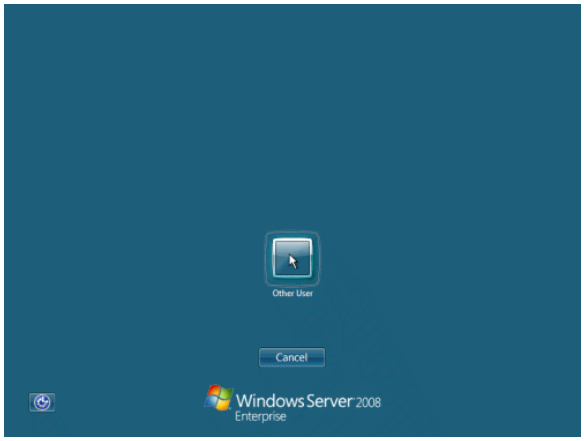


The installation process will reboot your computer, so, if in step #10 you inserted a floppy disk (either real or virtual), make sure you remove it before going to lunch, as you'll find the server hanged without the ability to boot (you can bypass this by configuring the server to boot from a CD/DVD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

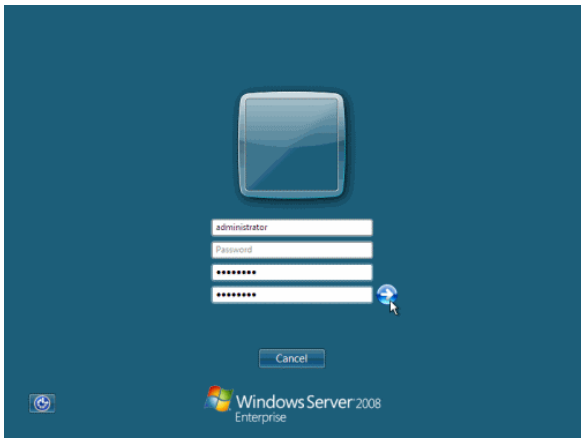
12. Then the server reboots you'll be prompted with the new Windows Server 2008 type of login screen. Press **CTRL+ALT+DEL** to log in.



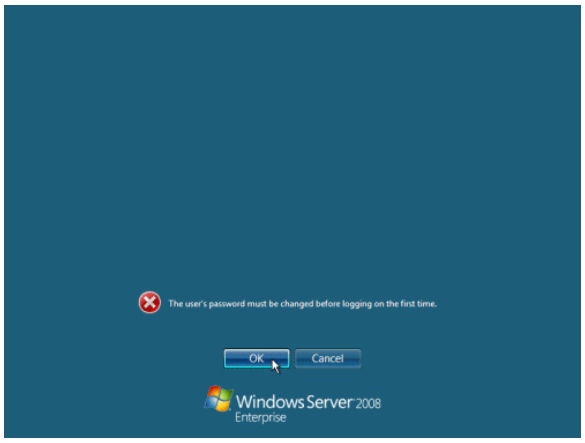
13. Click on **Other User.**



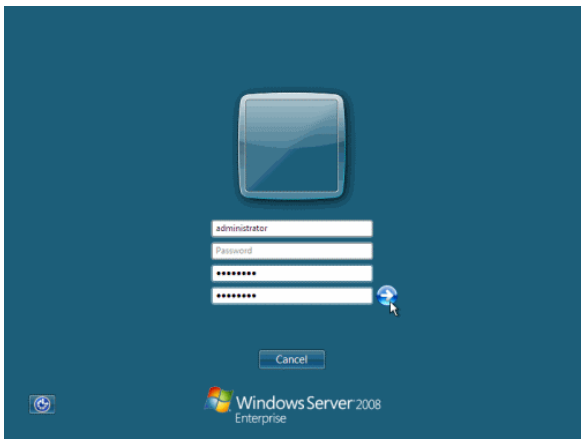
14. The default **Administrator** is **blank**, so just type **Administrator** and press **Enter**.



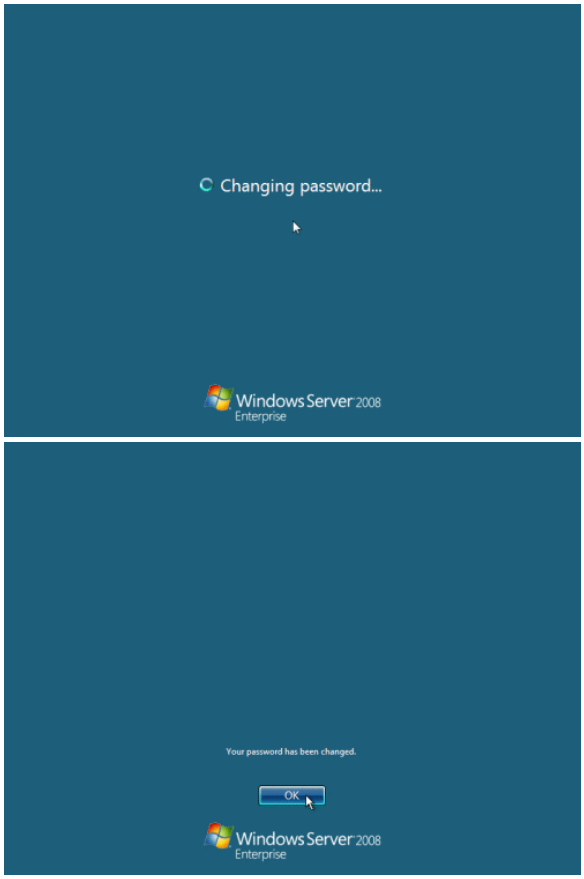
15. You will be prompted to change the user's password. You have no choice but to press **Ok**.



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

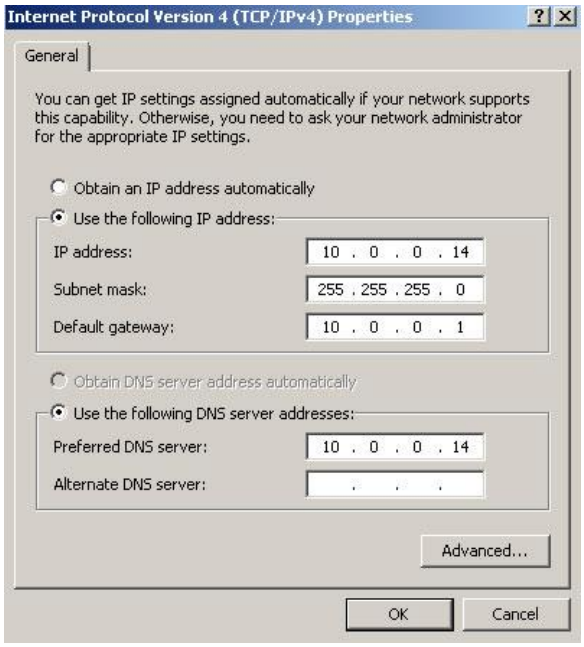


17. Someone thought it would be cool to nag you once more, so now you'll be prompted to accept the fact that the password had been changed. Press **Ok**.



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.

- The first step is to assign a ip to the server that you going to deploy the AD. Its nessary to install it as DNS server too. So its better to have fixed ip it doesn't mean you cannot install AD without fixed ip address but it will solve lot of issues if you used fixed ip.

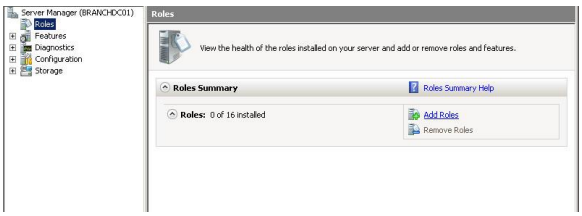


In here the server ip is 10.0.0.14. Since we going to make it as DNS server too you should use the same ip as the preferred DNS server.

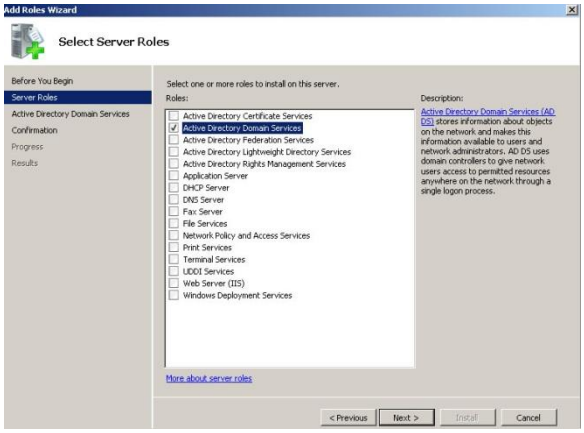
- Next step is to install the Active directory roles. Unlikely the older version of windows servers Microsoft highly recommend to use server manager option to install roles before you run dcpromo.

- Click on start menu and select the Server Manager

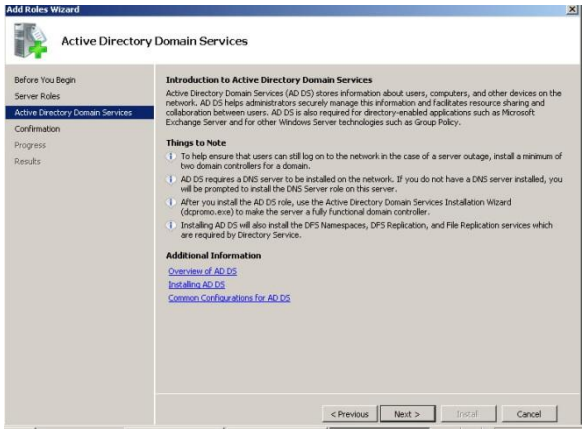
- Select the roles from the right hand panel and click on add roles option.



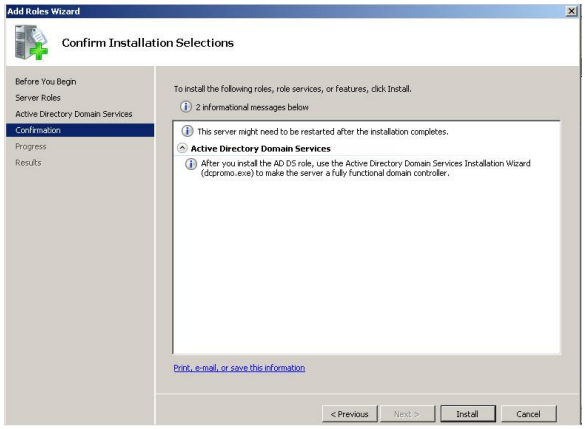
- From the roles list select the "Active Directory Domain Services" role and Click "Next"



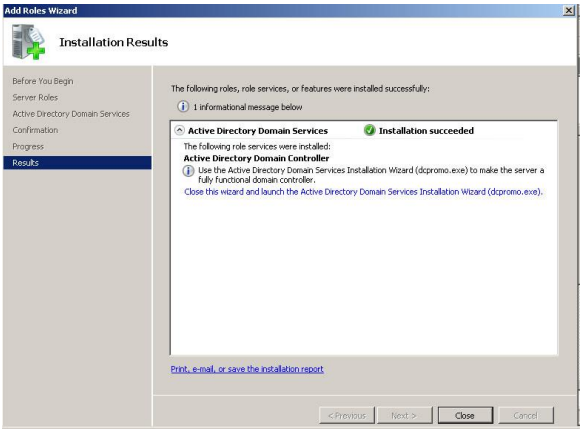
- Review the confirmation and click on "Next"



- Review the installation confirmation and click on "Next"

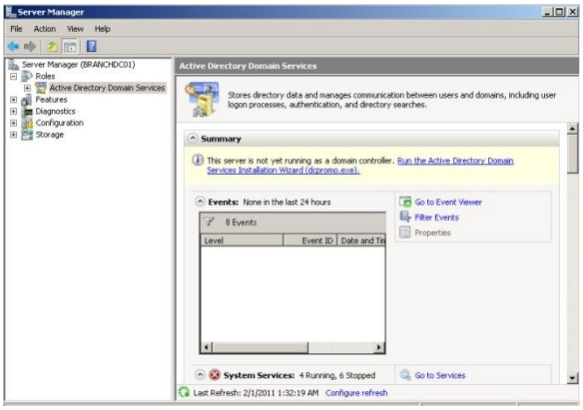


- It will take few minutes to complete and when its done you will get this confirmation. And then click on "Close"



After that you will need to do a reboot.

- After reboot please open up the "server Manager" again. And then click on "Roles" there you will see the "Active Directory Domain Services" is successfully installed in there. click on it then you will get a window like below.

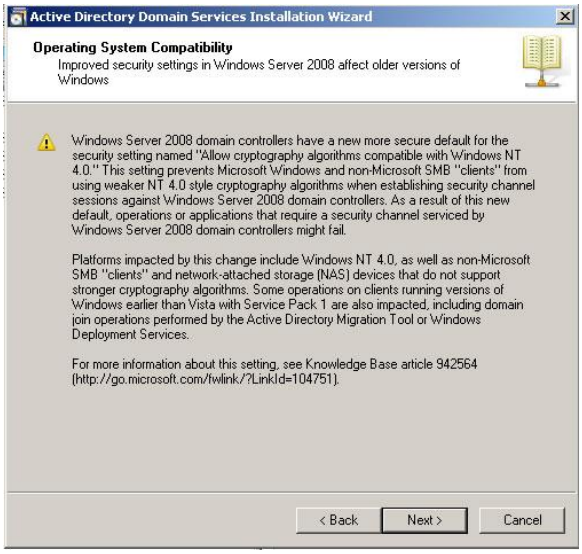


In their please pay attention to the message

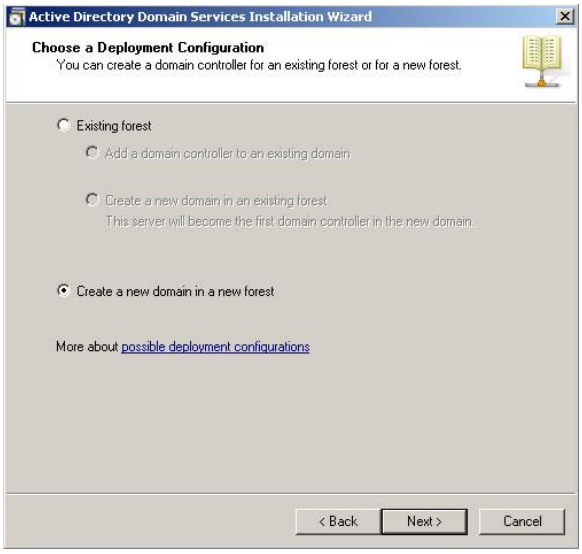
So please click on that link and it will start the DCPROMO wizard.

- So next step to go through the DC promo wizard.
- To start the installation click on "Next"

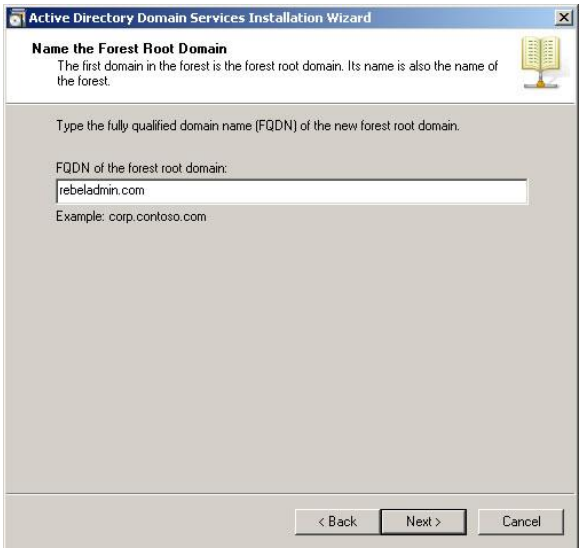
- Click on "Next"



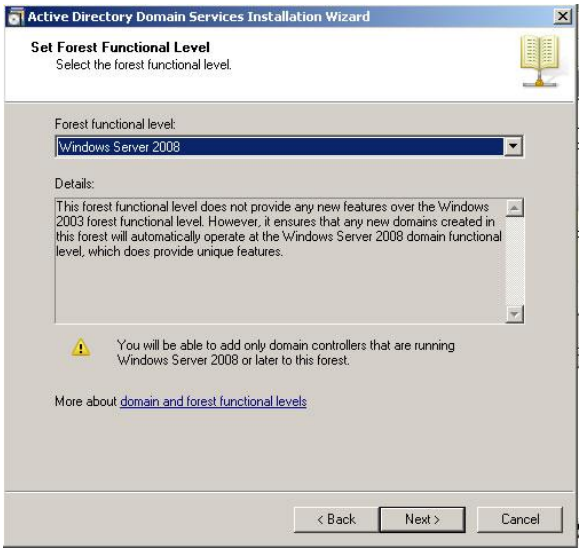
- Since we going to install New domain Controller in new forest please select the option "Create a new domain in new forest" option and click on "Next"



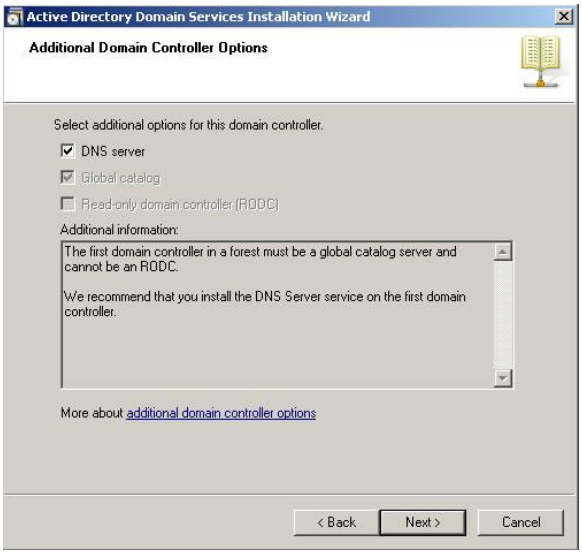
- Now we have to provide the name for our domain controller. It must be FQDN. In our case I used rebeladmin.com as the domain. Please click "Next" after it.



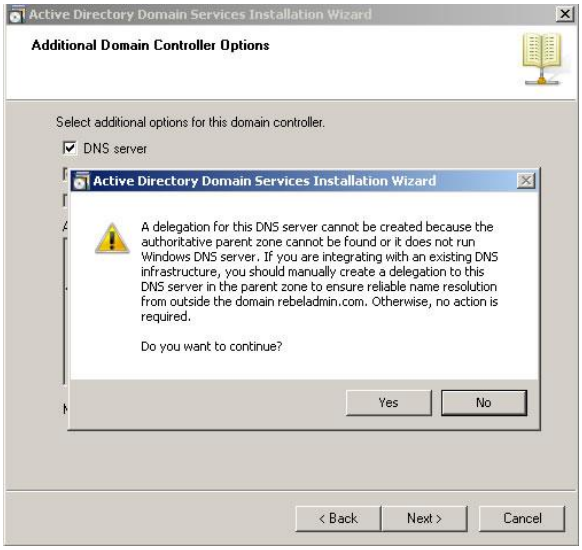
- In this window it will ask to select forest function level. If you going to add server 2003 domain controller to your forest later don't select the function level as server 2008. If you going to use full features of 2008 Ad you must select forest function level as server 2008. In my case I used server 2008. Click on "Next" after the select.



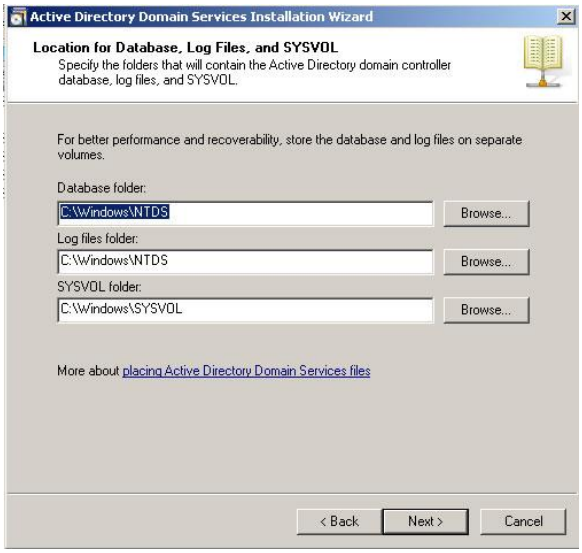
- In next window since it's the first DC we should make it as DNS server too. Leave the default selection and click on "Next"



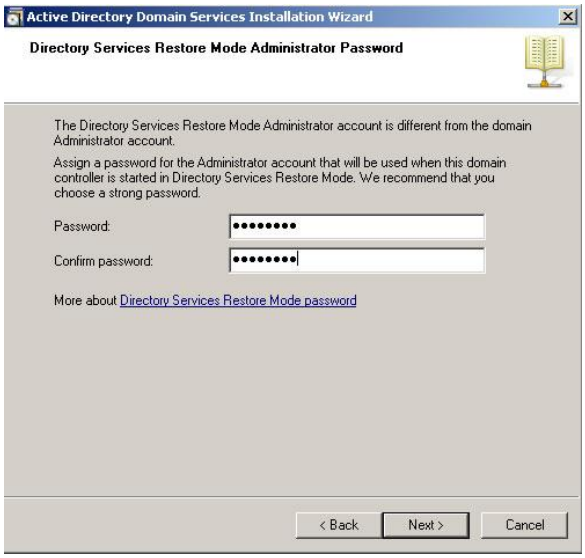
- If the wizard cannot create a delegation for the DNS server, it displays a message to indicate that you can create the delegation manually. To continue, click "Yes"



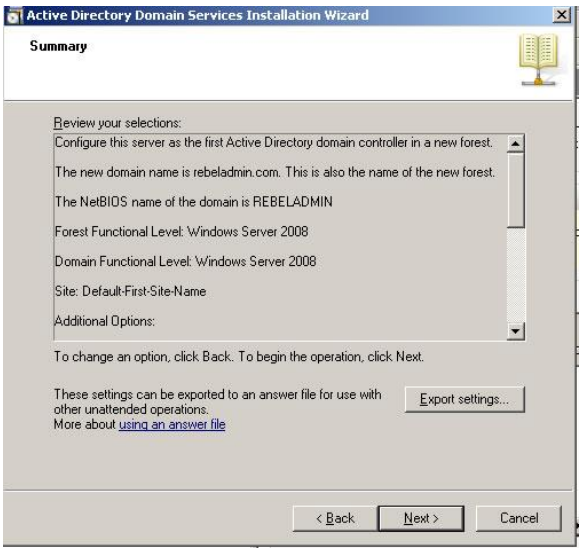
- In next window it will show up the database location. It its going to be bigger AD its good if you can keep NTDS database in different partition. Click on "Next" after changes.



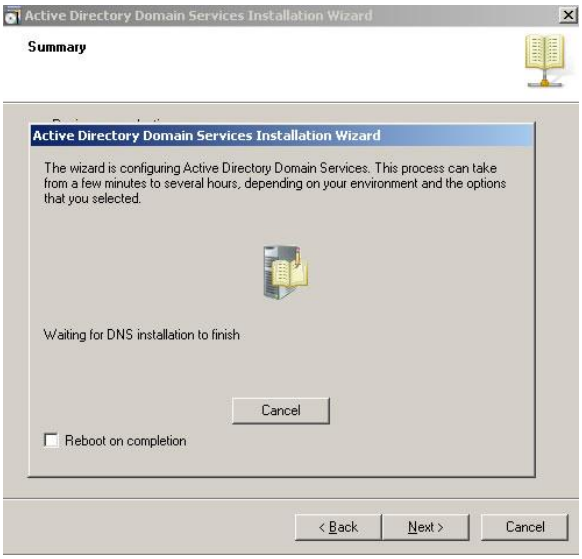
- In next window its asking to define a restore mode password. Its more important if you had to do a restore from backup in a server crash. Click on "Next" after filling it.



- Next window is giving you a brief of the installation. Click on "Next"



- Then it will start the installation of the AD. It will take some time to complete. After complete of the installation perform a server reboot.



- After the reboot now you can login to the domain. Please use the login as following example

User name : your domain\administrator

Password : XXXXXXXX

- Now its done and you can view the active directory options on administrative tools menu

Active Directory

- Active directory is technology created by Microsoft that provides a variety of network services as under
- LDAP (Lightweight directory access protocol) is the industry standard directory access protocol, making active directory access protocol, making active directory widely accessible to management and query application

- DNS based naming and other network information
- Central location for network administration and delegation of authority
- Information security and single sign on for user access to network based resources
- Central storage location for application data.Synchronization of directory updates amongst several servers

Domain, Forest, Trees

- All objects inside a common directory database is known as domain
- Each domain stores information only about the objects that belong to that domain
- A tree consists of single domain or multiple domains in a contiguous namespace
- A forest is a collection of trees and represents the outermost boundary within which users, computers, groups and other objects exits

Accounts (User, Groups, Computer)

- A user requires an active directory user account to log on to computer or to a domain. The account establishes and identity for the user, the operation system then uses this identity to authenticate the user and grant him or her authorization to access specific domain resources
- User account can also be used as service account for some application.
- Windows provide two predefined user accounts that are administrator and guest
- You can use these accounts to log on locally to computer or create a new account to access resources.Guest account is disabled and you must enable it to use.
- Administrator account is the most powerful account because it is a member of administrators group
- To enable user authentication and authorization features you must create individual accounts of user and create provide separate security (user authentication on every account)
- Groups are active directory objects that can contains users, contacts, computers and other groups
- We can nest groups i.e. you can add a group as a member of another group. Nesting group makes it easier to manage users and can reduce network traffic caused by replication of group membership changes
- Planning group strategies is an essential part of deploying active directory. Before you create groups determine the number of domains you will have on your network
- Windows uses computer accounts to authenticate the computer and to authorize or deny access to domain resources.
- You can add, disable, rest or delete user and computer accounts using the active directory users and computer tools

Monitoring Performance

- With the performance console, you can measure the activity of any computer on the network with the help of two powerful monitoring snap-ins: system monitor and performance logs.
- System monitor displays real time performance data collected from configurable components called performance counter.
- The performance logs and alerts records performance counter over period of time in logs.
- When you first open system monitor, three counters are loaded and begin to report real time data.Snap in includes dozens of other counter that you can add to display
- To add counters to system monitor details, click to add button in the toolbar or press CTRL +I. Default three counters are loaded that are memory, physical disk and processor
- Memory: the rate at which page are read form or written to disk
- Physical Disk: average disk queue length will display the average number of read and write request queued for the selected disk during the sample interval
- Processor: the percentage of elapsed time that the processor spends to execute a no idle thread. This counter is primary indicator of processor activity and display the average percentage of busy time observed during the sample interval
- To start performance monitor Start – Control Panel – Administrative Tools – Performance

Network Traffic Monitor

- As an administrator, he has to monitor and detect problem with traffic on your network
- With network monitor you can gather information about the network traffic that flows to and from network adapter of the computer on which it is installed.
- Once you capture the performance you can use network monitor to analyze the information, diagnose problem traffic patterns and device strategies to prevent future network traffic problems

STEPS TO INSTALL NETWORK MONITOR

- Open windows components wizard (Start – Control Panel – Add Remove Program)
- In the windows components wizard click management and monitoring tools and then click details
- In subcomponents of management and monitoring tools select the network monitor tools checkbox and then click ok
- If you are prompted for additional files, insert the installation CD for you operation system, or type path to location of files on the network

STEPS TO CAPTURE NETWORK FRAMES

- Open network monitor (Start – Control Panel – Administrative Tools – Network Monitor)

- If prompted select the local network from which you want to capture data by default
- On the capture menu, click buffer setting and then set the buffer and frame size as appropriate.On the capture menu click start

Logging Events

- Windows server 2003 maintains variety of logs that contains information about its ongoing processes.
- To view these logs we can use event viewer (Start – Control Panel – Administrative Tools – Event Viewer)
- By configuring the options on each of the logs to meet the requirement of our environment, we can collect data appropriate for trouble shooting hardware, application, system and resource access.
- In windows 2003, event log service is started automatically
- It store main three logs: Application, system and security.
- In application information about specific programs running on the computer as determined by application developers
- In system information about events generated by windows server components such as services and devices drivers are stored
- In security information about all security is stored, such as failed login attempts, tried to access printers, files, and folder having no permission.

MMC

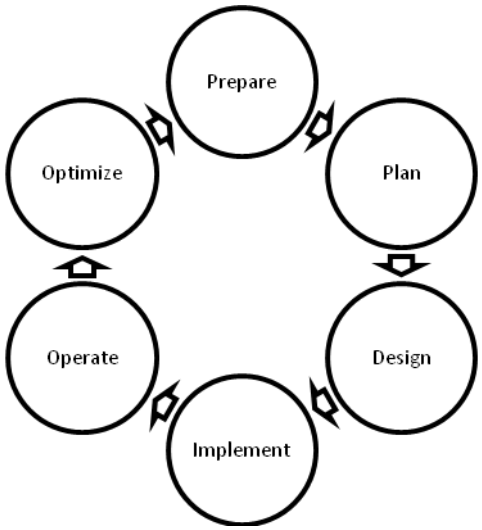
- Microsoft management console (MMC) is used to create, save and open various administrative tools called snap-in
- MMC does not perform administrative function but it host tools that do that. Snap-in are most common of these tools, other items that you can add include Active X controls, Links to web page, folder or files, etc
- Windows 2003 have various pre configured snap-in such as event viewer and system Monitor. We can create additional snap-in consoles to meet our needs; multifunction tools can also be customized.
- MMC can be used in two modes user mode and author mode.
- User mode, where you work with existing snap-in console. Author mode where you create new snap-in as required.
- To create author MMC go to run dialog box type MMC. Enter.On the file menu click add/remove MMC

  From the snap-in added to drop down click the snap-in which you want to add in new MMC. Save it before using/closing it.

Chapter 5: Basic of Network Security

Fundamentals of Network Security

- As the network is growing, they become more complex and bringing new challenges to those who run and manage them
- Also rapidly growing technologies introduce fresh security, therefore network manager's struggles to add latest technologies in network infrastructure.
- To help to face the complexities of managing modern network the core principles of security are used i.e. CIA Traid, confidentiality, integrity, availability.
- When you are planning, designing or implementing network security there are few question which should be kept in mind for securing network.
- The basic question could be: what you need to get your objectives, which technologies or solution is required, what you are trying to protect, what are your business objectives, etc.
- Advance technologies now offer opportunities for small and medium sized business (SMB) to protect system against wide range of security threats.
- At the same time organization aims for greater security with less resource. Without proper security unauthorized activity can be done from intruders (Robbers, Criminal, Competitors, Employee)
- Cisco has developed the Safe blueprint, comprehensive security plan that recommends and explain specific security solution for different networks.
- Cisco blueprints includes various stages : Prepare, Plan, Design, Implement, Operate and Optimize

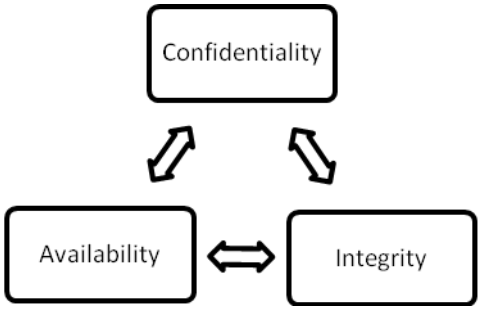


Security Paradigm[vi]

- As the size of network continues to grow and attack to those networks become increasingly sophisticated, the way we thing about security changes. Here are some of the major factors that are changing the security paradigm
- Security is no longer about products : Security solutions must be chosen with business objectives in mind and integrated with operational procedures and tools
- Scalability demands are increasing: With increasing number of vulnerabilities[vii] and security threats, solutions must scale to thousands of host in large enterprises.

- Legacy endpoint security Total cost of ownership is a challenge: reactive products force deployment and renewal of multiple agents and management paradigms
- Day zero damage: rapidly propagating attacks happens too fast for reactive products to control. Therefore an automated, proactive security system is needed to combat the dynamic array of modern day viruses and worms
- With modern day distributed networks, security cannot be enforced only at network edge or perimeter.
- Zero day attacks or new and unknown viruses continue to plague enterprise and service provider networks.
- To attempt to establish protection against attacks, enterprises try to patch systems as vulnerabilities become known. This clearly cannot scale in large networks, and these situations can be addressed only with real time proactive based system.
- Security now is about management and reduction of risk in rapidly evolving environment. Maximum risk reduction is achieved with an integrated solution built on a flexible and intelligent infrastructure and effective operations and management tools. Business objective should drive security decisions. Today, we are in new era that forces us to rethink security and outbreak prevention.

Security Principles (CIA Model)

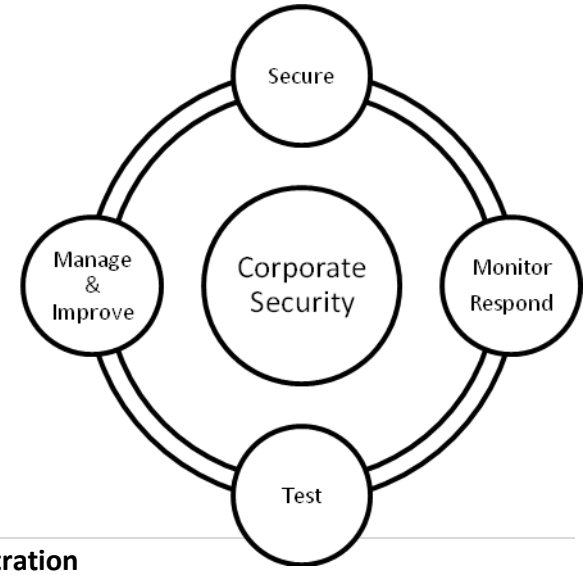


- Simple but widely applicable security model is the confidentiality, integrity and availability
- These three key principles provides all security system

1. **Confidentiality**
   - It provides unauthorized access of sensitive information. It has the capability to ensure that necessary level of secrecy is putted on information for unauthorized users.
   - Cryptography and encryption methods are example of confidentiality when data transferred from one computer to another.
2. **Integrity**
   - Integrity prevents unauthorized modification of data, system and information.
   - A common type of security attack in man in the middle
   - In this type of attack, when data is being transferred in the network, attackers will modify the data
3. **Availability**
   - It ensures that information is available to the authorized user every time when requested.
   - Denial of Service (DoS) is one of several types of attack, which will not allow the authorized user to access the data/system.
   - This kind of attack often done for sake of disturbance of services.

Security Policies, Standards, Procedure, Baseline, Guidelines

1. **Policies**
   - Security policy is set of rules, practices and procedure for sensitive information that are to be managed
   - The sample list that cover common policies that an organization should consider could be following
   - Acceptable user: It will outline the use of computer equipment, which equipment should be used by whom
   - Information sensitivity: It will help employee to determine what information should be disclosed to non-employees. What to be showed or not at what time. Whether to inform by telephone, video conferencing or orally or visually.
   - Email: It will look after that email address, email not sent to non-employee. If send to organization or any other user then it should contain proper information.
2. **Standards**
   - Standards are industry recognized best practices, frameworks and agreed principles of concepts and designs which are designed to implement, achieve and maintain the required levels of processes and procedures
   - Like security policies, standards are strategic in nature in that they define system parameters and processes.
3. **Procedures**
   - Procedures are low level documents which will provide systematic information about the security policies are to be implemented by employee for unauthorized users.
4. **Baseline**
   - It is the minimum level of security requirement for the system should be kept
   - In baseline will provide document having step by step information to implement basic security
5. **Guidelines**
   - Guidelines are recommended actions and operational guides for users.
   - Guidelines are tactical in nature i.e. they are also well planned, same as procedure to implement policies



Security Wheels

- Network security is a continues process for the perfection to achieve secured network infrastructure
- To achieve that goal 5 stage should be throughout the network, continuously.
- Stage 1: Develop Security Policy – Decide what kind of security is to be kept on which user on for what data, equipment or resource.
- Stage 2: Make network secure – After deciding security implement it on network
- Stage 3: Monitor and respond – Look on the security, check no mistake is been made.
- Stage 4: Test – Test Security through system auditing or by various any other ways.
- Stage 5: Mange and Improve – Manage the implemented security and try to improve it using various new technique if up gradation is been made in network.

Security models

- An important element in the design and analysis of secure system is the security model, because it integrates the security policy that should be enforced in system.
- A security model is a symbolic portrayal[viii] of security policy. It maps the requirement of policy makers into set of rules and regulations that are to be followed by computer system or network system.
- A security policy is a set of abstract goals and high level requirements and the security model is the do's and don'ts to make this happen
- Few security model are described below with very short details
  - The Bell-LaPadula Model (BLM) also called the multilevel model was introduced mainly to enforce access control in government and military application. BLM protects the confidentiality of the information within system.
  - The Biba model is modification of BLM that mainly emphasizes the integrity of information within system.
  - The Clark-Wilson model prevents authorized users from making unauthorized modification to the data. This model introduces system of triples: subject, program and object.
  - The Access Control Matrix is general model of access control that is based on the concept of subjects and objects.
  - Information Flow Model restricts information in its flow so that it moves only to and from approved security levels.
  - The Chinese wall model combines commercial discretion with legally enforceable mandatory controls. It is required in the operation of many financial services organizations.

Perimeter Security

- Opinions on perimeter[ix] security have changed a great deal over the past few years. Part of that change is that the very nature of perimeter security is becoming increasingly uncertain, and everyone has different view of just what it is.
- The limits of perimeter itself are becoming broad and extensive, with no geographic boundaries, and remote access is becoming part of integral networks.

Is perimeter security disappearing?

- In essence[x], perimeter has been transformed and extended to the various levels within the network.
- In other words, networks today do not have a single point of entrance; they are multi-entry open environments where controlled access is required from anywhere within network.
- This transformation leads us to start thinking in terms of multiperimeter networks.

Difficulty of Defining Perimeter

- Traditional networks are growing with the merging of remote network access. Wireless networks, laptops, mobile phones, PDAs and numerous other wireless gadgets needs to connect from outside the enterprise into corporate network.
- To fulfill these needs, the concept of inside versus outside becomes rather complicated. For example, when you connect to the corporate network using virtual private network you are no longer on the outside network. You are now inside network.
- Globally networked businesses rely on their network to communicate with employees, customers, partners and suppliers. Although immediate access to information and communication is an advantage, it raises concerns about security and protecting access network resources.
- Network administrator's needs to know who is accessing which resources and establish clear perimeters to control access.
- An effective security policy balances accessibility with protection. Security policies are enforced at network perimeters.
- Often people think of perimeter as boundary between internal network and public internet, but perimeter can be established anywhere within private network, or between you network and partner's network.

Security in Layers

- As discussed earlier, security in layers in the preferred and most scalable approach of safeguard a network.
- On single mechanism cannot be relied on for security of system. To protect your infrastructure, you must apply security in layers. This layered approach is also called defense in depth.
- The idea is that you create multiple systems so that failure in one does not leave you vulnerable, but is caught in next layer.
- Additionally, in layered approach, the vulnerability[xi] can be limited and contained to affected layers because of applied security at varying levels.

Basic of Internet

- The Internet is a worldwide telecommunications system that provides connectivity for millions of other, smaller networks; therefore, the Internet is often referred to as a network of networks. It allows computer users to communicate with each other across distance and computer platforms.
- The Internet began in 1969 as the U.S. Department of Defense's Advanced Research Project Agency (ARPA) to provide immediate communication within the Department in case of war.
- Computers were then installed at U.S. universities with defense related projects. As scholars began to go online, this network changed from military use to scientific use. As ARPAnet grew, administration of the system became distributed to a number of organizations, including the National Science Foundation (NSF).
- This shift of responsibility began the transformation of the science oriented ARPAnet into the commercially minded and funded Internet used by millions today.
- The Internet acts as a pipeline to transport electronic messages from one network to another network. At the heart of most networks is a server, a fast computer with large amounts of memory and storage space.
- The server controls the communication of information between the devices attached to a network, such as computers, printers, or other servers.
- An Internet Service Provider (ISP) allows the user access to the Internet through their server. Many teachers use a connection through a local university as their ISP because it is free.
- Other ISPs, such as America Online, telephone companies, or cable companies provide Internet access for their members.
- You can connect to the Internet through telephone lines, cable modems, cellphones and other mobile devices.

How Internet Is Connected To Computer

- All modern computers and laptops are capable of connecting to the internet, as are many other devices, including mobiles, tablets, e-readers, televisions, video games consoles.
- There are two ways of getting the internet at home. The most popular way is to have your telephone line (also known as a ‘landline’) converted to broadband so that it can carry normal phone calls and internet data at the same time.
- However, if you don’t have a landline or if you want to be able to use the internet when you’re out and about, you might prefer mobile internet from one of the mobile network providers. This can be used anywhere there’s a mobile signal but does tend to be slower and more expensive than broadband through a landline.

- **Step 1:** Choose an internet service provider (ISP). This could be the company that provides your telephone line or it could be one of the many independent providers. To help you choose, have a look at one of the many comparison websites and ask people you know for their opinion.
- When choosing a supplier, you need to take into account the various packages on offer. These will differ in price depending on the maximum speed they offer and the monthly usage allowance.
- The speed is measured in megabits (Mb). A 1Mb connection speed is perfectly acceptable for viewing websites. However, if you want to be able to play games or watch TV online or share your internet between two or more computers, you should choose at least 2Mb.
- **Step 2:** Having chosen an ISP and signed the contract, you'll have to wait a few days while your line is converted to broadband. During this time, you should receive a letter with your username and password and the hardware you'll need: a small box called a 'router' and its attachments. You can see an example on the right.
- **Step 3:** Once you're told that your broadband is active, you can set up your router. It should have come with three cables
  - A network cable to connect the router to your computer
  - A power cable
  - A cable that will go between your router and a microfilter (see below).
  - Plug one end of the network cable into the appropriately shaped socket in the router, and the other end in a similarly appropriately shaped socket in your computer.
  - Take the power cable and plug one end in the router and the other in a nearby power point.
- You should have also received a microfilter. This splits the signal in the telephone wire in two: voice and broadband. You plug the dangly end of the microfilter into your telephone socket. Then in the sockets at the other end, you plug in (1) the cable from your own telephone and (2) the cable that came with your router. As these two sockets are different shapes, you can't plug a cable into the wrong socket. Finally, plug in the other end of the router cable into the router itself.
- You'll also need to install a microfilter in any other telephone socket in the house that's in use. Not doing this can result in loss of internet speed and interference on the line. If no router is being used with a socket, you'll leave one of the microfilter's sockets empty.
- **Step 4:** When you get the router, you should also receive a CD. Once you've set up the router, all you need to do is put the CD into your computer and follow the step-by-step instructions. If you don't want to do this yourself, some companies offer a home installation service and, for an extra cost, will send an engineer to set up your broadband connection for you.

Technology Related To Internet

Dial up

- This type of Internet connection is the most common way that individuals use to connect to the Internet. In this type of connection, you can connect to the Internet via a modem and regular telephone line.
- The major advantage of dial-up connection is that it is less expensive as compared to the dedicated connection.
- Secondly it requires very modest hardware and software resources. But it provides you slower access speed and lower reliability.
- Moreover they use the regular telephone lines, which may be very busy during regular hours that affect speed and efficiency. Also the telephone lines are not very reliable.
- A little disturbance may break the connection.

Lease line

- In your computer needs to be connected to the Internet all the time. Contact your telephone company for a leased line, the same type of line that large organizations use.
- Leased line come in various speeds. Leased line cost more than the dial-up connection.

ISDN

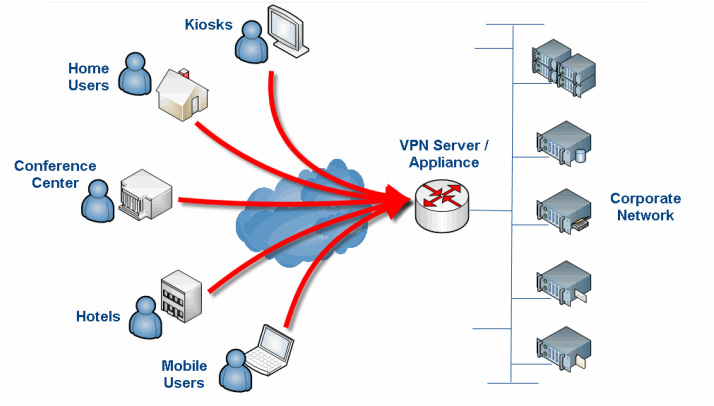
- Integrated services digital network, is available from nearly all-local telephone companies. ISDN is an upgraded phone line that can be used for faster Internet access and for regular voice calls.
- Using a single line of ISDN you can talk on phone while you are surfing on a web. ISDN is all digital, which means that data does not have to be converted to an analog signal for transmission, which is necessary in analog telephone line.
- The hardware requirements are ISDN modem also called terminal adapter and software requirement are communication software and a web browser.

VPN

- VPN is a network that is constructed by using public wires — usually the Internet to connect to a private network, such as a company's internal network.
- There are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.
- VPN follows a client and server approach. VPN clients authenticate users, encrypt data, and otherwise manage sessions with VPN servers utilizing a technique called tunneling.
- VPN clients and VPN servers are typically used in these three scenarios:

- To support remote access to an intranet,
- To support connections between multiple intranets within the same organization,
- To join networks between two organizations, forming an extranet.

- The main benefit of a VPN is the lower cost needed to support this technology compared to alternatives like traditional leased lines or remote access servers.
- VPN users typically interact with simple graphical client programs. These applications support creating tunnels, setting configuration parameters, and connecting to and disconnecting from the VPN server. VPN solutions utilize several different network protocols including PPTP, L2TP, IPsec, and SOCKS.
- VPN servers can also connect directly to other VPN servers. A VPN server-to-server connection extends the intranet or extranet to span multiple networks.
- Many vendors have developed VPN hardware and software products. Some of these do not interoperate due to the immaturity of some VPN standards.



PPTP

PPTP - Point-to-Point Tunneling Protocol - extends the Point to Point Protocol (PPP) standard for traditional dial-up networking. PPTP is best suited for the remote access applications of VPNs, but it also supports LAN internetworking. PPTP operates at Layer 2 of the OSI model.

L2TP

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet. L2TP merges the best features of two other tunneling protocols: PPTP from Microsoft and L2F from Cisco Systems. The two main components that make up L2TP are the L2TP Access Concentrator (LAC), which is the device that physically terminates a call and the L2TP Network Server (LNS), which is the device that terminates and possibly authenticates the PPP stream.

IPSec

- A site-to-site VPN could use either Internet protocol security protocol (IPSec) or generic routing encapsulation (GRE). GRE provides the framework for how to package the passenger protocol for transport over the Internet protocol (IP).
- This framework includes information on what type of packet you're encapsulating and the connection between sender and receiver.
- IPSec is a widely used protocol for securing traffic on IP networks, including the Internet. IPSec can encrypt data between various devices, including router to router, firewall to router, desktop to router, and desktop to server. IPSec consists of two sub-protocols which provide the instructions a VPN needs to secure its packets:
  - Encapsulated Security Payload (ESP) encrypts the packet's payload (the data it's transporting) with a symmetric key.
  - Authentication Header (AH) uses a hashing operation on the packet header to help hide certain packet information (like the sender's identity) until it gets to its destination.

Proxy Servers

A *proxy server* is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the proxy server, and then requests a connection, file, or other resource available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache. In some cases, the proxy may alter the client's request or the server's response for various purposes.

Transparent Proxy

This type of proxy server identifies itself as a proxy server and also makes the original IP address available through the http headers. These are generally used for their ability to cache websites and do not effectively provide any anonymity to those who use them. However, the use of a transparent proxy will get you around simple IP bans. They are transparent in the terms that your IP address is exposed, not transparent in the terms that you do not know that you are using it (your system is not specifically configured to use it.)

Anonymous Proxy

This type of proxy server identifies itself as a proxy server, but does not make the original IP address available. This type of proxy server is detectable, but provides reasonable anonymity for most users.

Distorting Proxy

This type of proxy server identifies itself as a proxy server, but make an incorrect original IP address available through the http headers.

High Anonymity Proxy

This type of proxy server does not identify itself as a proxy server and does not make available the original IP address.

GPS

The Global Positioning System (GPS) is a technical marvel made possible by a group of satellites in earth orbit that transmit precise signals, allowing GPS receivers to calculate and display accurate location, speed, and time information to the user.

By capturing the signals from three or more satellites (among a constellation of 31 satellites available), GPS receivers are able to use the mathematical principle of trilateration to pinpoint your location.

With the addition of computing power, and data stored in memory such as road maps, points of interest, topographic information, and much more, GPS receivers are able to convert location, speed, and time information into a useful display format.

GPS was originally created by the United States Department of Defense (DOD) as a military application. The system has been active since the early 1980s, but began to become useful to civilians in the late 1990s. Consumer GPS has since become a multi-billion dollar industry with a wide array of products, services, and Internet-based utilities.

GPS works accurately in all weather conditions, day or night, around the clock, and around the globe. There is no subscription fee for use of GPS signals. GPS signals may be blocked by dense forest, canyon walls, or skyscrapers, and they don't penetrate indoor spaces well, so some locations may not permit accurate GPS navigation.

GPS receivers are generally accurate within 15 meters, and newer models that use Wide Area Augmentation System (WAAS) signals are accurate within three meters.

While the U.S. owned and operated GPS is currently the only active system, five other satellite-based global navigation systems are being developed by individual nations and by multi-nation consortiums.

GPRS

GPRS (General Packet Radio Service) is a step between GSM and 3G cellular networks. GPRS offers faster data transmission via a GSM network within a range 9.6Kbits to 115Kbits. This new technology makes it possible for users to make telephone calls and transmit data at the same time. (For example, if you have a mobile phone using GPRS, you will be able to simultaneously make calls and receive e-mail messages.) The main benefits of GPRS are that it reserves radio resources only when there is data to send and it reduces reliance on traditional circuit-switched network elements.

With GPRS, an IP data transmission protocol, which is characteristic of computer networks, is being introduced to GSM. IP is a data transmission protocol which is used in Internet, the largest computer network in the world today.

Main features of GPRS

Before introduction of GPRS, the radio capacity was used for calls and data transmission within the GSM network in a rather inefficient way. For data transmission the entire channel was occupied and was thus insufficiently used. With the GPRS technology, the channel is used more efficiently owing to the possibility of more than one user sharing the same channel. GPRS telephones user several channels for data transfer thus facilitating greater transfer speeds.

The GPRS infrastructure and mobile phones support a data transmission speed of up to 13.4Kbits per channel.

GPRS signaling and data traffic do not travel through the GSM network. The GSM network is only used for table look up, in the Location Register (HLR and VLR) data bases, to obtain GPRS user profile data.

CCTV Tech

CCTV (closed-circuit television) is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes.

CCTV relies on strategic placement of cameras, and observation of the camera's input on monitors somewhere. Because the cameras communicate with monitors and/or video recorders across private coaxial cable runs or wireless communication links, they gain the designation "closed-circuit" to indicate that access to their content is limited by design only to those able to see it.

Older CCTV systems used small, low-resolution black and white monitors with no interactive capabilities. Modern CCTV displays can be color, high-resolution displays and can include the ability to zoom in on an image or track something (or someone) among their features. Talk CCTV allows an overseer to speak to people within range of the camera's associated speakers.

CCTV is commonly used for a variety of purposes, including:

- Maintaining perimeter security in medium- to high-secure areas and installations.
- Observing behavior of incarcerated inmates and potentially dangerous patients in medical facilities.
- Traffic monitoring.
- Overseeing locations that would be hazardous to a human, for example, highly radioactive or toxic industrial environments.
- Building and grounds security.
- Obtaining a visual record of activities in situations where it is necessary to maintain proper security or access controls (for example, in a diamond cutting or sorting operation; in banks, casinos, or airports).

CCTV is finding increasing use in law-enforcement, for everything from traffic observation (and automated ticketing) to observation of high-crime areas or neighborhoods. Such use of CCTV technology has fueled privacy concerns in many parts

of the world, particularly in those areas in the UK and Europe where it has become a routine part of police procedure.

---

[i] Make signal stronger so it can travel longer.
[ii] Decrease, Reduction
[iii] Deform, Disfigure, Twist, Bend…
[iv] Is it a series of Unix-based operating systems and graphical user interfaces developed, marketed, and sold by Apple Inc.
[v] Internet Protocol security (IPSec) is a framework of open standards for helping to ensure private, secure communications over Internet Protocol (IP)
[vi] Example, Model, Pattern, Standard
[vii] Week, at risk, in a weak position
[viii] Picture, Description
[ix] Border, Edge, Boundary
[x] Core, Real Meaning
[xi] Weakness