Unit 1: Introduction to data communication

Data communication refers to the exchange of data between a source and a receiver via form of transmission media such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. Delivery. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2. Accuracy. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3. Timeliness. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

4. Jitter. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

A Basic Communication Model:

A data communications system has five components.

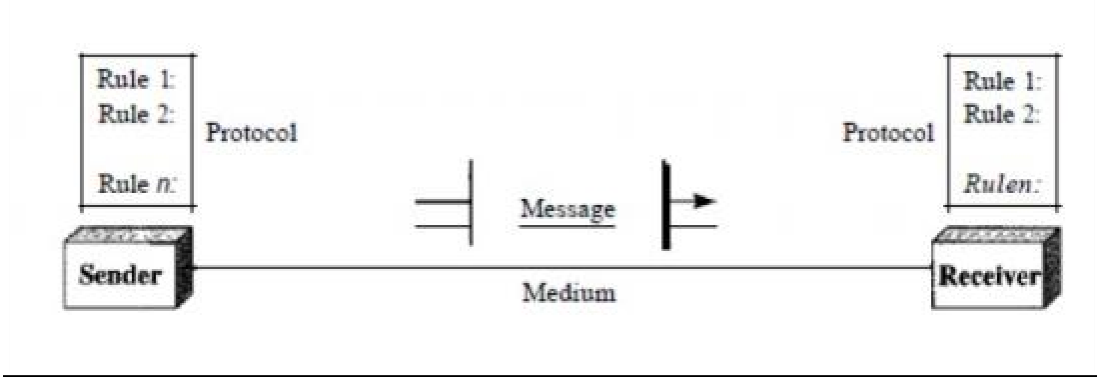


Fig: Data communication model

1. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2. Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves

5. Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

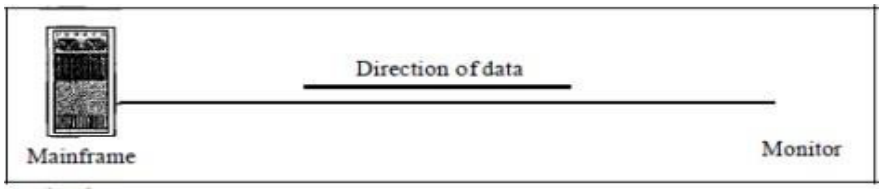
DATA TRANSMISSION MODES

Communication between two devices can be simplex, half-duplex, or full-duplex.

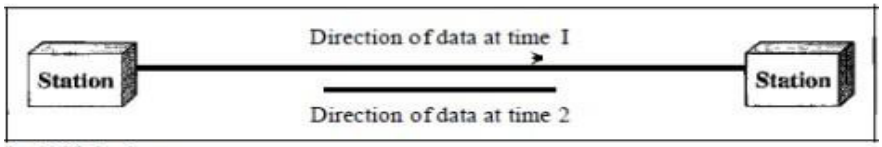
Simplex: In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

Half-Duplex: In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

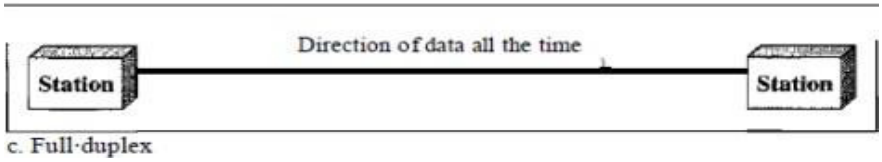
Full-Duplex: In full-duplex both stations can transmit and receive simultaneously. The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.



a. Simplex



b. Half-duplex



c. Full-duplex

Data Communication Networking:

Data communications refers to the transmission of digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange

data. The physical connection between networked computing devices is established using either cable media or wireless media. The best-known computer network is the Internet.

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Performance: Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Reliability: Network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

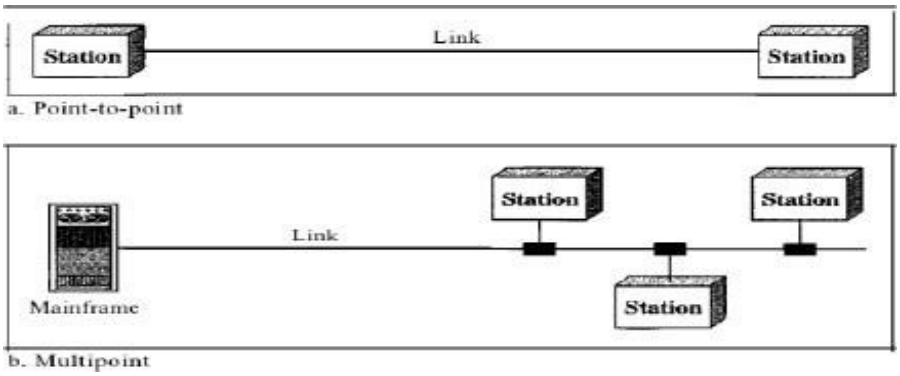
Security: Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Physical Structures:

TYPES OF CONNECTIONS: A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. There are two possible types of connections: point-to-point and multipoint.

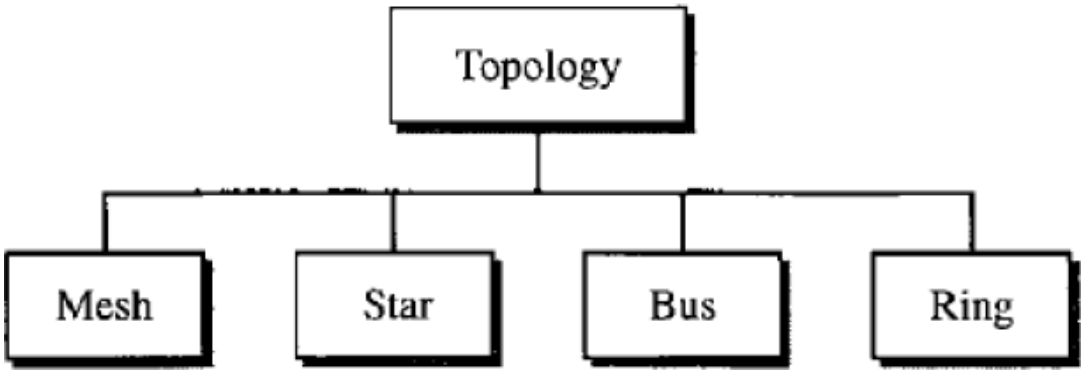
Point-to-Point: A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint: A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.



PHYSICAL TOPOLOGY:

The term physical topology refers to the way in which a network is laid out physically. One or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring.



1. Mesh:

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n - I nodes, node 2 must be connected to n – 1 node, and finally node n must be connected to n - 1 nodes. We need n(n - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need n(n -1) /2 duplex-mode links. To accommodate that many links, every device on the network must have n – 1 input/output ports to be connected to the other n - 1 stations.

Advantages:

1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

3. There is the advantage of privacy or security. When every message travel along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.

4. Point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

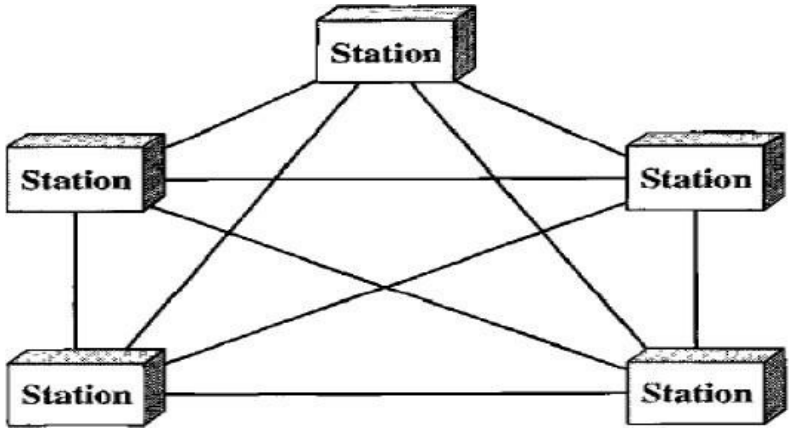
Disadvantages:

1. Disadvantage of a mesh are related to the amount of cabling because every device must be connected to every other device.

2. Installation and reconnection are difficult.

3. The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

4. The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.



2. Star Topology:

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

Advantages:

1. A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others.

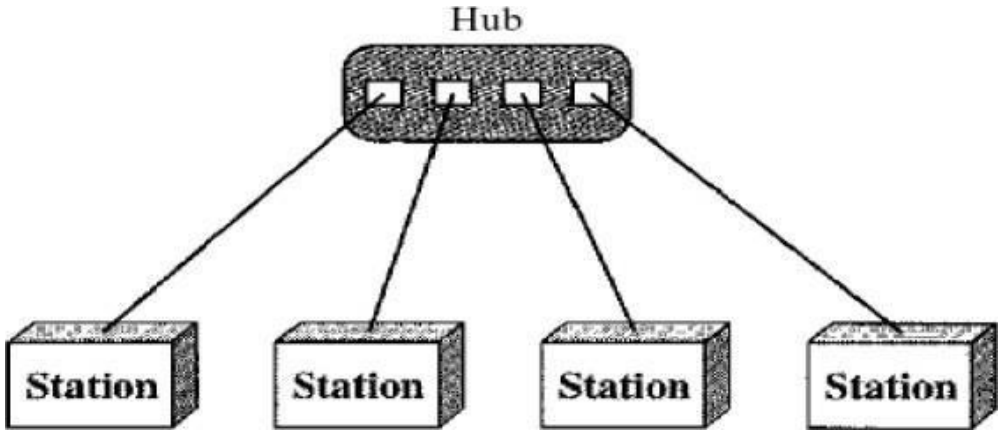
2. Easy to install and reconfigure.

3. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.

4. Other advantage include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages:

One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).



3. BUS:

A bus topology is multipoint. One long cable act as a backbone to link all the devices in a network. Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason, there is a limit on the number of taps a bus can support and on the distance between those taps.

Advantages:

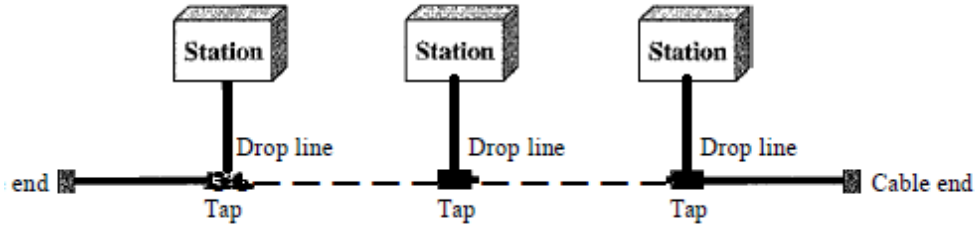
Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the

backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages:

Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone. In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

A bus topology connecting three stations



4. RING:

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

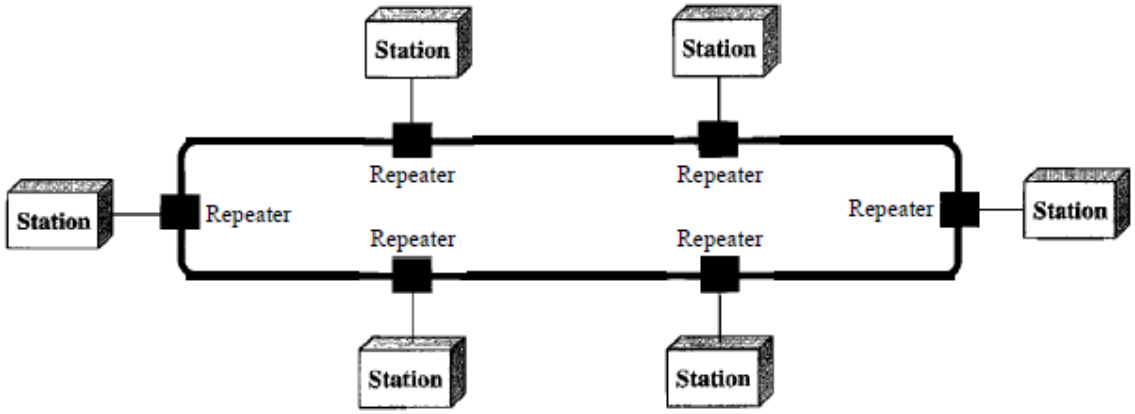
Advantages:

A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally, in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Disadvantages:

Unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break. Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

Figure 1.8 *A ring topology connecting six stations*



NETWORK CATEGORIES

Local Area Networks (LAN):

Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and organizations to share resources (e.g., printers) and exchange information. LANs are distinguished from other kinds of networks by three characteristics:

(1) Their size,

(2) Their transmission technology

(3) Their topology.

LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. Knowing this bound makes it possible to use certain kinds of designs that would not otherwise be possible. It also simplifies network management. Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs operate at up to 10 Gbps.

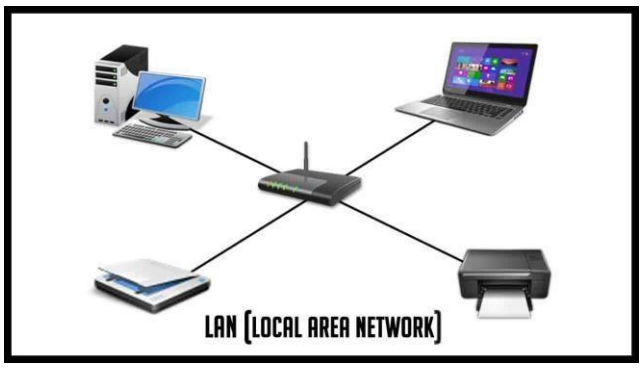


Fig: Local Area Network

Characteristics of LAN:

- LANs are private networks, not subject to external control
- Simple and better performance
- Work in a restricted geographical area

Advantages:

- Resource sharing
- Software applications sharing
- Easy and Cheap communication
- Data Security
- Internet sharing

Disadvantages

- Restricted to local area

Metropolitan Area Network (MAN):

A metropolitan area network, or MAN, covers a city. A MAN is a computer network that interconnects users with computer resources in a geographical area or region larger than that covered by a LAN. It can be an interconnection between several LANs by bridging them with backbone lines.

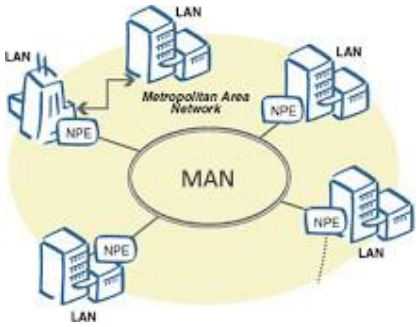


Fig: Metropolitan Area Network

Characteristics:

- Generally, covers towns and cities (up to 50km)
- Transmission medium used for MAN is optical fiber, coaxial cable etc.
- Data rates adequate for distributed computing applications

Advantages

- Extremely efficient and provide fast communication via high-speed carriers, such as fiber optic cables
- Good backbone for larger networks and provides greater access to WAN

Disadvantages

- Complex, more cabling required and expensive

The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses. At first, these were locally-designed, ad hoc systems. Then companies began jumping into the business, getting contracts from city governments to wire up an entire city. The next step was television programming and even entire channels designed for cable only. Often these channels were highly specialized, such as all news, all sports, all cooking, all gardening, and so on. But from their inception until the late 1990s, they were intended for television reception only. Cable television is not the only MAN. Recent developments in high-speed wireless Internet access resulted in another MAN, which has been standardized as IEEE 802.16.

Wide Area Network (WAN):

A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e., application) programs. These machines are called as hosts. The hosts are connected by a communication subnet, or just subnet for short. The hosts are owned by the customers (e.g., people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider. The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener. Separation of the pure communication aspects of the network (the subnet) from the application aspects (the hosts), greatly simplifies the complete network design. In most wide area networks, the subnet consists of two distinct components: transmission lines and switching elements. Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links. WANs are typically used to connect two or more LANs or MANs which are located relatively very far from each other.

In most WANs, the network contains numerous transmission lines, each one connecting a pair of routers. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers. When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded. A subnet organized according to this principle is called a store-and-forward or packet-switched subnet. Nearly all wide area networks (except those using satellites) have store-and-forward subnets. When the packets are small and all the same size, they are often called cells. The principle of a packet-switched WAN is so important. Generally, when a process on some host has a message to be sent to a process on some other host, the sending host first cuts the message into packets, each one bearing its number in the sequence. These packets are then injected into the network one at a time in quick succession. The packets are transported individually over the network and deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process. Not all WANs are packet switched. A second possibility for a WAN is a satellite system. Each router has an antenna through which it can send and receive. All routers can hear the output from the satellite, and in some cases, they can also hear the upward transmissions of their fellow routers to the satellite as well. Sometimes the routers are connected to a substantial point-to-point subnet, with only some of them having a satellite antenna. Satellite networks are inherently broadcast and are most useful when the broadcast property is important.

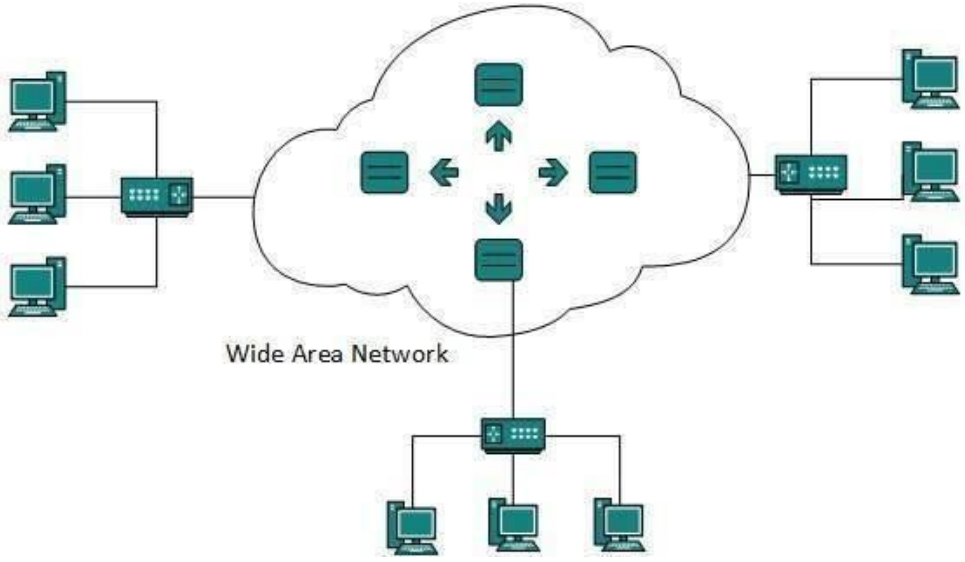


Fig: Wide Area Network

Characteristics

- Covers large distances (states, countries, continents)
- Communication medium used are satellite, public telephone networks which are connected by routers

Advantages

- Covers large geographical area
- Shares software and resources with connecting workstations
- Information can be exchanged to anyone else worldwide in the

network Disadvantages

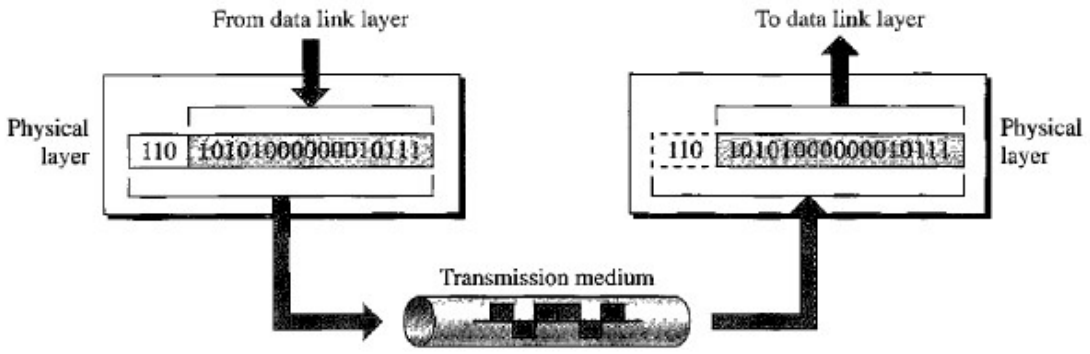
- Data security
- Network is very complex and management is difficult
- As size increases, the networks becomes more expensive

Physical Layer and Network Media

Physical Layer:

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur. Figure below shows the position of the physical layer with respect to the transmission medium and the data link layer.

Figure 2.5 *Physical layer*

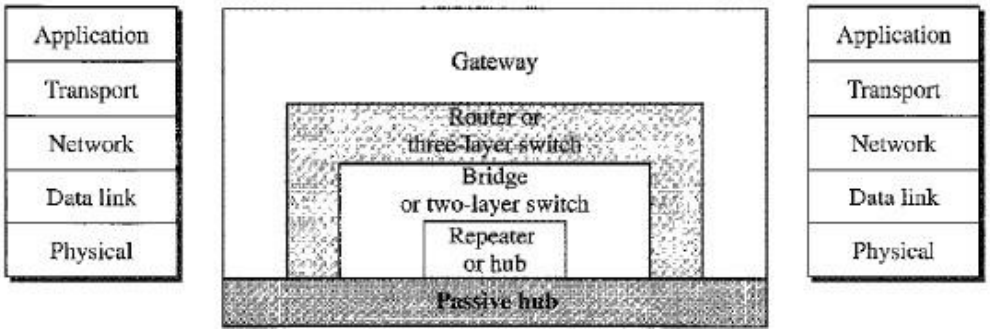


The physical layer is responsible for movements of individual bits from one hop (node) to the next.

Network Devices (Connecting Devices):

We divide connecting devices into five different categories based on the layer in which they operate in a network, as shown in Figure below.

Figure 15.1 *Five categories of connecting devices*



The five categories contain devices which can be defined as:

1. Those which operate below the physical layer such as a passive hub.
2. Those which operate at the physical layer (a repeater or an active hub).
3. Those which operate at the physical and data link layers (a bridge or a two-layer switch).
4. Those which operate at the physical, data link, and network layers (a router or a three-layer switch).
5. Those which can operate at all five layers (a gateway).

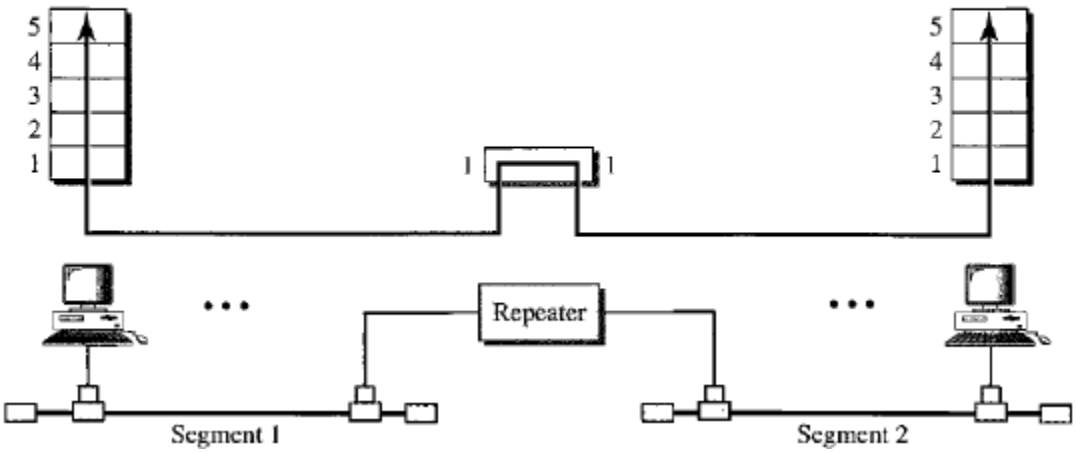
Passive Hubs:

A passive hub is just a connector. It connects the wires coming from different branches. In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point. This type of a hub is part of the media; its location in the Internet model is below the physical layer. It does not regenerate the signals, just provides the multipoint connection to extend the network.

Repeaters:

A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2-port device.

Figure 15.2 *A repeater connecting two segments of a LAN*

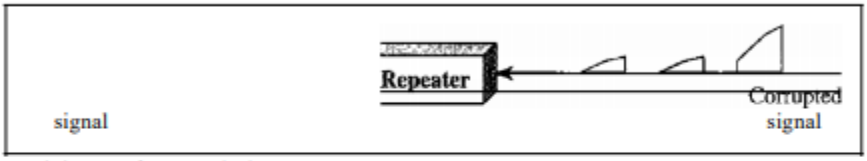


A repeater does not actually connect two LANs; it connects two segments of the same LAN. The segments connected are still part of one single LAN. A repeater is not a device that can connect two LANs of different protocols.

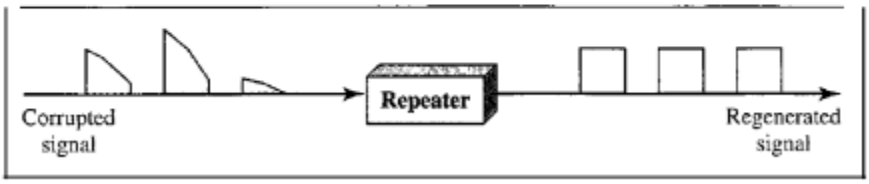
A repeater can overcome the Ethernet length restriction. In this standard, the length of the cable is limited to 500 m. To extend this length, we divide the cable into segments and install repeaters between segments. Note that the whole network is still considered one LAN, but the portions of the network

separated by repeaters are called segments. The repeater acts as a two-port node, but operates only in the physical layer. When it receives a frame from any of the ports, it regenerates and forwards it to the other port.

Figure 15.3 *Function ofa repeater*



a. Right-to-teft transmission.



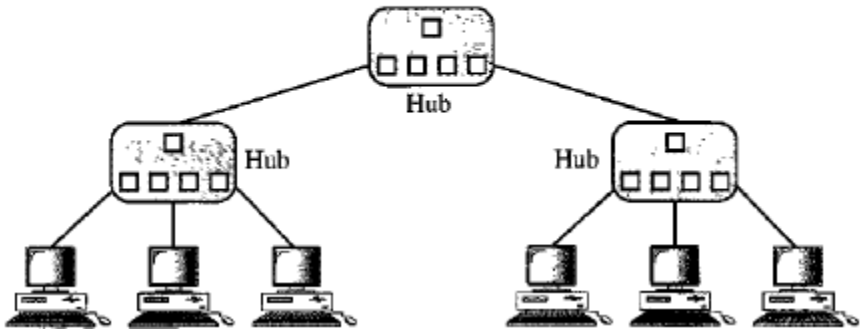
b. Left-to·right transmission.

Active Hubs:

An active hub is actually a multiport repeater. It is normally used to create connections between stations in a physical star topology. However, hubs can also be used to create multiple levels of hierarchy, as shown in Figure below. The hierarchical use of hubs removes the length limitation of Ethernet.

The following diagram represents a Tree Topology. There is a central hub which is acting as active hub, the other two secondary hubs connected are acting as passive hubs.

Figure 15.4 *A hierarchy of hubs*



Difference between Active and passive hub:

- Active hub strengthens the signal where passive hub repeat/copy signals.
- Active hub needs Electricity whereas passive hub work without it.
- Active hub is smarter than passive hub.

- Passive hub is just a connector which connects wire coming from other devices.
- Active hub is multi-point repeater with capability of regeneration of signals.
- Active hub can process and monitor information while passive hub cannot do this.

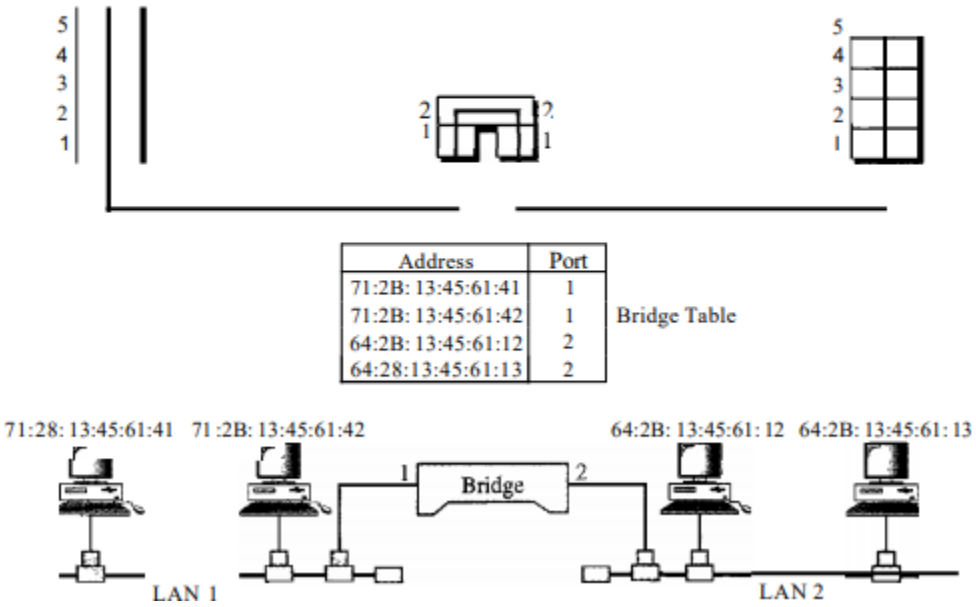
Bridges:

A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2-port device.

Types of Bridges

- Transparent Bridges: - These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- Source Routing Bridges: - In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The route can be discovered by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

Figure 15.5 *A bridge connecting two LANs*



Switch:

A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. We can have a two-layer switch or a three-layer switch. A three-layer switch is used at the network layer; it is a kind of router. The two-layer switch performs at the physical and data link layers.

Two Layer Switch:

A two-layer switch is a bridge, a bridge with many ports and a design that allows better (faster) performance. A bridge with a few ports can connect a few LANs together. A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity. This means no competing traffic (no collision, as we saw in Ethernet).

A two-layer switch, as a bridge does, makes a filtering decision based on the MAC address of the frame it received. However, a two-layer switch can be more sophisticated. It can have a buffer to hold the frames for processing. It can have a switching factor that forwards the frames faster. Some new two-layer switches, called cut-through switches, have been designed to forward the frame as soon as they check the MAC addresses in the header of the frame.

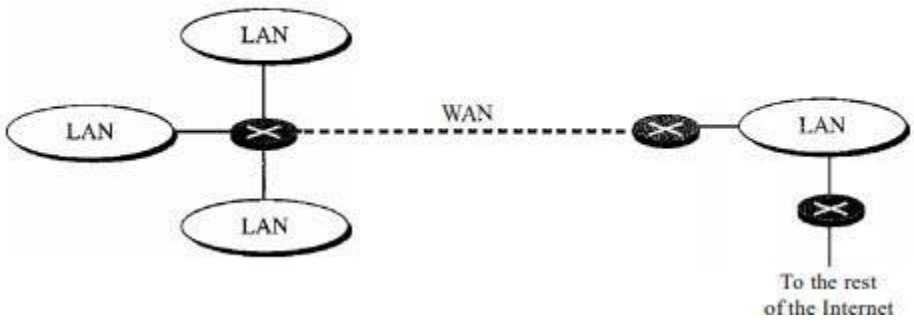
Three Layer Switch:

A three-layer switch is a router, but a faster and more sophisticated. The switching fabric in a three-layer switch allows faster table lookup and forwarding. In this book, we use the terms router and three-layer switch interchangeably.

Routers:

A router is a three-layer device that routes packets based on their logical addresses (host-to-host addressing). A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route. The routing tables are normally dynamic and are updated using routing protocols. Figure below shows a part of the Internet that uses routers to connect LANs and WANs.

igure 15.11 *Routers connecting independent LANs and WANs*



Gateway:

Although some sources use the terms gateway and router interchangeably, most of the literature distinguishes between the two. A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model. A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internetworks that use different models. For example, a network designed to use the OSI model can be connected to another network using the Internet model. The gateway connecting the two systems can take a frame as it arrives from the first system, move it up to the OSI application layer, and remove the message. Gateways can provide security by filtering unwanted application-layer messages.

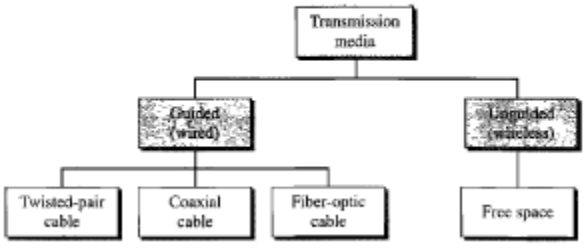
TRANSMISSION MEDIA:

A transmission medium can be broadly defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air. For a written message, the transmission medium might be a mail carrier, a truck, or an airplane.

In data communications, the definition of the information and the transmission medium is more specific. The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form.

Classification of Transmission Media:

Figure 7.2 *Classes of transmission media*



Guided Media

Guided media, which are those that provide a channel from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

1. Twisted-Pair Cable

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure below.

Figure 7.3 *Twisted-pair cable*

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals. If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e,g., one is closer and the other is farther). This results in a difference at the receiver.

By twisting the pairs, a balance is maintained. For example, suppose in one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true. Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly canceled out. From the above discussion, it is clear that the number of twists per unit of length (e.g., inch) has some effect on the quality of the cable.

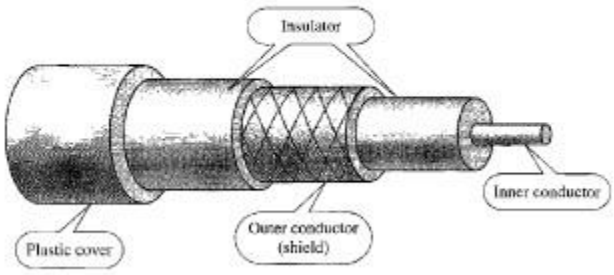
Applications

Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop-the line that connects subscribers to the central telephone office-commonly consists of unshielded twisted-pair cables. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables. Local-area networks also use twisted-pair cables.

2. Coaxial Cable

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover (see Figure below).

Figure 7.7 *Coaxial cable*



Applications

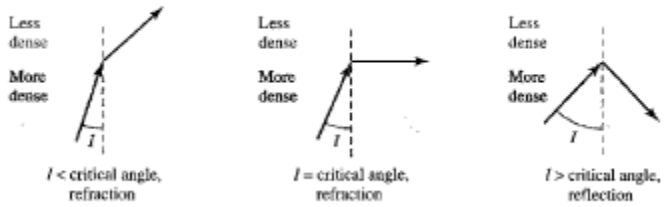
Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals. Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps. However, coaxial cable in telephone networks has largely been replaced today with fiber-optic cable. Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Later, however, cable TV providers replaced most of the media with fiber-optic cable; hybrid networks use coaxial cable only at the network boundaries, near the consumer premises. Cable TV uses RG-59 coaxial cable. Another common application of coaxial

cable is in traditional Ethernet LANs. Because of its high bandwidth, and consequently high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs.

3. Fiber Optic Cable:

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. To understand optical fiber, we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is moving through a single uniform If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction. Figure below shows how a ray of light changes direction when going from a more dense to a less dense substance.

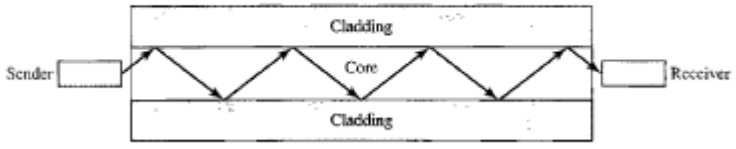
Figure 7.10 *Bending of light ray*



As the figure shows, if the angle of incidence I (the angle the ray makes with the line perpendicular to the interface between the two substances) is less than the critical angle, the ray refracts and moves closer to the surface. If the angle of incidence is equal to the critical angle, the light bends along the interface. If the angle is greater than the critical angle, the ray reflects (makes a turn) and travels again in the denser substance. Note that the critical angle is a property of the substance, and its value differs from one substance to another.

Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it. See Figure below.

Figure 7.11 *Optical fiber*

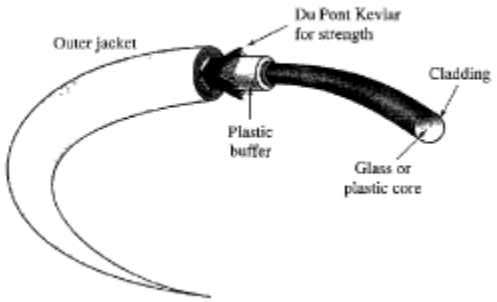


Cable Composition

Figure below shows the composition of a typical fiber-optic cable. The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable. Kevlar is a strong material used in

the fabrication of bulletproof vests. Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core.

Figure 7.14 *Fiber construction*



Applications

Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Today, with wavelength-division multiplexing (WDM), we can transfer data at a rate of 1600 Gbps. Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network. Optical fiber provides the backbone structure while coaxial cable provides the connection to the user premises. This is a cost-effective configuration since the narrow bandwidth requirement at the user end does not justify the use of optical fiber. Local-area network such as Fast Ethernet uses fiber-optic cable.

Advantages and Disadvantages of Optical

Fiber Advantages

Fiber-optic cable has several advantages over metallic cable (twisted pair or coaxial).

a. Higher bandwidth. Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.

b. Less signal attenuation. Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.

c. Immunity to electromagnetic interference. Electromagnetic noise cannot affect fiber-optic cables.

d. Resistance to corrosive materials. Glass is more resistant to corrosive materials than copper.

e. Light weight. Fiber-optic cables are much lighter than copper cables.

f. Greater immunity to tapping. Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

Disadvantages

There are some disadvantages in the use of optical fiber.

a. Installation and maintenance. Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.

b. Unidirectional light propagation. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.

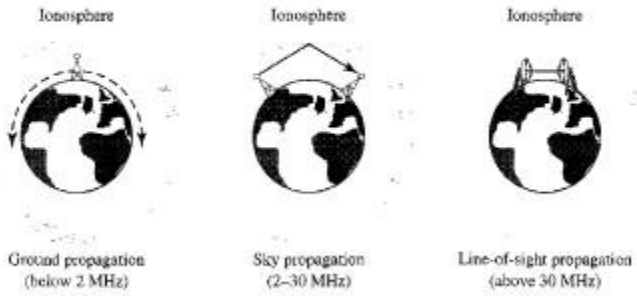
c. Cost. The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

UNGUIDED MEDIA: WIRELESS

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation, as shown in Figure below.

Figure 7.18 *Propagation methods*



In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance. In sky propagation, higher-frequency radio waves radiate upward into the ionosphere where they are reflected back to earth. This type of transmission allows for greater distances with lower output power. In line-or-sight propagation, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other, and either tall enough or close enough together not to be affected by the curvature of the earth. Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.

1. Radio Waves

Waves ranging in frequencies between 3 kHz and 1 GHz are called radio waves. Radio waves, for the most part, are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna. The omnidirectional property has a disadvantage, too. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band. Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio. Radio waves, particularly those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, for example, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building. The radio wave band is relatively narrow, just under 1 GHz, compared to the microwave band. When this band is divided into sub bands, the sub bands are also narrow, leading to a low data rate for digital communications.

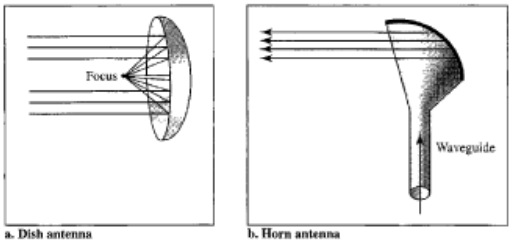
Figure 7.20 *Omnidirectional antenna*

Applications: The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, maritime radio, cordless phones are examples of multicasting.

2. Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

Figure 7.21 *Unidirectional antennas*



Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn (see Figure). A parabolic dish antenna is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus. Outgoing transmissions are broadcast through a horn aimed at the dish. The microwaves hit the dish and are deflected outward in a reversal of the receipt path.

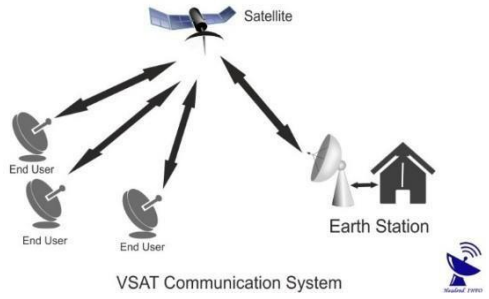
3. Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room. When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.

VSAT:

A very small aperture terminal (VSAT) is a small telecommunication earth station that receives and transmits real-time data via satellite. VSAT is a satellite communications system that serves home and business users. A VSAT end user needs a box that interfaces between the user's computer and an outside antenna with a transceiver. The tranceiver receives or sends a signal to a satellite transponder in the sky. The satellite sends and receives signals from an earth station computer that acts as a hub for the system. For one end user to communicate with another, each transmission has to first go to the hub station which retransmits it via the satellite to the other end user's VSAT.



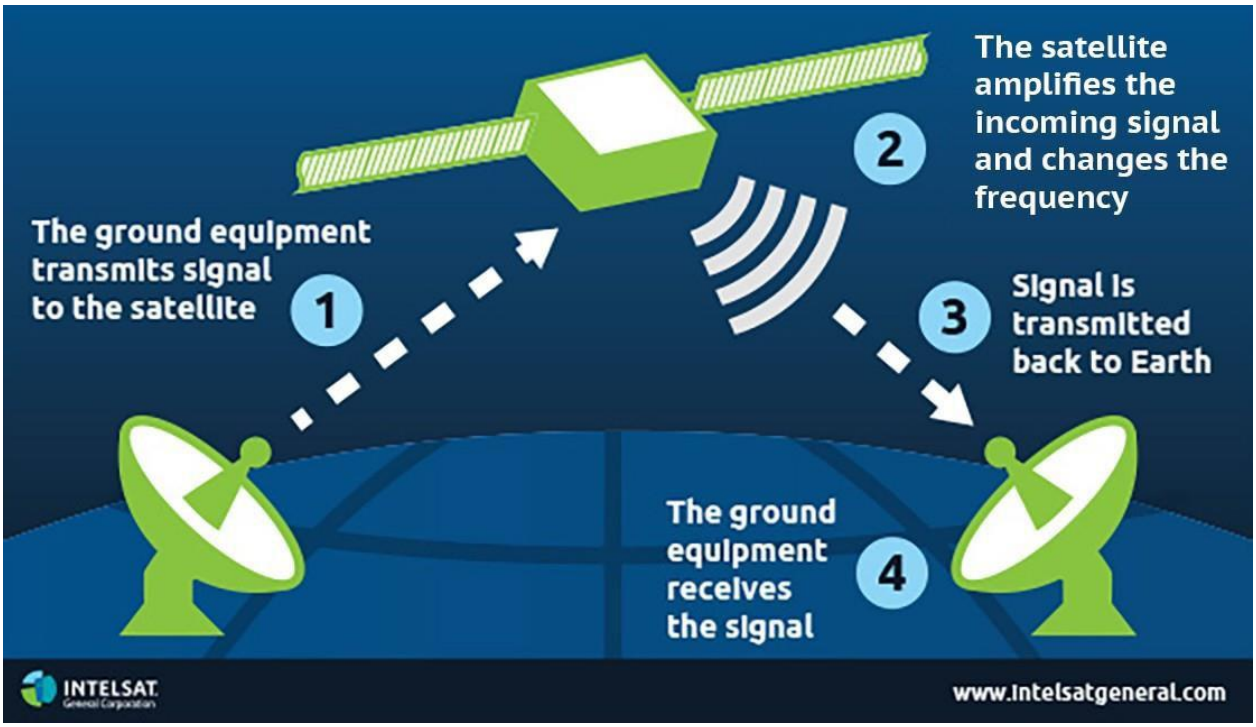
VSAT Communication System

VSAT is designed to serve both businesses and individuals and involves the use of specific technology and devices that are designed to facilitate effective telecommunications and Internet connectivity. When the system is comprised of multiple users, in order to establish communications with one another the data must be transmitted to the station-based PC which sends the signal to the sky satellite. The satellite sky transponder then forwards the data transmission to the end user’s VSAT antenna and finally to the end user’s device. VSAT can be used by both home users who sign up with a primary VSAT service and by private organizations and companies that lease or operate their own VSAT infrastructure. A main

advantage of VSAT is it provides companies with complete control over their own communications infrastructure without having to depend upon third party sources.

Satellite:

A communications satellite is an artificial satellite that relays and amplifies radio telecommunications signals via a transponder; it creates a communication channel between a source transmitter and a receiver at different locations on Earth. Communications satellites are used for television, telephone, radio, internet, and military applications. The purpose of communications satellites is to relay the signal around the curve of the Earth allowing communication between widely separated geographical points.



Applications: Television, Internet, Military

Ethernet Cable Standards:

Ethernet, developed by the Electrical and Electronic Engineers Institute, IEEE Standard 802, is the most popular LAN (local area network) technology used today. It defined the number of conductors that are required for a connection, the performance thresholds that can be expected, and provides the framework for data transmission.

The Ethernet cables for connectivity in most office and home environments rely on twisted wire pairs within an overall cable - Cat 5, Cat 6 and Cat 7 all used this format.

The Ethernet cables are available in a variety of lengths as patch cables, or the cable itself is available for incorporating into systems, buildings, etc. The terminations can then be made to the required connector using a crimp tool. These network cables are available in a variety of lengths - long Ethernet cables are available, some of the longest being up to 75 meters.

Earlier network cables were unshielded, but later ones were shielded to improve the performance. For example, an unshielded twisted pair (UTP) cable may be satisfactory for a short run between a computer

and router, but a foil shielded cable, FTP, is best longer runs or where the cable passes through areas of high electrical noise.

Flat Ethernet cable and connector

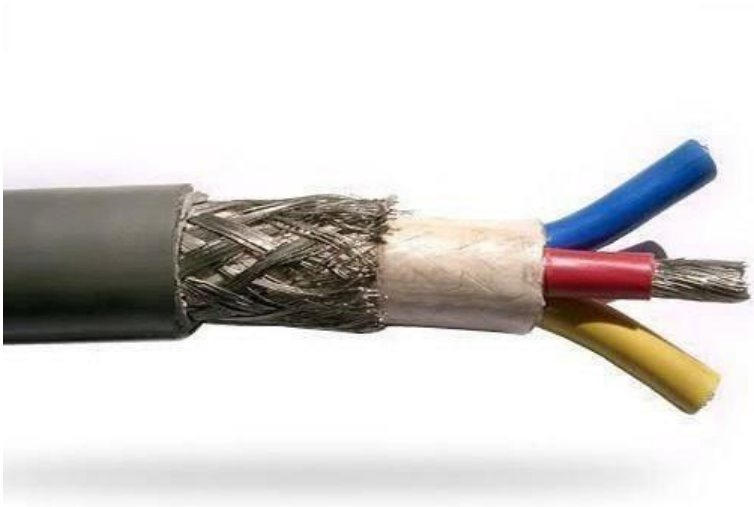
There are different methods that can be used for shielding Ethernet cables. The most common is to place a shield around each twisted pair. This not only provides shielding for the cable externally, but also reduces crosstalk between the internal twisted pairs as well. Manufacturers can further enhance the performance by placing shielding around all the wires in the cable just under the cable sheath. There are different codes used to indicate the different types of shielding:

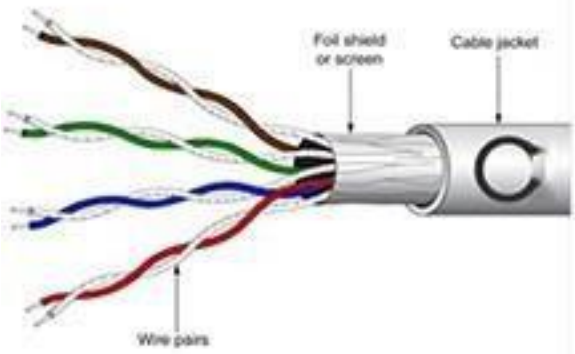
- U/UTP - Unshielded cable, unshielded twisted pairs
- F/UTP - Foil shielded cable, unshielded twisted pairs
- U/FTP - Unshielded cable, foil shielded twisted pairs
- S/FTP - braided shielded cable, foil shielded twisted pairs

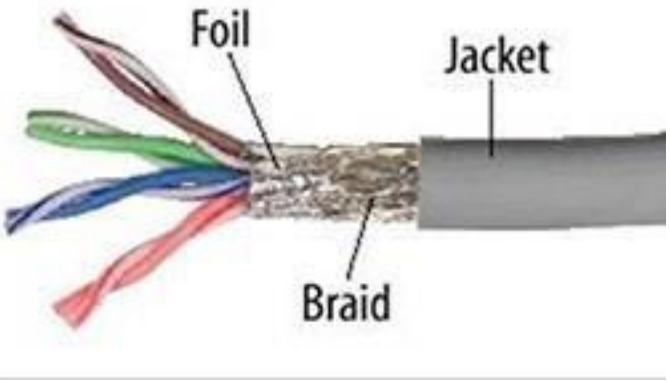
Where: TP = twisted pair, U = unshielded, F = foil shielded, S = braided shielding.

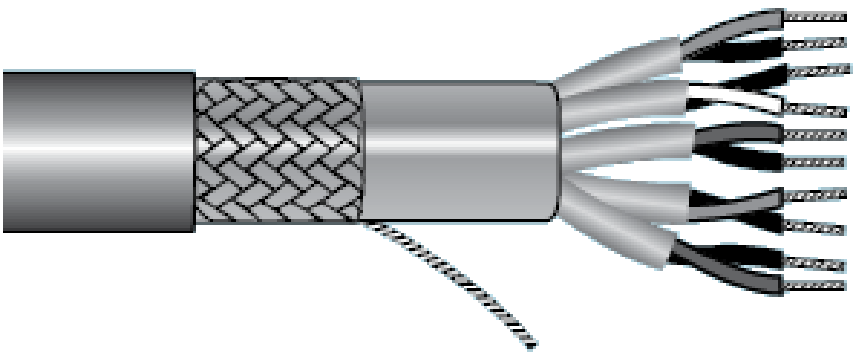
A further difference within the Ethernet cables whether Cat 5, Cat 5e, Cat 6, Cat 6e, or Cat 7 can be whether solid or stranded wires are used within the cable. As the description implies, a solid cable uses a single piece of copper for the electrical conductor within each wire of the cable whilst stranded wire uses a series of copper strands twisted together. Although when buying a patch cable, it may not be necessary to know this, when installing a long cable run it may be important as each type is slightly more suitable for different applications.

- Stranded cable: This type of wire is more flexible and it is more applicable for Ethernet cables where the cable may be moved - often it is idea for patch leads at desks or general connections to PCs, etc where some movement may be needed and expected.
- Solid cable: Solid cable is not as flexible as the stranded type, but it is also more durable. This makes it best for use in permanent installations like cable installations under floors, embedded in walls and the like.



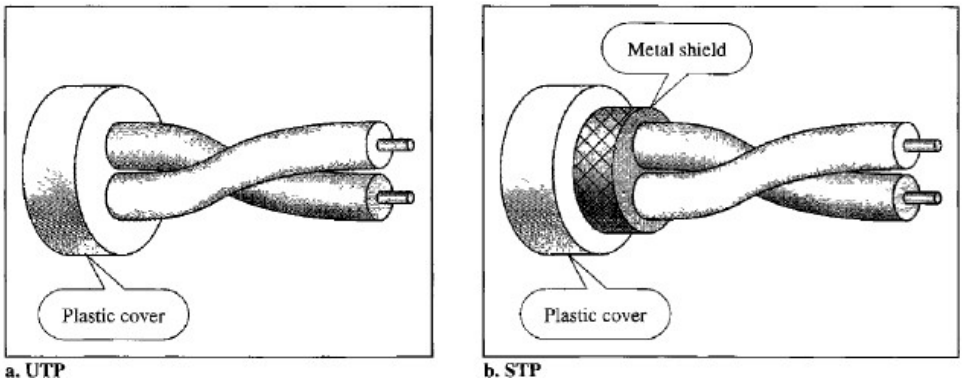

Foil shield
or screen
Cable jacket
Wire pairs


Foil
Jacket
Braid



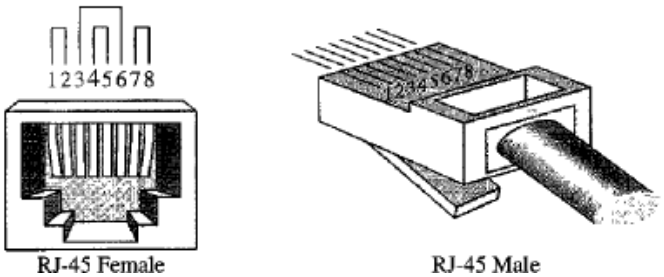
Category	Shielding	Maximum Transmission Speec (at 100m)	Maximum Bandwidth
Cat 3 cable	unshielded	10 Mbps	16 MHz
Cat 5 cable	unshielded>	10/100 Mbps	100 MHz
Cat 5e cable	unshielded	1000 Mbps / 1 Gbps	100 MHz
Cat 6 cable	shielded or unshielded	1000 Mbps / 1 Gbps	250 MHz
Cat 6a cable	shielded	10000 Mbps/ 10 Gbps	500 MHz
Cat 7 cable	shielded	10000 Mbps / 10 Gbps	600 MHz

Figure 7.4 *UTP and STP cables*



a. UTP **b. STP**

UTP connector



RJ-45 Female RJ-45 Male

Fiber Cable Standards:

Optical Fiber cables can support high bit rates, up to Gbps, immune to EMI, has very low signal attenuation up to 100 km. Standard is optical carrier (OC), ranges from 51.8 Mbps to39.8 Gbps.

There are two primary types of fiber – multimode and single mode. With the great popularity of optical links in the last few years, the main part of them is currently based on modern single-mode fibers. However, both single-mode and multimode fibers are divided into many types/categories that comply with established standards and factory specifications.

The popular markings are based on shorts of the fiber kinds:

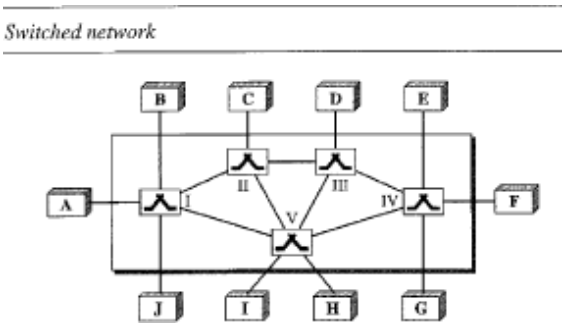
- Single Mode (Mono Mode): Single mode transmits a single beam of light from the core, hence with much smaller diameter. Used for longer distance and LASER is used as light source.
- Multi-Mode: Multimode is so named because multiple beams from a light source move through the core in different paths. Used for shorter distance and LED is used as light source. Two popular sizes of multimode fiber exist today for use in commercial applications: 50 micron and 62.5 micron. Each has a common cladding diameter (125 microns), but different core diameters (50 microns and 62.5 microns).

With demand increasing for bandwidth on data networks and LANs, single-mode fiber is becoming steadily more popular in new applications. Many installations include multimode fiber for current systems and single-mode fiber in the event of future expansion.

Switching:

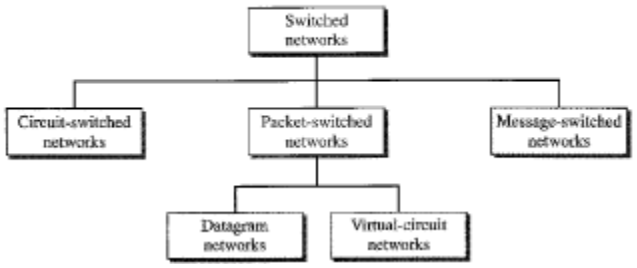
A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible. One solution is to make a point-to-point connection between each pair of devices (Mesh topology) or between a central device and every other device (a star topology). These methods are not applicable for very large networks. Other topologies employing multipoint connections are also not efficient due to the distances between devices and the total number of devices increase beyond the capacities of the media and equipment.

A better solution is **switching**. A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch.



We can divide today's network into three broad categories: circuit-switched networks, packet-switched networks and message-switched networks.

8.2 *Taxonomy of switched networks*

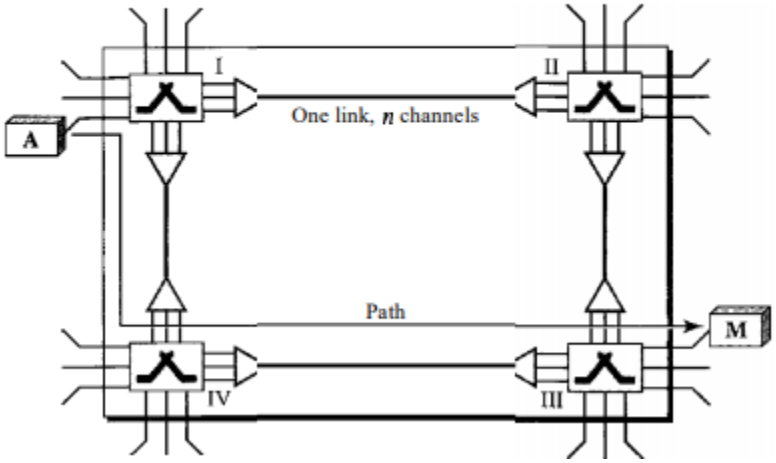


Circuit Switched Networks:

A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM.

Figure below shows a trivial circuit-switched network with four switches and four links. Each link is divided into n (n is 3 in the figure) channels by using FDM or TDM.

A trivial circuit-switched network



We have explicitly shown the multiplexing symbols to emphasize the division of the link into channels even though multiplexing can be implicitly included in the switch fabric.

The end systems, such as computers or telephones, are directly connected to a switch. We have shown only two end systems for simplicity. When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself. This is called the setup phase; a circuit (channel) is reserved on each link, and the combination of circuits or channels defines the dedicated path. After the dedicated path made of connected circuits (channels) is established, data transfer can take place. After all data have been transferred, the circuits are torn down.

We need to emphasize several points here:

- Circuit switching takes place at the physical layer.
- Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the teardown phase.
- Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.
- There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to-end addressing used during the setup phase.

Three Phases:

The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, and connection teardown.

Setup Phase

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches.

Data Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Packet Switched Networks:

A packet switched network (PSN) is a type of computer communications network that groups and sends data in the form of small packets. It enables the sending of data or network packets between a source and destination node over a network channel that is shared between multiple users and/or applications. A packet switched is also known as a connectionless network, as it does not create a permanent connection between a source and destination node. Packet-switched describes the type of network in which packets are routed through a network based on the destination address contained within each packet. Breaking communication down into packets allows the same data path to be shared among many users in the network.

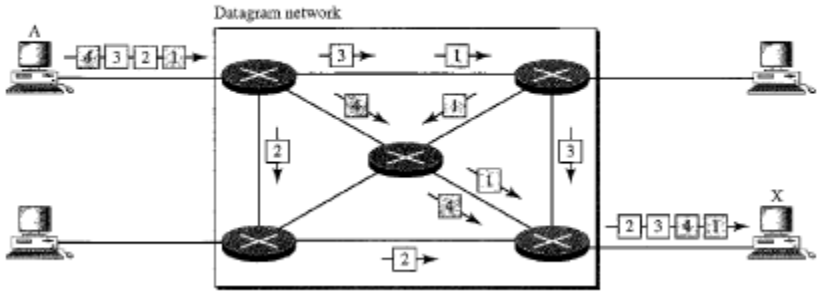
In packet switching, there is no resource allocation for a packet. This means that there is no reserved bandwidth on the links, and there is no scheduled processing time for each packet. Resources are allocated on demand. The allocation is done on a first-come, first serve basis. When a switch receives a packet, no matter what is the source or destination, the packet must wait if there are other packets being processed.

Packet switching may be classified into connectionless packet switching, also known as datagram switching, and connection-oriented packet switching, also known as virtual circuit switching.

Datagram Approach:

In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagrams. Datagram switching is normally done at the network layer.

Figure 8.7 *A datagram network with four switches (routers)*

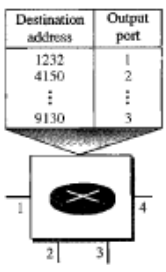


In this example, all four datagrams belong to the same message, but may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X. This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources.

The datagram networks are sometimes referred to as connectionless networks. The term connectionless here means that the switch does not keep information about the connection state. There are no setup and or teardown phases. Each packet is treated the same by a switch regardless of its source or destination.

Since there are no setup or teardown phases, each switch has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination address and the corresponding forwarding output ports are recorded in the tables. This is different from circuit-switched network in which each entry is created when the setup phase is completed and deleted when the teardown phase is over.

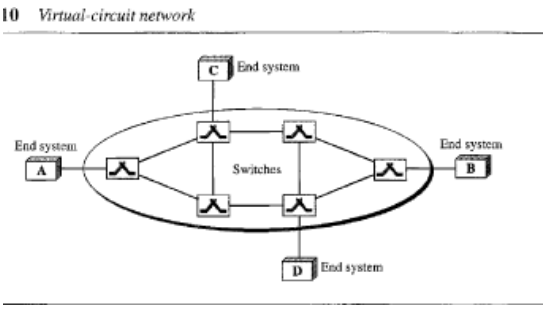
Routing table in a datagram network



Virtual Circuit Networks:

A virtual circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

- As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
- Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
- As in a datagram network, data are packetized and each packet carries an address in the header. However, the address is of the next hop to be reached towards the destination.
- As in a circuit-switched network, all packets follow the same path established during the connection.
- A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is implemented in the physical layer and a datagram network is implemented in the network layer.

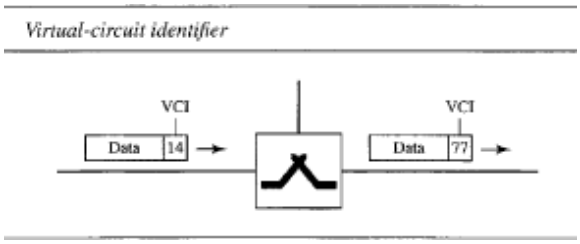


Addressing:

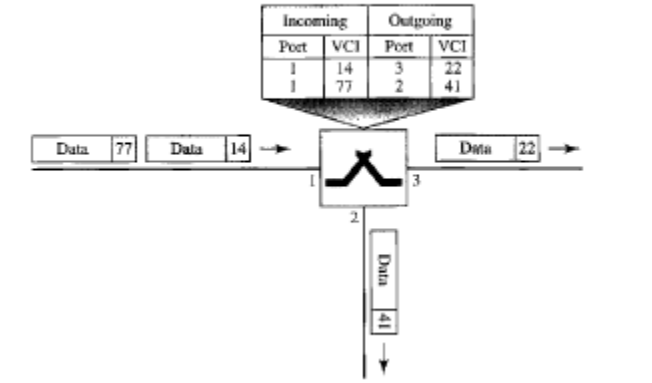
In a virtual-circuit network, two types of addressing are involved: global and local.

Global addressing: A source or a destination needs to have a global address-an address that can be unique in the scope of the network or internationally.

Local Addressing: The address that is actually used for data transfer is called the virtual-circuit identifier (VCI). A VCI, unlike a global address, is a smaller number that has only one switch scope; it is used by a frame between two switches.



Switch and tables in a virtual-circuit network



Three phases:

As in circuit-switched network, a source and destination need to go through three phases in a virtual circuit network: setup, data transfer, and teardown.

In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection.

In the teardown phase, the source and destination inform the switches to delete the corresponding entry.

Data transfer occurs between these two phases.

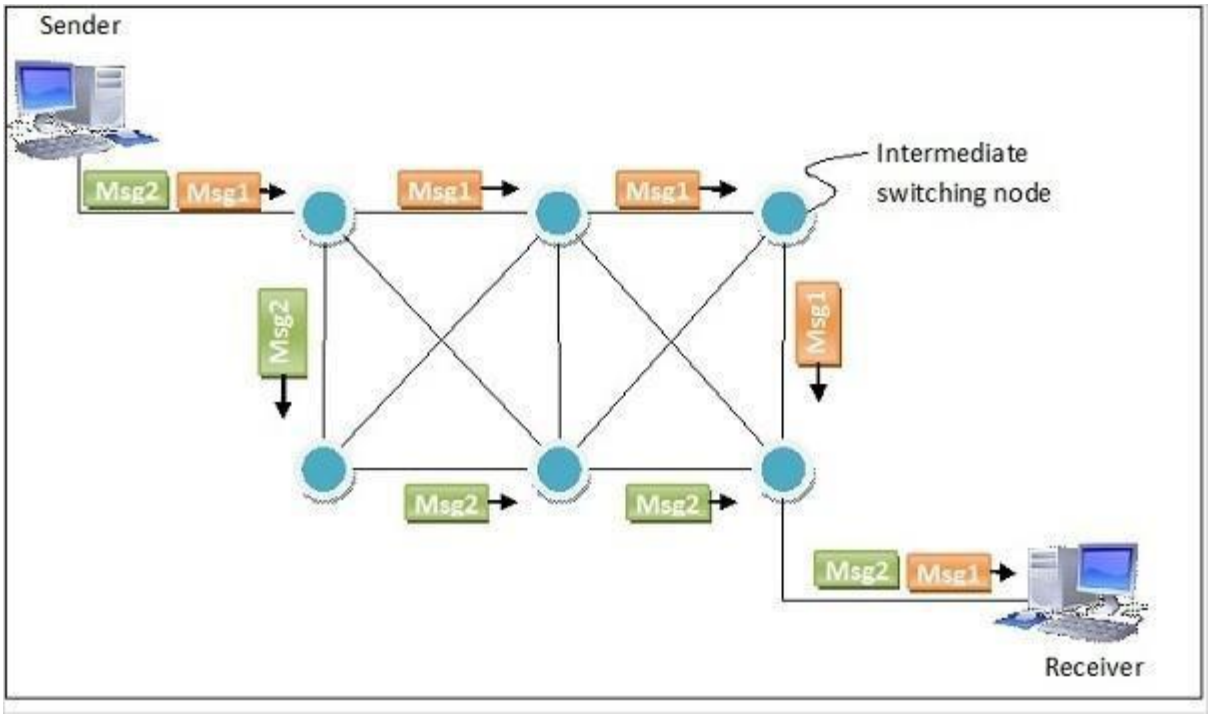
Message Switched Networks:

Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hop at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Before the advancements in packet switching, message switching acted as an efficient substitute for circuit switching.

In message switching, the source and destination nodes are not directly connected. Instead, the intermediary nodes (mainly switches) are responsible for transferring the message from one node to the next. Thus, every intermediary node inside the network needs to store every message prior to retransferring the messages one-by-one as adequate resources become available. If the resources are not available, the messages are stored indefinitely. This characteristic is known as store and forward.

The following diagram represents routing of two separate messages from the same source to same destination via different routes, using message switching.



Public Switched Telephone Network (PSTN):

The public switched telephone network (PSTN) is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephone operators, providing infrastructure and services for public telecommunication. The PSTN consists of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all interconnected by switching centers, thus allowing most telephones to communicate with each other. The public switched telephone network was formerly known simply as the public telephone network. The task of building the networks and selling services to customers fell to the network operators. In some countries, however, the job of providing telephone networks fell to government as the investment required was very large and the provision of telephone service was increasingly becoming an essential public utility.

The original concept was that the telephone exchanges are arranged into hierarchies, so that if a call cannot be handled in a local cluster, it is passed to one higher up for onward routing. This reduced the number of connecting trunks required between operators over long distances and also kept local traffic separate. A PSTN is made up of switches at centralized points on a network that function as nodes to enable communication between two points on the network. A call is placed after being routed through multiple switches. Voice signals can then travel over the connected phone lines.

Integrated Services Digital Network (ISDN):

Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. Prior to ISDN, the telephone system was viewed as a way to transport voice, with some special services available for data. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system.

ISDN Interfaces:

Among the types of several interfaces present, some of them contains channels such as the B-Channels or Bearer Channels that are used to transmit voice and data simultaneously; the D- Channels or Delta Channels that are used for signaling purpose to set up communication.

The ISDN has several kinds of access interfaces such as −

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)
- Narrowband ISDN
- Broadband ISDN

Basic Rate Interface

(BRI)

The Basic Rate Interface or Basic Rate Access, simply called the ISDN BRI Connection uses the existing telephone infrastructure. The BRI configuration provides two data or bearer channels at 64 Kbits/sec speed and one control or delta channel at 16 Kbits/sec. This is a standard rate. The ISDN BRI interface is commonly used by smaller organizations or home users or within a local group, limiting a smaller area.

Primary Rate Interface (PRI)

The Primary Rate Interface or Primary Rate Access, simply called the ISDN PRI connection is used by enterprises and offices. The PRI configuration is based on T-carrier or T1 in the US, Canada and Japan countries consisting of 23 data or bearer channels and one control or delta channel, with 64kbps speed for a bandwidth of 1.544 M bits/sec. The PRI configuration is based on E-carrier or E1 in Europe, Australia and few Asian countries consisting of 30 data or bearer channels and two-control or delta channel with 64kbps speed for a bandwidth of 2.048 M bits/sec. The ISDN PRI interface is used by larger organizations or enterprises and for Internet Service Providers.

Narrowband ISDN

The Narrowband Integrated Services Digital Network is called the N-ISDN. This can be understood as a telecommunication that carries voice information in a narrow band of frequencies. This is actually an attempt to digitize the analog voice information. This uses 64kbps circuit switching. The narrowband ISDN is implemented to carry voice data, which uses lesser bandwidth, on a limited number of frequencies.

Broadband ISDN

The Broadband Integrated Services Digital Network is called the B-ISDN. This integrates the digital networking services and provides digital transmission over ordinary telephone wires, as well as over other media. It is defined as, “Qualifying a service or system requiring transmission channels capable of supporting rates greater than primary rates.” The broadband ISDN speed is around 2 MBPS to 1 GBPS and the transmission is related to ATM, i.e., Asynchronous Transfer Mode. The broadband ISDN communication is usually made using the fiber optic cables. As the speed is greater than 1.544 Mbps, the communications based on this are called Broadband Communications. The broadband services provide a continuous flow of information, which is distributed from a central source to an unlimited number of authorized receivers connected to the network.

ISDN Standards:

The ISDN works based on the standards defined by ITU-T. The Telecommunication Standardization Sector (ITU-T) coordinates standards for telecommunications on behalf of the International Telecommunication Union (ITU) and is based in Geneva, Switzerland. The various principles of ISDN as per ITU-T recommendation are:

- To support switched and non-switched applications
- To support voice and non-voice applications
- Reliance on 64-kbps connections
- Intelligence in the network
- Layered protocol architecture
- Variety of

configurations Advantages of

ISDN

ISDN is a telephone network-based infrastructure, which enables the transmission of both voice and data simultaneously. There are many advantages of ISDN such as −

- As the services are digital, there is less chance for errors.
- The connection is faster.
- The bandwidth is higher.
- Voice, data and video − all of these can be sent over a single ISDN

line. Disadvantages of ISDN

The disadvantage of ISDN is that it requires specialized digital services and is costlier. However, the advent of ISDN has brought great advancement in communications. Multiple transmissions with greater speed are being achieved with higher levels of accuracy.

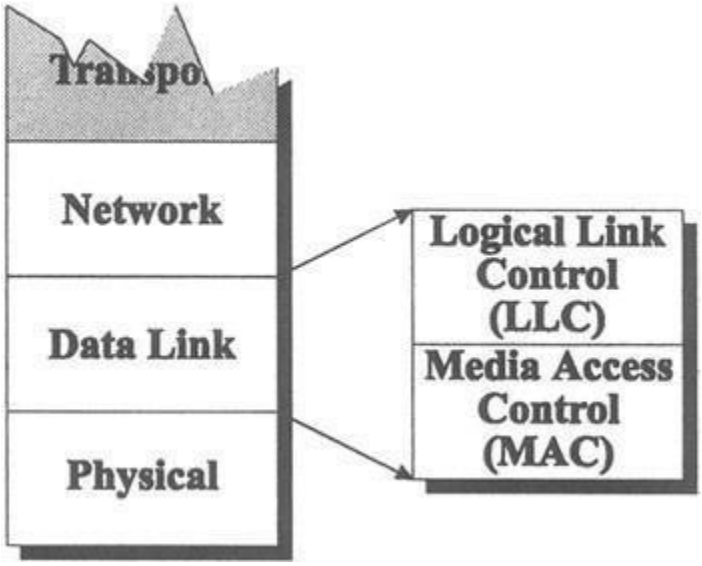
Unit 2: Data Link Layer

Functions of Data Link Layer:

The data link layer transforms the physical layer, a raw transmission facility, to a link responsible for node-to-node (hop-to-hop) communication. Specific responsibilities of the data link layer include framing, addressing, flow control, error control, and media access control. The data link layer divides the stream of bits received from the network layer into manageable data units called frames. The data link layer adds a header to the frame to define the addresses of the sender and receiver of the frame. If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver. The data link layer also adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged, duplicate, or lost frames. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Overview of Logical Link Control (LLC) and Media Access Control (MAC):

The data link layer is divided into two sublayers:

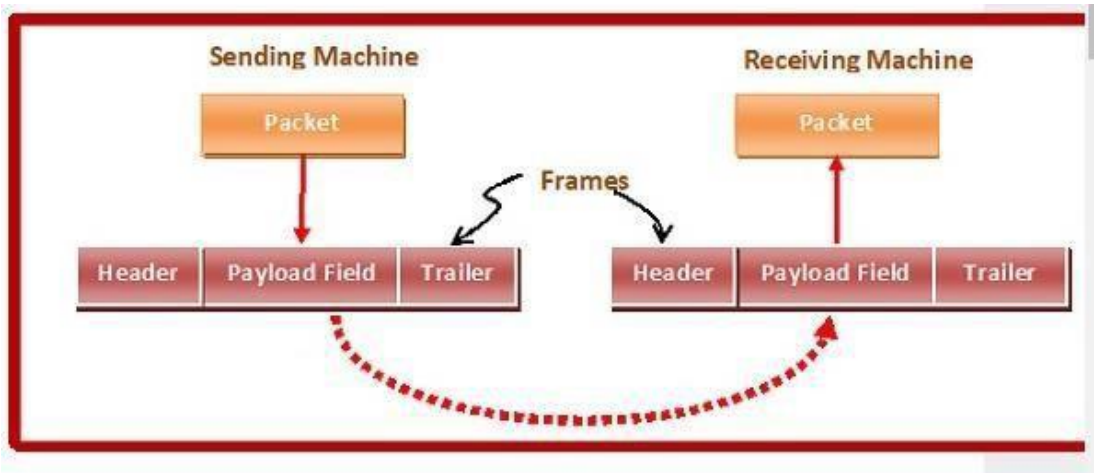


- The LLC sublayer acts as an interface between the media access control (MAC) sublayer and the network layer. Logical Link Control (LLC) sublayer provides the logic for the data link. The LLC sublayer provides multiplexing mechanisms that make it possible for several network protocols to coexist within a multipoint network and to be transported over the same network medium. Thus, it controls the synchronization, flow control, and error checking functions of the data link layer.
- Media Access Control (MAC) sublayer provides control for accessing the transmission medium. It is responsible for moving data packets from one network interface to another, across a shared transmission medium. Physical addressing is handled at the MAC sublayer. When sending data to another device on the network, the MAC sublayer encapsulates higher-level frames into frames appropriate for the transmission medium, adds a frame check sequence to identify transmission

errors, and then forwards the data to the physical layer. Additionally, the MAC is also responsible for compensating for collisions by initiating retransmission if a jam signal is detected.

Framing:

In the physical layer, data transmission involves synchronized transmission of bits from the source to the destination. The data link layer packs these bits into frames. Data-link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames. Smaller sized frames make flow control and error control more efficient. Then, it sends each frame bit-by-bit on the hardware. At receiver's end, data link layer picks up signals from hardware and assembles them into frames.



Parts of a Frame

A frame has the following parts −

Frame Header − It contains the source and the destination addresses of the frame.

Payload field − It contains the message to be delivered.

Trailer − It contains the error detection and error correction bits.

Flag − It marks the beginning and end of the frame.

Types of Framing

Framing can be of two types, fixed sized framing and variable sized framing.

Fixed-sized Framing

Here the size of the frame is fixed and so the frame length acts as delimiter of the frame.
Consequently, it does not require additional boundary bits to identify the start and end of the frame.

Example − ATM cells.

Variable – Sized Framing

Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame.

It is used in local area networks.

Flow Control Mechanisms:

Flow control coordinates the amount of data that can be sent before receiving an acknowledgment and is one of the most important duties of the data link layer. In most protocols, flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. The flow of data must not be allowed to overwhelm the receiver. Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data. The receiving device must be able to inform the sending device before those limits are reached and to request that the transmitting device send fewer frames or stop temporarily. Incoming data must be checked and processed before they can be used. The rate of such processing is often slower than the rate of transmission. For this reason, each receiving device has a block of memory, called a buffer, reserved for storing incoming data until they are processed. If the buffer begins to fill up, the receiver must be able to tell the sender to halt transmission until it is once again able to receive.

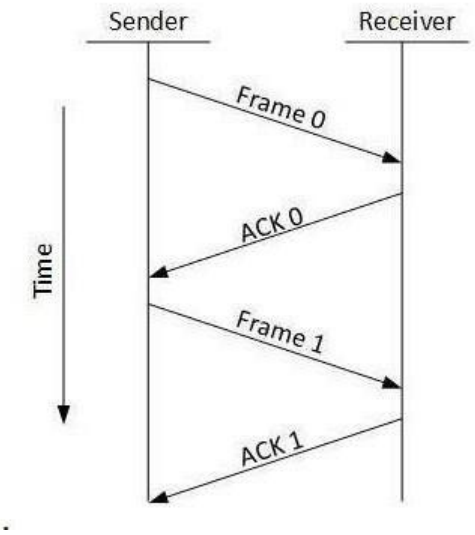
When a data frame is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. If sender is sending too fast, the receiver may be overloaded and data may be lost.

Two types of mechanisms can be deployed to control the flow:

- A simple stop and wait Protocol
- Sliding Window Protocol

<u>Simplex Stop and Wait</u>

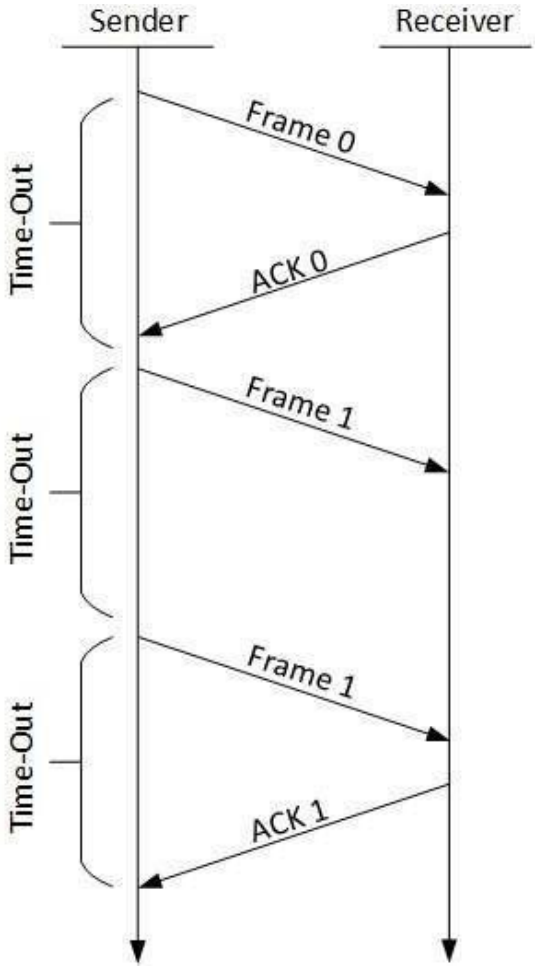
This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received. The sender sends the next frame only when it has received a positive acknowledgement from the receiver that it is available for further data processing. Data transmission is one directional, but must have bidirectional line.



Stop and Wait ARQ

The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.



Sliding Window

In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible. In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver. The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing. In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window. The size of the sending window determines the sequence number of the outbound frames. The size of the receiving window is the maximum number of frames that the receiver can accept at a time. It determines the maximum number of frames that the sender can send before receiving acknowledgment.

The types of sliding window protocol include:

- A One Bit Sliding Window Protocol
- A Protocol Using Go Back N
- A Protocol Using Selective Repeat

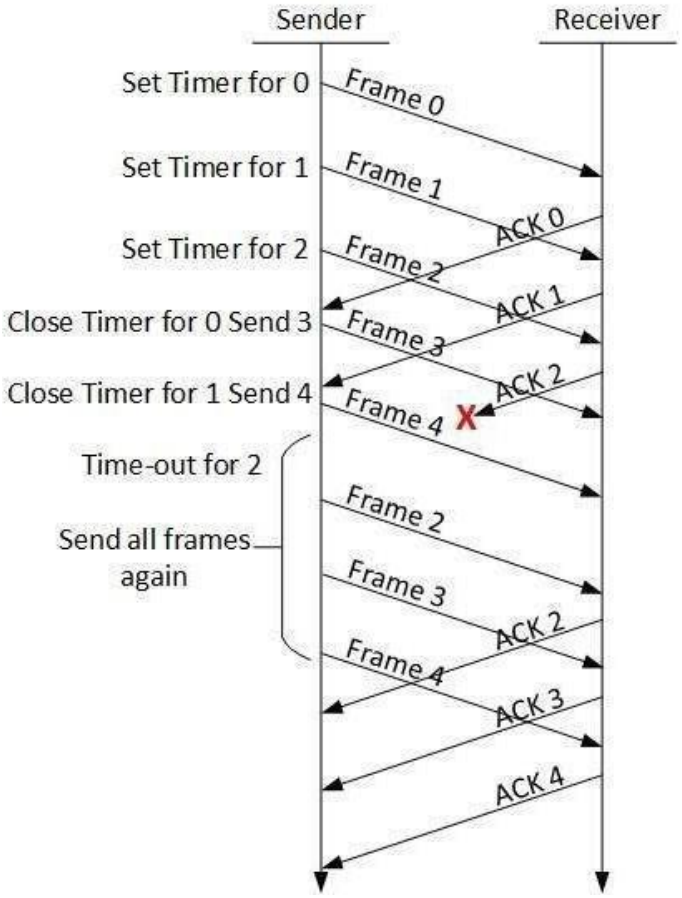
Note: ARQ (Automatic Repeat Request) is designed for noisy channels.

One Bit sliding window protocol:

In one – bit sliding window protocol, the size of the window is 1. So, the sender transmits a frame, waits for its acknowledgment, then transmits the next frame. Thus, it uses the concept of stop and wait protocol. This protocol provides for full – duplex communications. Hence, the acknowledgment is attached along with the next data frame to be sent called piggybacking. So, it is better compared to stop and wait due to full duplex communications.

Go-Back-N ARQ:

In this protocol, we can send several frames before receiving acknowledgements; we keep a copy of these frames until the acknowledgements arrive. Stop and wait mechanism does not utilize the resources at their best. When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N method, both sender and receiver maintain a window.



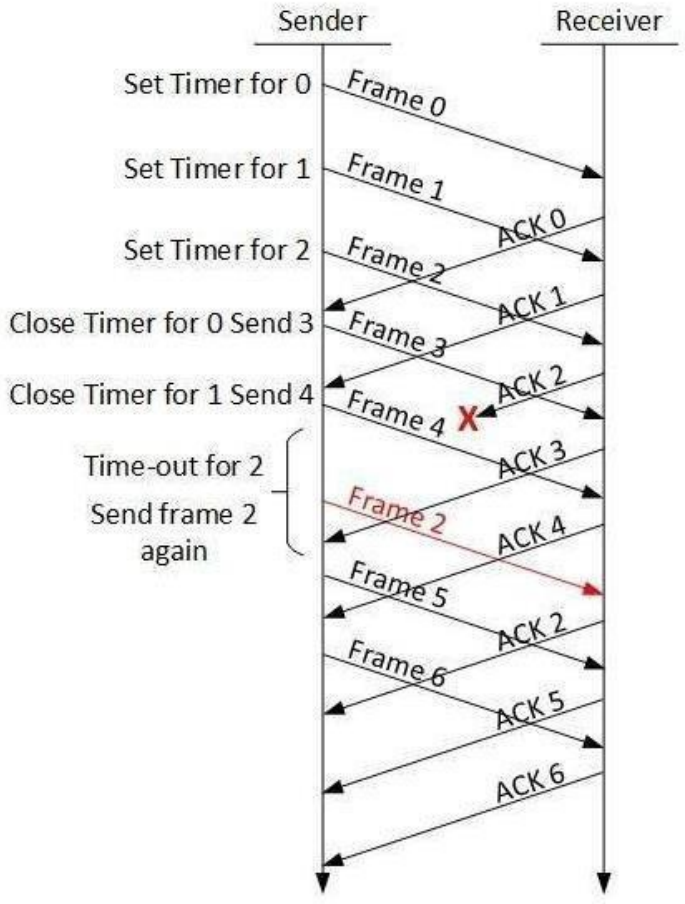
The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames.

If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

Selective Repeat ARQ:

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.



In Selective-Repeat, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged. The sender in this case, sends only packet for which NACK is received.

Error Detection and Correction Techniques:

Networks must be able to transfer data from one device to another with acceptable accuracy. For most applications, a system must guarantee that the data received are identical to the data transmitted. Any time data are transmitted from one node to the next, they can become corrupted in passage. Many factors can alter one or more bits of a message. Some applications require a mechanism for detecting and correcting errors.

Some applications can tolerate a small level of error. For example, random errors in audio or video transmissions may be tolerable, but when we transfer text, we expect a very high level of accuracy.

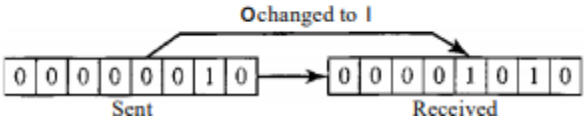
Types of Errors:

Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal. In a single-bit error, a 0 is changed to a 1 or a 1 to a 0. In a burst error, multiple bits are changed.

Single-Bit Error:

The term single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1.

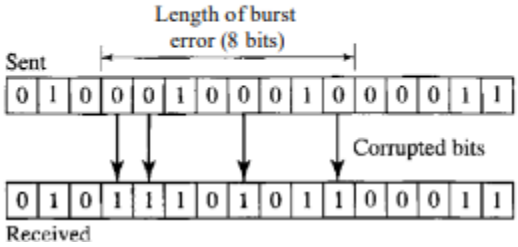
Single-bit error



Burst Error:

The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

Burst error of length 8



A burst error is more likely to occur than a single-bit error. The duration of noise is normally longer than the duration of 1 bit, which means that when noise affects data, it affects a set of bits. The number of bits affected depends on the data rate and duration of noise.

Redundancy

The central concept in detecting or correcting errors is redundancy. To be able to detect or correct errors, we need to send some extra bits with our data. These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits.

Detection Versus Correction

The correction of errors is more difficult than the detection. In error detection, we are looking only to see if any error has occurred. The answer is a simple yes or no. We are not even interested in the number of errors. A single-bit error is the same for us as a burst error. In error correction, we need to know the exact number of bits that are corrupted and more importantly, their location in the message. The number of the errors and the size of the message are important factors. If we need to correct one single error in an 8-bit data unit, we need to consider eight possible error locations; if we need to correct two errors in a data unit of the same size, we need to consider 28 possibilities.

Forward Error Correction Versus Retransmission

There are two main methods of error correction. Forward error correction is the process in which the receiver tries to guess the message by using redundant bits. This is possible if the number of errors is small. Correction by retransmission is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message. Resending is repeated until a message arrives that the receiver believes is error-free.

Error Detecting Codes

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message.

Some popular techniques for error detection are:

- Parity
- Checksum
- Cyclic redundancy check

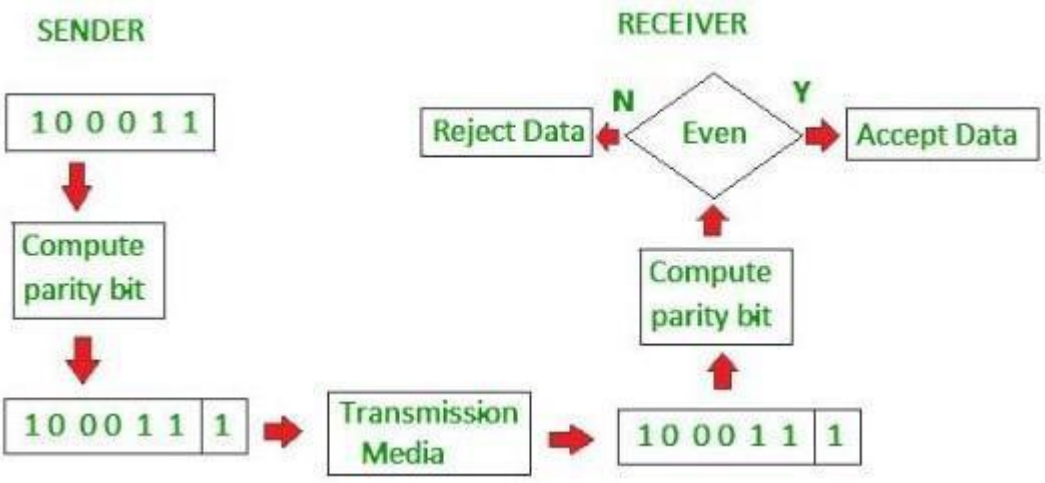
Parity check

The most common and least expensive mechanism for error- detection is the parity check. The parity check is done by adding an extra bit, called parity bit to the data to make a number of 1s either even in case of even parity or odd in case of odd parity. While creating a frame, the sender counts the number of 1s in it and adds the parity bit in the following way:

- In case of even parity: If a number of 1s is even then parity bit value is 0. If the number of 1s is odd then parity bit value is 1.
- In case of odd parity: If a number of 1s is odd then parity bit value is 0. If a number of 1s is even then parity bit value is 1.

On receiving a frame, the receiver counts the number of 1s in it. In case of even parity check, if the count of 1s is even, the frame is accepted, otherwise, it is rejected. A similar rule is adopted for odd parity check.

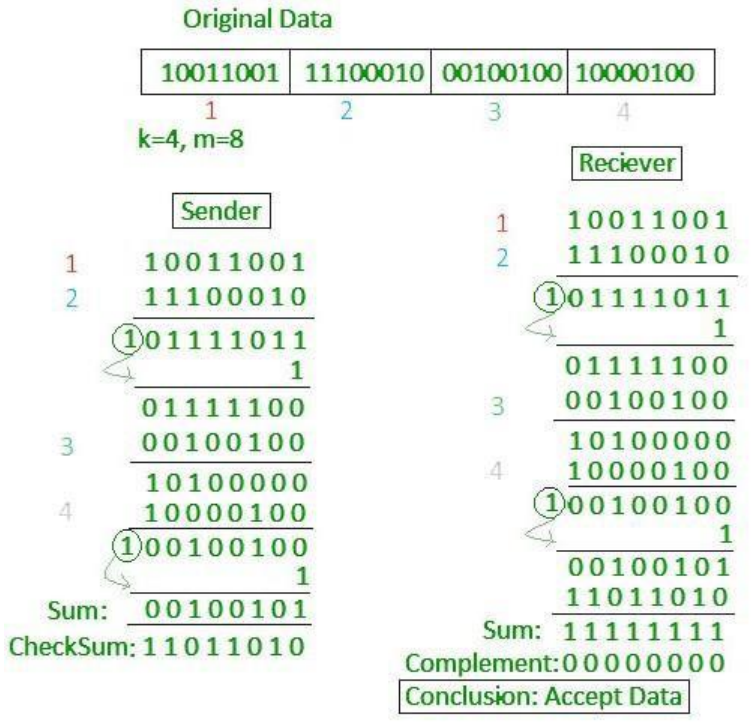
The parity check is suitable for single bit error detection only.



Checksum

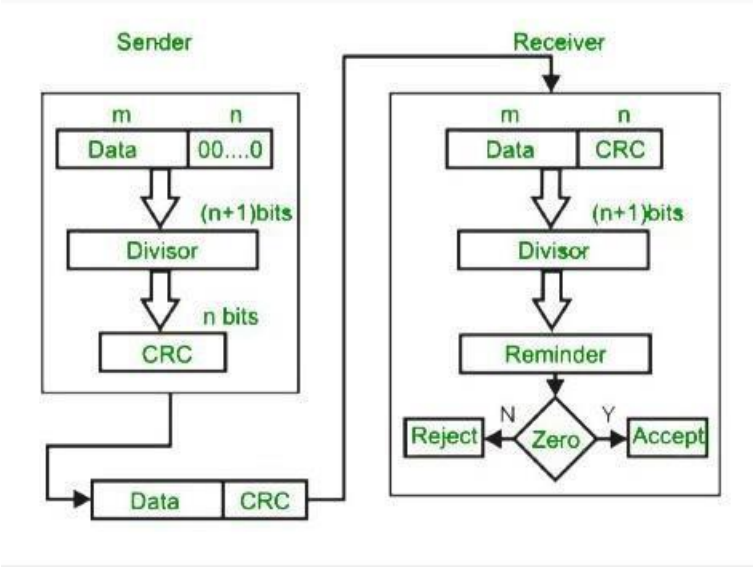
In this error detection scheme, the following procedure is applied:

- Data is divided into fixed sized frames or segments. (k segments each of m bits)
- The sender adds the segments using 1's complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames.
- The receiver adds the incoming segments along with the checksum using 1's complement arithmetic to get the sum and then complements it.
- If the result is zero, the received frames are accepted; otherwise, they are discarded.

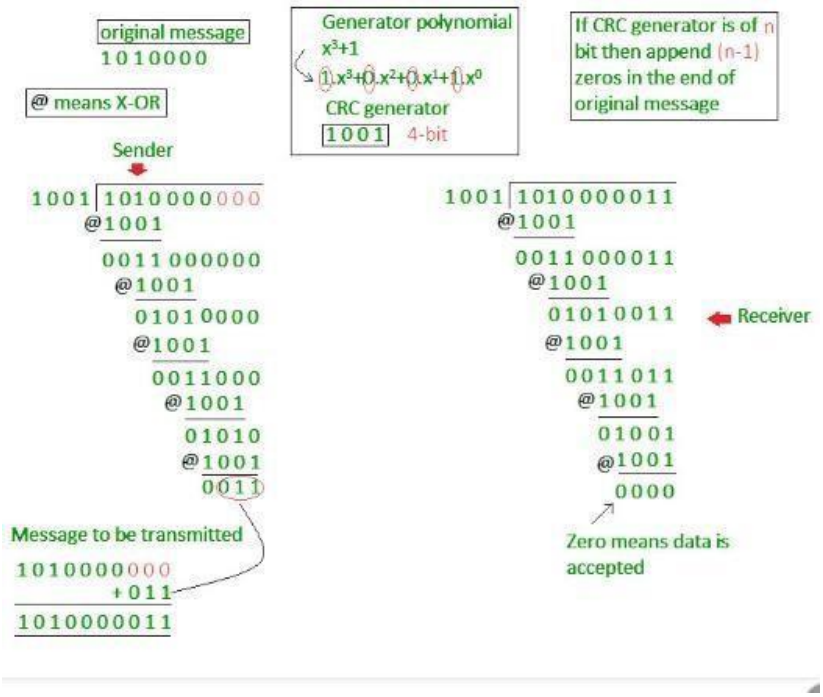


Cyclic Redundancy Check:

A cyclic redundancy check (CRC) is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Unlike checksum scheme, which is based on addition, CRC is based on binary division. In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number. At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted. A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



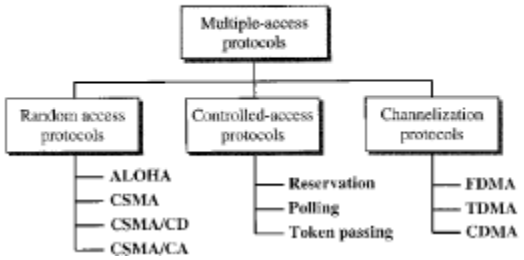
At the sender side, the data unit to be transmitted IS divided by a predetermined divisor (binary number) in order to obtain the remainder. This remainder is called CRC. The CRC has one bit less than the divisor. It means that if CRC is of n bits, divisor is of n+ 1 bit. The sender appends this CRC to the end of data unit such that the resulting data unit becomes exactly divisible by predetermined divisor i.e. remainder becomes zero. At the destination, the incoming data unit i.e. data + CRC is divided by the same number (predetermined binary divisor). If the remainder after division is zero then there is no error in the data unit & receiver accepts it. If remainder after division is not zero, it indicates that the data unit has been damaged in transit and therefore it is rejected. This technique is more powerful than the parity check and checksum error detection.



Multiple Access Protocols (Channel Allocation Techniques):

When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple access protocol to coordinate access to the link. Many formal protocols have been devised to handle access to a shared link. We categorize them into three groups.

Taxonomy of multiple-access protocols discussed in this chapter



Random access:

In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits or does not permit another station to send. At each instance, a station that has to send uses a procedure defined by the protocol to make a decision on whether or not to send. This decision depends on the state of the medium (idle or busy). In other words, each station can transmit when it desires on testing of the state of the medium.

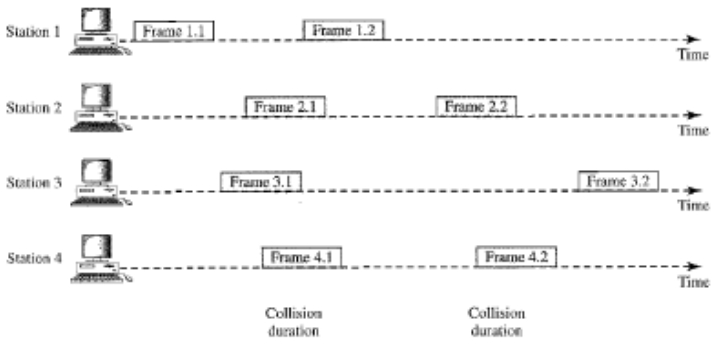
ALOHA:

ALOHA is the earliest random-access method developed for wireless LAN but can be used on any shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision. The data from the two stations collide.

Pure ALOHA:

The idea behind this protocol is that each station sends a frame whenever it has a frame to send. However, since there is only one channel to share, there is possibility of collision between frames from different stations. Even if one bit of a frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed.

Figure 12.3 *Frames in a pure ALOHA network*



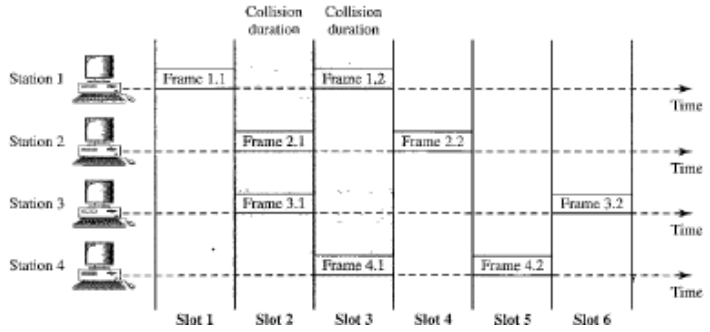
The pure ALOHA protocol relies on acknowledgements from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgement. If the acknowledgement does not arrive after the time out period, the station assumes that the frame (or the acknowledgement) has been destroyed and resends the frame. A collision involves two or more stations. If all these stations try to resend their frames after the time out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions, called back-off time. Since different stations may wait for different amount of time, the probability of further collision decreases.

Slotted ALOHA:

In pure ALOHA, there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. So, still the collision may occur.

Slotted ALOHA is similar to pure ALOHA, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

Figure 12.6 *Frames in a slotted ALOHA network*



Allowing a station to send only at the beginning of the time slot means that the station sending in the previous slot has finished sending its frame already. However, there is still possibility of collision if two stations try to send at the beginning of the same time slot.

Carrier Sense Multiple Access (CSMA):

The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. (listen before talk)

However, there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA access modes-

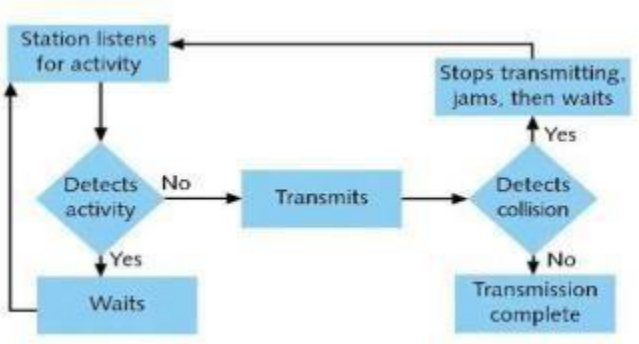
- 1-persistent: The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally (with 1 probability) as soon as the channel gets idle.
- Non-Persistent: The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- P-persistent: The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it sends with p probability. This repeat continues until the frame is sent. It is used in Wi-Fi and packet radio systems.
- O-persistent: Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

Carrier sense multiple access with collision detection (CSMA/CD):

The CSMA method does not specify the procedure following a collision. In Carrier sense multiple access with collision detection method, a station monitors the medium after it sends a frame to see if the

transmission was successful. If so, the transmission is completed. However, if there is a collision, the frame is sent again.

The basic idea behind CSMA/CD is that a station needs to be able to receive while transmitting, to detect a collision. When there is no collision, the station receives one signal; its own signal. When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station. To distinguish between these two cases, the received signals in these two cases must be significantly different. In other words, the signal from the second station needs to add a significant amount of energy to the one created by the first station.

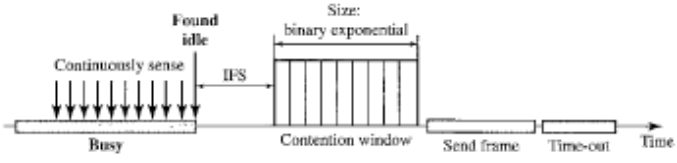


Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA):

The process of collision detection involves sender receiving acknowledgement signals. If there is just one signal (its own), then the data is successfully sent but if there are two signals (its own and the one with which it has collided), then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. The second signal adds significant amount of energy to the first signal. However, this applies only to the wired networks since the received signal has almost the same energy as the sent signal. In wireless networks, much of the sent energy is lost in transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10 percent additional energy. This is not useful for effective collision detection.

We need to avoid collisions on wireless networks because they cannot be detected. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) was invented for this network. In contrast to the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) protocol, which handles transmissions only after a collision has taken place, CSMA/CA works to avoid collisions prior to their occurrence. Collisions are avoided through the use of CSMA/CA's three strategies as shown in figure below.

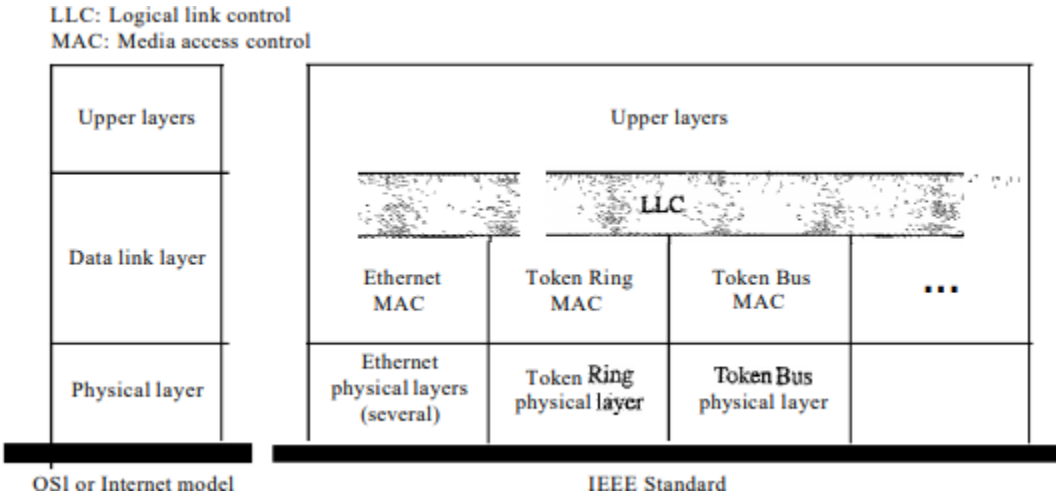
Figure 12.16 *Timing in CSMA/CA*



- Interframe space – Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time, it again checks the medium for being idle. IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.
- Contention Window –It is the amount of time divided into slots. A station which is ready to send frames chooses random number of slots as wait time.
- Acknowledgement – The positive acknowledgements and time-out timer can help guarantee a successful transmission of the frame.

Overview of IEEE Standard 802:

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 does not seek to replace any part of the OSI or the Internet model. Instead, it is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

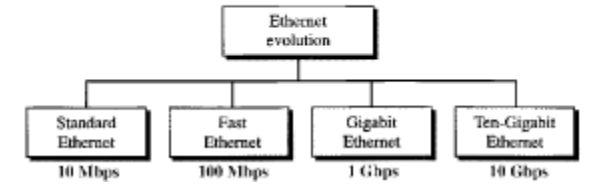


IEEE 802 is comprised of standards with separate working groups that regulate different communication networks, including IEEE 802.1 for bridging (bottom sublayer), 802.2 for Logical link (upper sublayer), 802.3 for Ethernet, 802.5 for token ring, 802.11 for Wi-Fi, 802.15 for Wireless Personal area networks, 802.15.1 for Bluetooth, 802.16 for Wireless Metropolitan Area Networks etc.

Ethernet:

The original Ethernet was created in 1976 and since then, it has gone through four generations.

Ethernet evolution through four generations



Ethernet is a family of computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN). Systems using Ethernet communication divide data streams into packets, which are known as frames. Frames include source and destination address information, as well as mechanisms used to detect errors in transmitted data and retransmission requests. An Ethernet cable is the physical, encased wiring over which the data travels. Compared to wireless LAN technology, Ethernet is typically less vulnerable to disruptions. It can also offer a greater degree of network security and control than wireless technology, as devices must connect using physical cabling, making it difficult for outsiders to access network data or hijack bandwidth for unsanctioned devices.

Token Ring:

Token ring is the IEEE 802.5 standard for a token-passing ring in Communication networks. A ring consists of a collection of ring interfaces connected by point-to-point lines i.e. ring interface of one station is connected to the ring interfaces of its left station as well as right station. Internally, signals travel around the Communication network from one station to the next in a ring. These point-to-point links can be created with twisted pair, coaxial cable or fiber optics. Each bit arriving at an interface is copied into a 1-bit buffer. In this buffer the bit is checked and may be modified and is then copied out to the ring again. This copying of bit in the buffer introduces a 1-bit delay at each interface.

Token Ring is a LAN protocol defined in the IEEE 802.5 where all stations are connected in a ring and each station can directly hear transmissions only from its immediate neighbor. Permission to transmit is granted by a message (token) that circulates around the ring. A token is a special bit pattern (3 bytes long). There is only one token in the network. Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token in order to transmit data, it seizes the token, alters 1 bit of the token (which turns the token into a start-of- frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. Since only one station can possess the token and transmit data at any given time, there are no collisions.

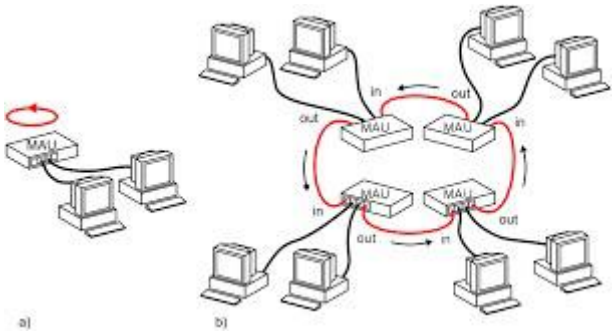


Fig: Two examples of Token Ring networks a) Using a single MAU b) Using several MAUs connected to each other

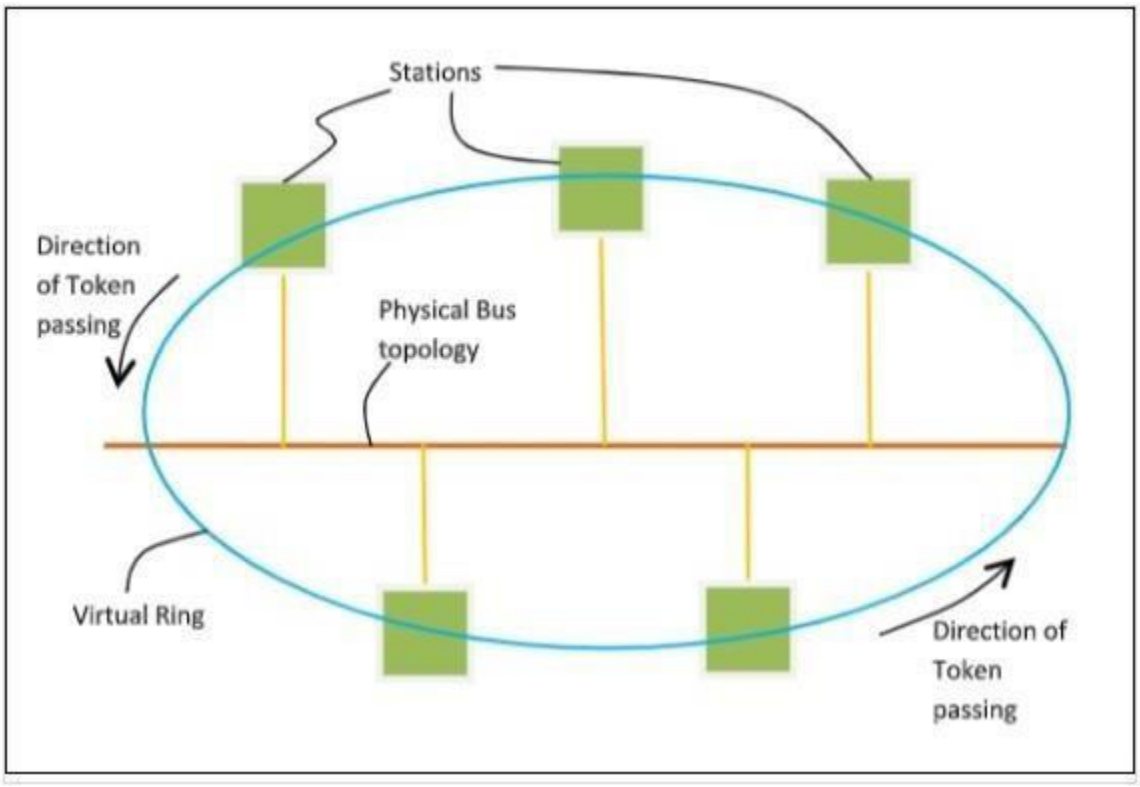
MAU (Media Access Unit)

Token Bus:

Token Bus (IEEE 802.4) is a standard for implementing token ring over virtual ring in LANs. The physical media has a bus or a tree topology and uses coaxial cables. A virtual ring is created with the nodes/stations and the token is passed from one node to the next in a sequence along this virtual ring. Each node knows the address of its preceding station and its succeeding station. A station can only transmit data when it has the token. The working principle of token bus is similar to Token Ring.

Token Passing Mechanism in Token Bus

A token is a small message that circulates among the stations of a computer network providing permission to the stations for transmission. If a station has data to transmit when it receives a token, it sends the data and then passes the token to the next station; otherwise, it simply passes the token to the next station. This is depicted in the following diagram:



Differences between Token Ring and Token Bus

Token Ring	Token Bus
The token is passed over the physical ring formed by the stations and the coaxial cable network.	The token is passed along the virtual ring of stations connected to a LAN.
The stations are connected by ring topology, or sometimes star topology.	The underlying topology that connects the stations is either bus or tree topology.
It is defined by IEEE 802.5 standard.	It is defined by IEEE 802.4 standard.
The maximum time for a token to reach a station can be calculated here.	It is not feasible to calculate the time for token transfer.

Wireless LANs:

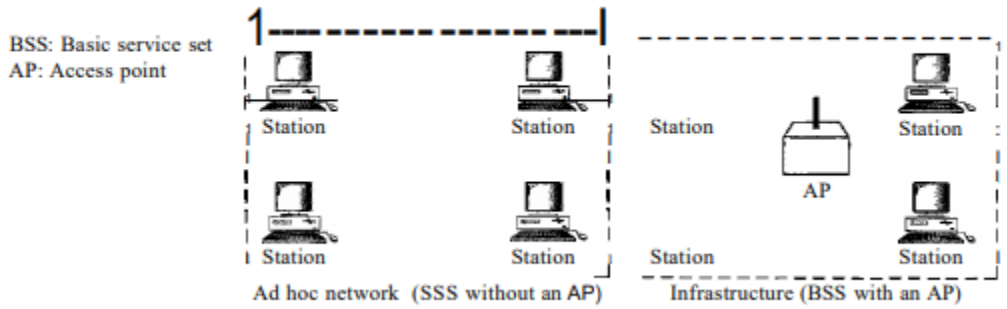
IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

Basic Service Set

IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made up of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). Figure below shows two sets in this standard.

Figure 14.1 *Basic service sets (BSSs)*

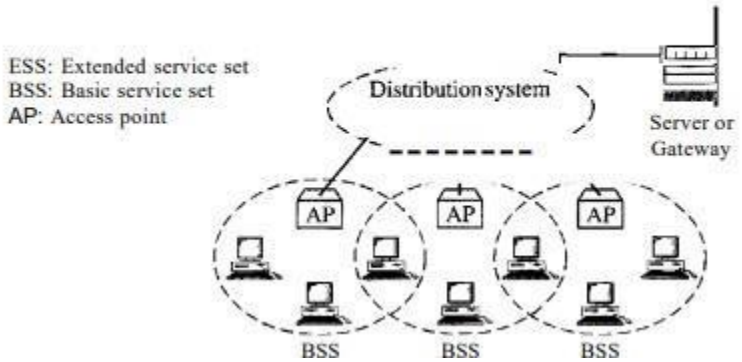


The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure network.

Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is usually a wired LAN. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN.

Extended service sets (ESSs)



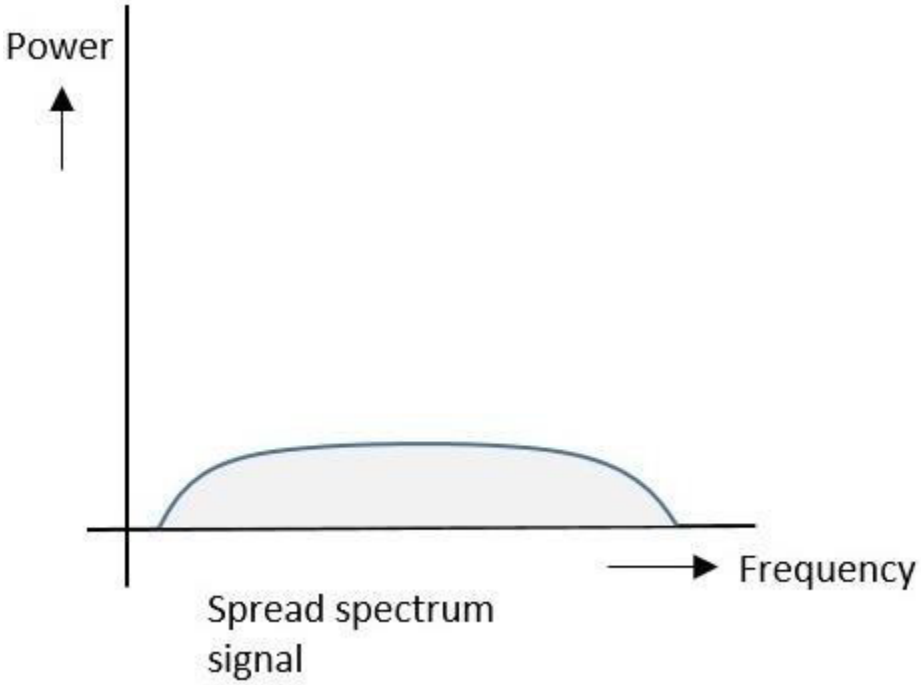
When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs. The idea is similar to communication in a cellular network if we consider each BSS to be a cell and each AP to be a base station. Note that a mobile station can belong to more than one BSS at the same time.

Spread Spectrum:

Spread spectrum is currently the most widely used transmission technique for wireless LANs. It was initially developed by the military to avoid jamming and eavesdropping of the signals. This is done by spreading the signal over a range of frequencies.

A collective class of signaling techniques are employed before transmitting a signal to provide a secure communication, known as the Spread Spectrum Modulation. The main advantage of spread spectrum communication technique is to prevent “interference” whether it is intentional or unintentional.

The signals modulated with these techniques are hard to interfere and cannot be jammed. An intruder with no official access is never allowed to crack them. Hence, these techniques are used for military purposes. These spread spectrum signals transmit at low power density and has a wide spread of signals.



Bluetooth:

Bluetooth is a short-range wireless communication technology that allows devices such as mobile phones, computers, and peripherals to transmit data or voice wirelessly over a short distance. The purpose of Bluetooth is to replace the cables that normally connect devices, while still keeping the communications between them secure. It creates a 10-meter radius wireless network, called a personal area network (PAN) or piconet, which can network between two and eight devices. Bluetooth uses less power and costs less

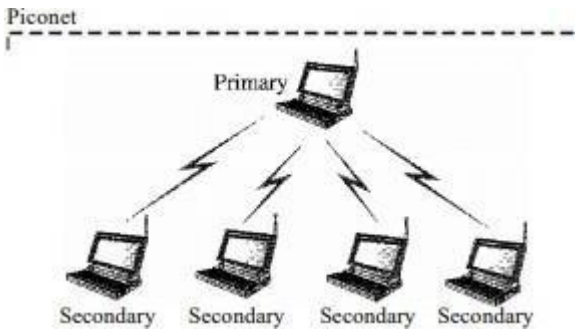
to implement than Wi-Fi. Its lower power also makes it far less prone to suffering from or causing interference with other wireless devices in the same 2.4GHz radio band.

There are some downsides to Bluetooth. The first is that it can be a drain on battery power for mobile wireless devices like smartphones, though as the technology (and battery technology) has improved, this problem is less significant than it used to be. Also, the range is fairly limited, usually extending only about 30 feet, and as with all wireless technologies, obstacles such as walls, floors, or ceilings can reduce this range further. The pairing process may also be difficult, often depending on the devices involved, the manufacturers, and other factors that all can result in frustration when attempting to connect.

Bluetooth defines two types of networks: piconet and scatternet.

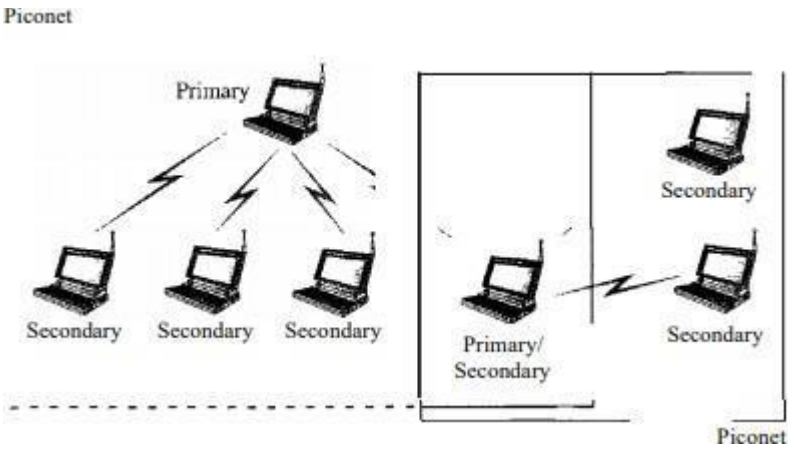
Piconets

A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; t the rest are called secondaries. All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station. The communication between the primary and the secondary can be one-to-one or one-to-many. Figure below shows a piconet.



Scatternet

Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets. Figure below illustrates a scatternet.



Wi-Fi:

The IEEE 802.11 wireless LAN, also known as Wi-Fi, is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. Wi-Fi networks have no physical wired connection between sender and receiver, by using radio frequency (RF) technology (a frequency within the electromagnetic spectrum associated with radio wave propagation). When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space.

There are several 802.11 standards for wireless LAN technology, including 802.11b, 802.11a, and 802.11g. Table below summarizes the main characteristics of these standards. 802.11g is by far the most popular technology.

Standard	Frequency Range (United States)	Data Rate
802.11b	2.4–2.485 GHz	up to 11 Mbps
802.11a	5.1–5.8 GHz	up to 54 Mbps
802.11g	2.4–2.485 GHz	up to 54 Mbps

Wi-Fi uses multiple parts of the IEEE 802 protocol family and is designed to seamlessly interwork with its wired sister protocol Ethernet. Devices that can use Wi-Fi technologies include desktops and laptops, smartphones and tablets, smart TVs, printers, digital audio players, digital cameras, cars and drones. Compatible devices can connect to each other over Wi-Fi through a wireless access point as well as to connected Ethernet devices and may use it to access the Internet. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometers achieved by using multiple overlapping access points.

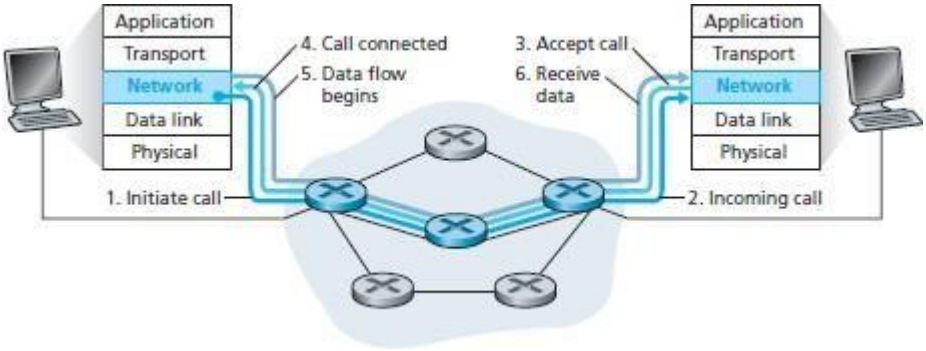
Wi-Fi is potentially more vulnerable to attack than wired networks because anyone within range of a network with a wireless network interface controller can attempt access. Wi-Fi Protected Access (WPA) is

a family of technologies created to protect information moving across Wi-Fi networks and includes solutions for personal and enterprise networks.

Overview of Virtual Circuit Switching:

Virtual circuit switching is a packet switching methodology whereby a path is established between the source and the final destination through which all the packets will be routed during a call. This path is called a virtual circuit because to the user, the connection appears to be a dedicated physical circuit. However, other communications may also be sharing the parts of the same path. So, virtual circuit packet switching is connection oriented.

Before the data transfer begins, the source and destination identify a suitable path for the virtual circuit. All intermediate nodes between the two points put an entry of the routing in their routing table for the call. Additional parameters, such as the maximum packet size, are also exchanged between the source and the destination during call setup. The virtual circuit is cleared after the data transfer is completed.



Advantages of virtual circuit switching are:

- Packets are delivered in order, since they all take the same route;
- The overhead in the packets is smaller, since there is no need for each packet to contain the full address;
- The connection is more reliable, network resources are allocated at call setup so that even during times of congestion, provided that a call has been setup, the subsequent packets should get through;
- Billing is easier, since billing records need only be generated per call and not per packet.

Overview of Frame Relay:

Frame Relay is a virtual-circuit wide-area network that was designed in response to demands for a new type of WAN. Frame Relay is a wide area network with the following features:

1. Frame Relay operates at a higher speed (1.544 Mbps and recently 44.376 Mbps).

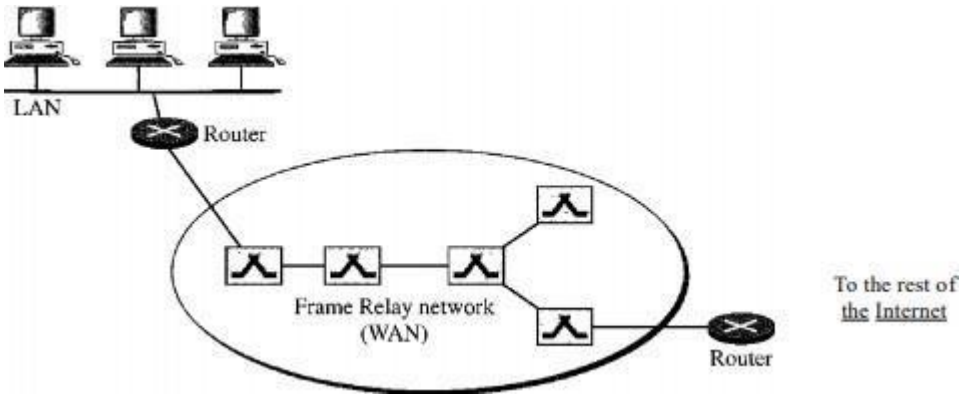
2. Frame Relay operates in just the physical and data link layers. This means it can easily be used as a backbone network to provide services to protocols that already have a network layer protocol, such as the Internet.

3. Frame Relay allows bursty data.

4. Frame Relay allows a frame size of 9000 bytes, which can accommodate all local area network frame sizes.

5. Frame Relay is less expensive than other traditional WANs.

6. Frame Relay has error detection at the data link layer only. There is no flow control or error control. There is not even a retransmission policy if a frame is damaged; it is silently dropped. Frame Relay was designed in this way to provide fast transmission capability for more reliable media and for those protocols that have flow and error control at the higher layers.



Frame relay is a virtual circuit packet switching technology that fragmented into transmission units called frames and sent in high-speed bursts through a digital network. Establishes an exclusive connection during the transmission period called virtual connection. Frame relay puts data in a variable-size unit called a frame and leaves any necessary error correction (retransmission of data) up to the endpoints, which speeds up overall data transmission. Configuring user equipment in a Frame Relay network is extremely simple. The connection-oriented service provided by Frame Relay has properties like non-duplication of frames, preservation of the frame transfer order and small probability of frame loss. The features provided by Frame Relay make it one of the best choices for interconnecting local area networks using a wide area network. However, the drawback in this method is that it becomes prohibitively expensive with growth of the network.

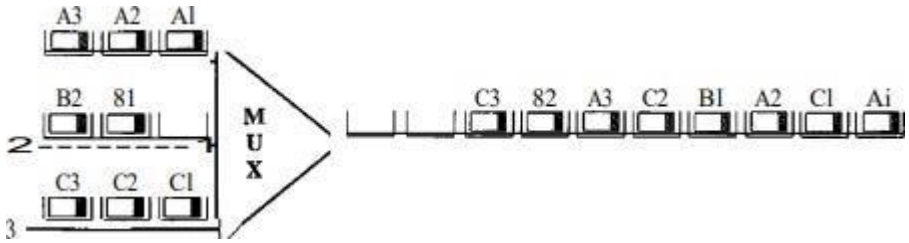
There are certain benefits which are associated with Frame Relay.

- It helps in reducing the cost of internetworking, as there is considerable reduction in the number of circuits required and the associated bandwidths.
- It helps in increasing the performance due to reduced network complexity.
- It increases the interoperability with the help of international standards.
- Frame Relay is protocol independent and can easily be used to combine traffic from other networking protocols.

In business scenarios, where there is a slow connection or continuous traffic flow due to applications like multimedia, Frame Relay is not a recommended choice.

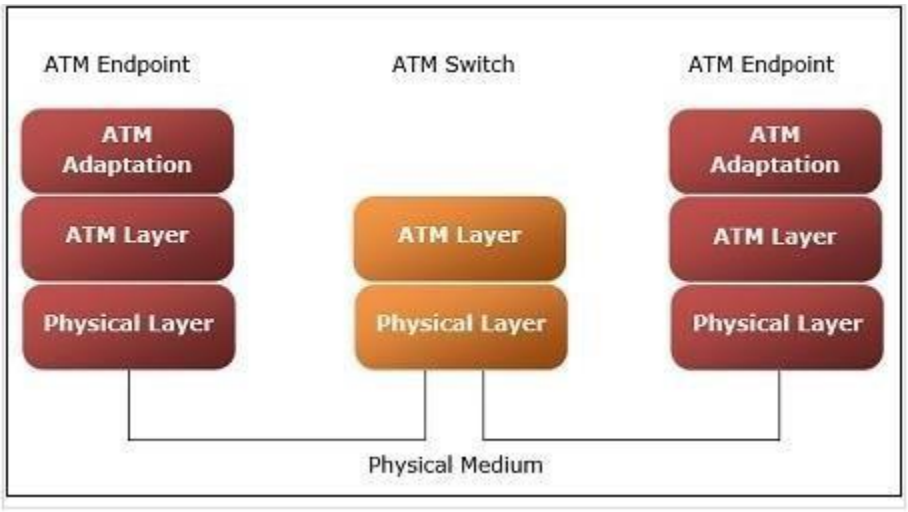
Overview of ATM:

Asynchronous transfer mode (ATM) is a switching technique used by telecommunication networks that uses asynchronous time-division multiplexing to encode data into small, fixed-sized cells.



ATM networks are connection-oriented networks that supports voice, video and data communications. It encodes data into small fixed - size cells so that they are suitable for TDM and transmits them over a physical medium.

The size of an ATM cell is 53 bytes: 5-byte header and 48-byte payload.



Physical Layer − This layer corresponds to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium.

ATM Layer −This layer is comparable to data link layer of OSI model. It accepts the 48-byte segments from the upper layer, adds a 5-byte header to each segment and converts into 53-byte cells. This layer is responsible for routing of each cell, traffic management, multiplexing and switching.

ATM Adaptation Layer −This layer corresponds to network layer of OSI model. It provides facilities to the existing packet switched networks to connect to ATM network and use its services. It accepts the data and converts them into fixed sized segments.

Benefits of ATM Networks are

- It provides the dynamic bandwidth that is particularly suited for bursty traffic.

- Since all data are encoded into identical cells, data transmission is simple, uniform and predictable.
- Uniform packet size ensures that mixed traffic is handled efficiently.
- Small sized header reduces packet overload, thus ensuring effective bandwidth usage.
- ATM networks are scalable both in size and speed.

Data Link Layer Protocols (DLL):

Data Link Layer protocols are generally responsible to simply ensure and confirm that the bits and bytes that are received are identical to the bits and bytes being transferred. It is basically a set of specifications that are used for implementation of data link layer just above the physical layer of the OSI Model.

High-Level Data Link Protocol (HDLC):

HDLC is basically a protocol that is now assumed to be an umbrella under which many Wide Area protocols reside. It is used to connect all of the remote devices to mainframe computers at central locations may be in point-to-point or multipoint connections. It is also used to make sure that the data units should arrive correctly and with right flow from one network point to next network point. It also provides best- effort unreliable service and also reliable service. HDLC is a bit-oriented protocol that is applicable for point-to-point and multipoint communications both.

Point to Point Protocol (PPP):

PPP is a protocol that is basically used to provide functionality to add a framing byte at end of IP packet. It is basically a data link control facility that is required for transferring IP packets usually among Internet Service Providers (ISP) and a home user. It is most robust protocol that is used to transport other types of packets also along with IP Packets. It is a byte-oriented protocol that is also used for error detection.

Difference Between High-level Data Link Control (HDLC) and Point-to-Point Protocol (PPP):

The main difference between High-level Data Link Control (HDLC) and Point-to-Point Protocol (PPP) is that High-level Data Link Control is the bit-oriented protocol, on the other hand, Point-to-Point Protocol is the byte-oriented protocol.

Another difference between HDLC and PPP is that HDLC is implemented by Point-to-point configuration and also multi-point configurations on the other hand While PPP is implemented by Point-to-Point configuration only.

S.NO	HDLC	PPP
1.	HDLC stands for High-level Data Link Control.	PPP stands for Point-to-Point Protocol.
2.	HDLC is a bit oriented protocol.	PPP is a byte oriented protocol.
3.	HDLC is implemented by Point-to-point configuration and also multi-point configurations.	PPP is implemented by Point-to-Point configuration only.
4.	Dynamic addressing is not offered by HDLC.	While in this Dynamic addressing is offered.
5.	HDLC is used in synchronous media.	PPP is used in synchronous media as well as asynchronous media.
6.	HDLC is not compatible with non-Cisco devices.	PPP is compatible with non-Cisco devices.
7.	HDLC does not provide link authentication.	While PPP provide link authentication using various protocols.
8.	HDLC is more costly comparatively.	While PPP is comparatively less costly.

Unit 3: Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links) i.e., it ensures that each packet gets from its point of origin to its final destination. The network layer is considered the backbone of the OSI Model. It selects and manages the best logical path for data transfer between nodes. The routing information contained within a packet includes the source of the sending host and the eventual destination of the remote host. This information is contained within the network layer header that encapsulates network frames at the data link layer. The primary function of the network layer is to permit different networks to be interconnected. It does this by forwarding packets to network routers, which rely on algorithms to determine the best paths for the data to travel. The network layer can support either connection-oriented or connectionless networks, but such a network can only be of one type and not both.

Internet Protocol:

The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

IP Address:

An Internet Protocol address (IP address) is a logical numeric address that is assigned to every single computer, printer, switch, router or any other device that is part of a TCP/IP-based network. The IP address is the core component on which the networking architecture is built; no network exists without it. An IP address is a logical address that is used to uniquely identify every node in the network. Because IP addresses are logical, they can change. They are similar to addresses in a town or city because the IP address gives the network node an address so that it can communicate with other nodes or networks.

The numerals in an IP address are divided into 2 parts:

- The network part specifies which networks this address belongs to and
- The host part further pinpoints the exact location.

IPv4:

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device to the internet. If a device operating in the network layer has m connections, then it needs to have m addresses. Router is such type of device.

An IPV4 address consists of 4 bytes in the form a.b.c.d (E.g. 173.14.2.225, 11.12.13.3). It can be logically divided into a network and a host portion. While the network portion identifies the network to which the

end node belongs to, the host portion uniquely identifies the end node, from the other end nodes, inside the network.

Binary Format	**Dotted Decimal Notation**
11000000 10101000 00000011 00011000	192.168.3.24

IPv4 uses 32-bit addresses, which means that the address space is 2^{32} (more than 4 billion). This means that, theoretically, if there were no restrictions, more than 4 billion devices could be connected to the internet.

IPv4 ADDRESSING SCHEME

IP addresses falls into two types:

- Classful IP addressing is a legacy scheme which divides the whole IP address pools into 5 distinct classes—A, B, C, D and E.
- Classless IP addressing has an arbitrary length of the prefixes.

Classful Addressing

Class A

The first octet denotes the network address, and the last three octets are the host portion. Any IP address whose first octet is between 1 and 126 is a Class A address. Note that 0 is reserved as a part of the default address and 127 is reserved for internal loopback testing.

Format: network.host.host.host

Default subnet mask = 255.0.0.0 or (slash notation) /8

Class B

The first two octets denote the network address, and the last two octets are the host portion. Any address whose first octet is in the range 128 to 191 is a Class B address.

Format: network.network.host.host

Default subnet mask =255.255.0.0 or

/16 Class C

The first three octets denote the network address, and the last octet is the host portion. The first octet range of 192 to 223 is a Class C address.

Format: network.network.network.host

Default subnet mask = 255.255.255.0 or

/24 Class D

Used for multicast. Multicast IP addresses have their first octets in the range 224 to 239.

Class E

Reserved for future use or research purpose and includes the range of addresses with a first octet from 240 to 255.

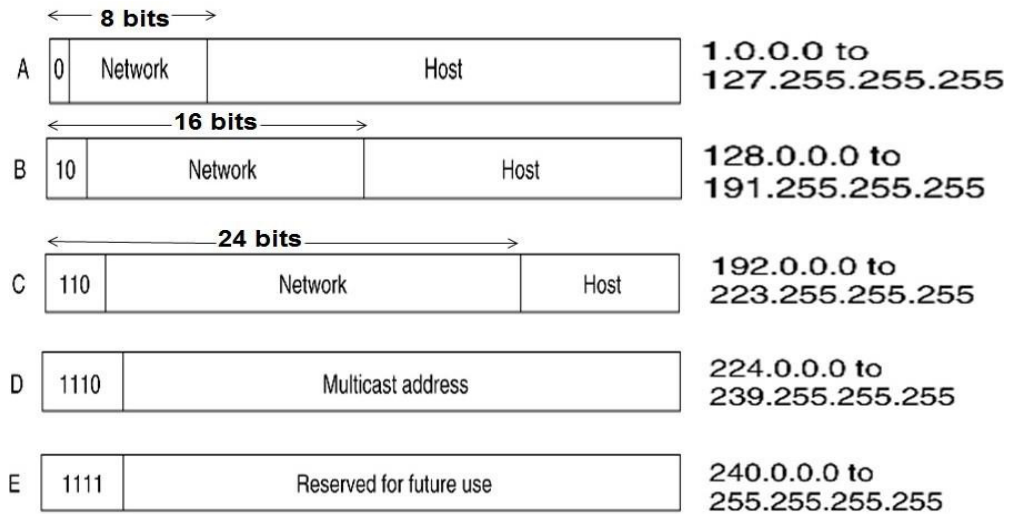


Figure 19.2 *Finding the classes in binary and dotted-decimal notation*

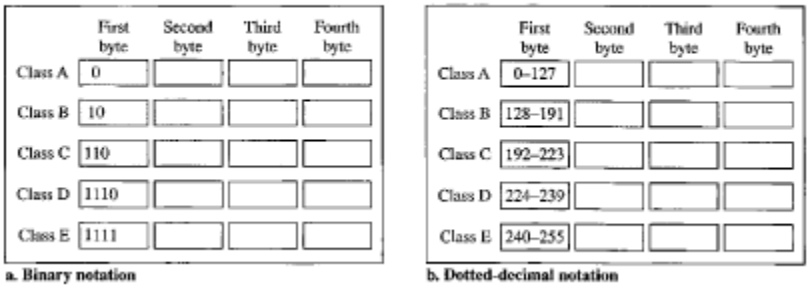


Table 19.1 *Number of blocks and block size in classful IPv4 addressing*

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Netid and Hostid

In classful addressing, an IP address in class A, B, or C is divided into **netid** and **hostid.** These parts are of varying lengths, depending on the class of the address. Figure 19.2 shows some netid and hostid bytes. The netid is in color, the hostid is in white. Note that the concept does not apply to classes D and E.

In class A, one byte defines the netid and three bytes define the hostid. In class B, two bytes define the netid and two bytes define the hostid. In class C, three bytes define the netid and one byte defines the hostid.

Mask

Although the length of the netid and hostid (in bits) is predetermined in classful addressing, we can also use a **mask** (also called the **default mask**), a 32-bit number made of

contiguous 1s followed by contiguous 0s. The masks for classes A, B, and C are shown in Table 19.2. The concept does not apply to classes D and E.

Table 19.2 *Default masks for classful addressing*

Class	*Binary*	*Dotted-Decimal*	*CIDR*
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

The mask can help us to find the netid and the hostid. For example, the mask for a class A address has eight 1s, which means the first 8 bits of any address in class A define the netid; the next 24 bits define the hostid.

The last column of Table 19.2 shows the mask in the form */n* where *n* can be 8, 16, or 24 in classful addressing. This notation is also called slash notation or **Classless Interdomain Routing (CIDR)** notation. The notation is used in classless addressing, which we will discuss later. We introduce it here because it can also be applied to classful addressing. We will show later that classful addressing is a special case of classless addressing.

Subnetting

During the era of classful addressing, **subnetting** was introduced. If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called **subnets**) or, in rare cases, share part of the addresses with neighbors. Subnetting increases the number of 1s in the mask, as we will see later when we discuss classless addressing.

Supernetting

The time came when most of the class A and class B addresses were depleted; however, there was still a huge demand for midsize blocks. The size of a class C block with a maximum number of 256 addresses did not satisfy the needs of most organizations. Even a midsize organization needed more addresses. One solution was **supernetting.** In supernetting, an organization can combine several class C blocks to create a larger range of addresses. In other words, several networks are combined to create a supernetwork or a **supernet.** An organization can apply for a set of class C blocks instead of just one. For example, an organization that needs 1000 addresses can be granted four contiguous class C blocks. The organization can then use these addresses to create one supernetwork. Supernetting decreases the number of 1s in the mask. For example, if an organization is given four class C addresses, the mask changes from /24 to /22. We will see that classless addressing eliminated the need for supernetting.

Address Depletion

The flaws in classful addressing scheme combined with the fast growth of the Internet led to the near depletion of the available addresses. Yet the number of devices on the Internet is much less than the 2^{32} address space. We have run out of class A and B addresses, and

a class C block is too small for most midsize organizations. One solution that has alleviated the problem is the idea of classless addressing.

Classful addressing, which is almost obsolete, is replaced with classless addressing.

Classless IP addresses

Classful IP addresses is no longer popular and instead has been replaced with the concept of classless IP address, where there is no concept of IP address classes and no strict network and host boundaries. In classless IP addressing, there is no concept of Classful addressing like Classes A, B, C, D and E. IPv4 address range 0.0.0.0 to 223.255.255.255 treated as a single class. No strict 8-byte boundaries for the network and host portions. A Subnet masks defines network & host boundaries. This approach is very useful for optimizing address usage.

Examples of Classless Addressing

Network address – 22.10.0.0 /16

Network address – 173.2.224.0 /

In the above address, 16 and 21 denote the subnet masks respectively. This means that in the first address 22.10.0.0, the first 16 bits are reserved for the network portion and the rest of the 16 bits are reserved for the host portion. Similarly, in the second address 173.2.224.0/21, the first 21 bits are reserved for the network portion and the remaining 13 bits are reserved for the host portion. Thus, it can be seen that classless addressing gives a flexible boundary between the network and host portions, thereby allowing lot of flexibility in partitioning the networks.

Subnetting:

Subnetting is the practice of dividing a network into two or more smaller networks. The major advantage of subnetting is to reduce the address wastage. It increases routing efficiency, enhances the security of the network and reduces the size of the broadcast domain.

The reasons to use subnetting are:

- Conservation of IP addresses
- Reduced network traffic
- Simplified troubleshooting

FLSM vs VLSM:

FLSM stands for Full Length Subnet Mask. It means all the subnets are of the same size. In FLSM, the subnet mask remains the same for all the subnets.

VLSM stands for Variable Length Subnet Mask. It means the size of the subnet varies according to the needs. In VLSM, the subnet mask is different normally but it can be same for any two or more subnets depending upon the situation.

Internet Service Providers may face a situation where they need to allocate IP subnets of different sizes as per the requirement of customer. One customer may ask Class C subnet of 3 IP addresses and another may ask for 100 IPs. For an ISP, it is not feasible to divide the IP addresses into fixed size subnets, rather he may want to subnet the subnets in such a way which results in minimum wastage of IP addresses.

For example, an administrator has 192.168.1.0/24 network. The suffix /24 (pronounced as "slash 24") tells the number of bits used for network address. In this example, the administrator has three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers. In CIDR, the subnets are of fixed size. Using the same methodology, the administrator cannot fulfill all the requirements of the network.

The following procedure shows how VLSM can be used in order to allocate department-wise IP addresses as mentioned in the example.

Step 1: Make a list of Subnets possible.

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Step 2: Sort the requirements of IPs in descending order (Highest to Lowest).

Sales 100

Purchase 50

Accounts 25

Management 5

Step 3: Allocate the highest range of IPs to the highest requirement, so let's assign 192.168.1.0 /25 (255.255.255.128) to the Sales department. This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses which satisfy the requirement of the Sales department. The subnet mask used for this subnet has 10000000 as the last octet.

Step 4: Allocate the next highest range, so let's assign 192.168.1.128 /26 (255.255.255.192) to the Purchase department. This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses which can be easily assigned to all the PCs of the Purchase department. The subnet mask used has 11000000 in the last octet.

Step 5: Allocate the next highest range, i.e. Accounts. The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs. The network number of Accounts department will be 192.168.1.192. The last octet of subnet mask is 11100000.

Step 6: Allocate the next highest range to Management. The Management department contains only 5 computers. The subnet 192.168.1.224 /29 with the Mask 255.255.255.248 has exactly 6 valid host IP

addresses. So, this can be assigned to Management. The last octet of the subnet mask will contain 11111000.

By using VLSM, the administrator can subnet the IP subnet in such a way that least number of IP addresses are wasted. Even after assigning IPs to every department, the administrator, in this example, is still left with plenty of IP addresses which was not possible if he has used FLSM.

Numerically, we can show the VLSM subnetting process as:

The given network address is: 192.168.1.0/24

Given requirement in descending order is:

Sales 100

Purchase 50

Accounts 25

Management 5

The complete range of the address in the above provided network is:

192.168.1.0 to 192.168.1.255

Divide the given network consisting 256 hosts into 2 networks with 128 hosts

each: 192.168.1.0-192.168.1.127 (192.168.1.0/25)

192.168.1.128-192.168.1.255 (192.168.1.128/25)

The largest network requirement is of 100 hosts for Sales department. For this, we need to assign subnetwork with 128 hosts.

Let us assign the first divided subnetwork 192.168.1.0/25 to Sales Department.

We now have remaining subnetwork 192.168.1.128/25.

Dividing this subnetwork, two subnetworks with 64 hosts each are

formed. 192.168.1.128 to 192.168.1.191 (192.168.1.128/26)

192.168.1.192 to 192.168.1.255 (192.168.1.192/26)

Our second network requirement is of 50 hosts for Purchase department. We need to assign subnetwork consisting of 64 hosts.

Assigning 192.168.1.128/26 to Purchase department.

The remaining subnetwork available is 192.168.192/26.

Dividing this subnetwork, two subnetworks with 32 hosts each are formed.

192.168.1.192 to 192.168.1.223 (192.168.1.192/27)

192.168.1.224 to 192.168.1.255 (192.168.1.224/27)

The third largest requirement is of 25 hosts for Account department.

Assigning 192.168.1.192/27 to Account Department.

Remaining subnetwork is 192.168.1.224/27

Dividing this subnetwork, two subnetworks with 16 hosts each are

formed. 192.168.1.224 to 192.168.1.239 (192.168.1.224/28)

192.168.1.240 to 192.168.1.255 (192.168.1.240/28)

Our fourth network requirement is of 5 hosts for Management department. We need to assign subnetwork consisting of 8 hosts, which is sufficient.

So, again dividing the subnetwork 192.168.1.240/28, two subnetworks with 8 hosts each are

formed. 192.168.1.240 to 192.168.1.247 (192.168.1.240/29)

192.168.1.248 to 192.168.1.255 (192.168.1.248/29)

Our fourth network requirement is of 5 hosts for Management department. We need to assign subnetwork consisting of 8 hosts.

We can Assign either of the subnetwork to Management department.

Summarizing the subnetting results,

Network Name	**Network ID**	**Subnet mask**	**No. of usable hosts**	**Usable Host ID Range**	**Broadcast address**
Sales	192.168.1.0	/25	126	192.168.1.1 to 192.168.1.126	192.168.1.127
Purchase	192.168.1.128	/26	62	192.168.129 to 192.168.1.190	192.168.1.191
Account	192.168.1.192	/27	30	192.168.1.193 to 192.168.1.222	192.168.1.223
Management	192.168.1.240	/29	6	192.168.1.241 to 192.168.1.246	192.168.1.247
Unused	192.168.1.224/28 (192.168.1.224 to 192.168.1.239)				
Unused	192.168.1.247/29 (192.168.1.247 to 192.168.1.255)				

FLSM Numerical Example:

Q1. If you are given a network 210.25.23.0 with the subnet mask 255.255.255.0, assign the networks to four different departments with 50 hosts each.

Ans: The complete range of the address in the above provided network is:

210.25.23.0 to 210.25.23.255

Total no of hosts available: 256 hosts

Each subnetwork requires 50 usable hosts. So, we need to assign n/w with 64 hosts each to the four departments.

Since we are using FLSM, the divided networks will be of same size. The given network consists of 256 hosts which needs to be divided into four subnetworks with 64 hosts each.

The process is as follows:

First of all, divide the given network range into four equal parts.

210.25.23.0 to 210.25.23.63 (210.25.23.0/26)

210.25.23.64 to 210.25.23.127 (210.25.23.64/26)

210.25.23.128 to 210.25.23.191 (210.25.23.128/26)

210.25.23.192 to 210.25.23.255 (210.25.23.192/26)

Now, as per the requirement, there are four networks required and we can assign the above networks to each of the four departments.

Network Name	**Network ID**	**Subnet mask**	**No. of usable hosts**	**Usable Host ID Range**	**Broadcast address**
Dept 1	210.25.23.0	/26	62	210.25.23.1 to 210.25.23.62	210.25.23.63
Dept 2	210.25.23.64	/26	62	210.25.23.65 to 210.25.23.126	210.25.23.127
Dept 3	210.25.23.128	/26	62	210.25.23.129 to 210.25.23.190	210.25.23.191
Dept 4	210.25.23.192	/26	62	210.25.23.193 to 210.25.23.254	210.25.23.255

Q2. Suppose you are network administrator with provided network 172.16.0.0/24. You need to manage the entire n/w by dividing into subnetworks so that each of the Development, Sales, Reception, HR and Production. How would you do so?

Ans: Provided network: 172.16.0.0/24. Here, /24 indicates 256 hosts are contained in the given network.

There are five departments to address the networks with. So, we divide the given network into 8 networks. 256/8 = 32

Each of the 8 subnetworks will contain 32 hosts each. The divided networks will be:

172.16.0.0 to 172.16.0.31 (172.16.0.0/27)

172.16.0.32 to 172.16.0.63 (172.16.0.32/27)

172.16.0.64 to 172.16.0.95 (172.16.0.64/27)

172.16.0.96 to 172.168.0.127 (172.16.0.96/27)

172.16.0.128 to 172.16.0.159 (172.16.0.128/27)

172.16.0.160 to 172.16.0.191 (172.16.0.160/27)

172.16.0.192 to 172.16.0.223 (172.16.0.192/27)

172.16.0.224 to 172.16.0.255) (172.16.0.224/27)

Now, we can assign 5 of the above 8 subnetworks to the departments of our requirement.

The result will be as follows:

Network Name	**Network ID**	**Subnet mask**	**No. of usable hosts**	**Usable Host ID Range**	**Broadcast address**
Development	172.16.0.0	/27	30	172.16.0.1 to 172.16.0.30	172.16.0.31
Sales	172.16.0.32	/27	30	172.16.0.33 to 172.16.0.62	172.16.0.63
Reception	172.16.0.64	/27	30	172.16.0.65 to 172.16.0.94	172.16.0.95
HR	172.16.0.96	/27	30	172.16.0.97 to 172.168.0.126	172.168.0.127
Production	172.16.0.128	/27	30	172.16.0.129 to 172.16.0.158	172.16.0.159
Unused	172.16.0.160 to 172.16.0.191 (172.16.0.160/27)				
Unused	172.16.0.192 to 172.16.0.223 (172.16.0.192/27)				
Unused	172.16.0.224 to 172.16.0.255) (172.16.0.224/27)				

VLSM Numerical Example:

Q. If you are assigned an IP address 92.16.1.0/24 and plans to deploy CIDR. Here are some requirements which you have to fulfill for Subnet A= 120 hosts, Subnet B=60 hosts, Subnet C=30 hosts, Subnet D= 10 hosts, Subnet E= 5. You are also required to calculate subnet mask, range, netid, broadcast id for each subnet.

Ans: The given network address is: 92.16.1.0/24

Given requirement in descending order is:

Subnet A: 120

Subnet B: 60

Subnet C: 30

Subnet D: 10

Subnet E: 5

The complete range of the address in the above provided network is:

92.16.1.0 to 92.16.1.255

The largest network requirement is of 120 hosts for Subnet A. For this, we need to assign subnetwork with 128 hosts.

Divide the given network consisting 256 hosts into 2 networks with 128 hosts

each: 92.16.1.0-92.16.1.127 (92.16.1.0/25)

92.16.1.128-92.16.1.255 (92.16.1.128/25)

Let us assign the first divided subnetwork 92.16.1.0/25 to Subnet A.

We now have remaining subnetwork 92.16.1.128/25.

Our second network requirement is of 60 hosts for Subnet B. We need to assign subnetwork consisting of 64 hosts.

Dividing this subnetwork, two subnetworks with 64 hosts each are formed.

92.16.1.128 to 92.16.1.191 (92.16.1.128/26)

92.16.1.192 to 92.16.1.255 (92.16.1.192/26)

Assigning 92.16.1.128/26 to Subnet B.

The remaining subnetwork available is 92.16.1.192/26.

The third largest requirement is of 30 hosts for Subnet

C.

Dividing this subnetwork, two subnetworks with 32 hosts each are formed.

92.16.1.192 to 92.16.1.223 (92.16.1.192/27)

92.16.1.224 to 92.16.1.255 (92.16.1.224/27)

Assigning 92.16.1.192/27 to Subnet C.

Remaining subnetwork is 92.16.1.224/27

Our fourth network requirement is of 10 hosts for Subnet D. We need to assign subnetwork consisting of 16 hosts.

Dividing this subnetwork, two subnetworks with 16 hosts each are

formed. 92.16.1.224 to 92.16.1.239 (92.16.1.224/28)

92.16.1.240 to 92.16.1.255 (92.16.1.240/28)

Assigning 92.16.1.224/28 to Subnet D.

Remaining subnetwork is

92.16.1.240/28

Our fifth network requirement is of 5 hosts for Subnet E. We need to assign subnetwork consisting of 8 hosts.

So, again dividing the subnetwork 92.16.1.240/28, two subnetworks with 8 hosts each are

formed. 92.16.1.240 to 92.16.1.247 (92.16.1.240/29)

92.16.1.248 to 92.16.1.255 (92.16.1.248/29)

We can Assign either of the subnetwork to Subnet E. Let us assign 92.16.1.240/29 to Subnet E.

Summarizing the subnetting results,

Network Name	**Network ID**	**Subnet mask**	**No. of usable hosts**	**Usable Host ID Range**	**Broadcast address**
Subnet A	92.16.1.0	/25	126	92.16.1.1 to 92.16.1.126	92.16.1.127
Subnet B	92.16.1.128	/26	62	92.16.129 to 92.16.1.190	92.16.1.191
Subnet C	92.16.1.192	/27	30	92.16.1.193 to 92.16.1.222	92.16.1.223
Subnet D	92.16.1.224	/28	14	92.16.1.225 to 92.16.1.238	92.16.1.239
Subnet E	92.16.1.240	/29	6	92.16.1.241 to 92.16.1.246	92.16.1.247
Unused	92.16.1.248/29 (92.16.1.248 to 92.16.1.255)				

Note:

1. Network: 192.168.0.0/24, 2^8, 256 hosts

   Total Range: 192.168.0.0 to 192.168.0.255

2. Network: 192.168.1.0/25, 2^7, 128 hosts
   Total Range: 192.168.1.0 to 192.168.1.127

3. Network: 192.168.3.0/26, 2^6, 64 hosts
   Total Range: 192.168.3.0 to 192.168.3.63

4. Network: 192.168.0.0/23, 2^9, 512 hosts
   Total Range: 192.168.0.0 to 192.168.0.255, 192.168.1.0 to 192.168.1.255

5. Network: 192.168.1.0/23, 2^9, 512 hosts
   Total Range: 192.168.1.0 to 192.168.1.255, 192.168.2.0 to 192.168.2.255

6. Network: 172.16.10.0/23, 2^9, 512 hosts
   Total Range: 172.16.10.0 to 172.16.10.255, 172.16.11.0 to 172.168.11.255

7. Network: 172.16.10.0/22, 2^10, 1024 hosts
   Total Range: 172.16.10.0 to 172.16.10.255
   172.16.11.0 to 172.16.11.255
   172.16.12.0 to 172.16.12.255
   172.16.13.0 to 172.16.13.255

8. Network: 172.16.10.0/21, 2^11, 2048 hosts
   Total Range: 172.16.10.0 to 172.16.10.255
   172.16.11.0 to 172.16.11.255
   172.16.12.0 to 172.16.12.255
   172.16.13.0 to 172.16.13.255
   172.16.14.0 to 172.16.14.255
   172.16.15.0 to 172.16.15.255
   172.16.16.0 to 172.16.16.255
   172.16.17.0 to 172.16.17.255

Q2. Given Network: 192.168.0.0/23

Requirement:

A: 128 hosts, B: 64 hosts, C: 31 hosts, D: 15 hosts

Solution: Total Range= 192.168.0.0 to 192.168.0.255 (192.168.0.0/24)

192.168.1.0 to 192.168.1.255 (192.168.1.0/24)

A-> 128 hosts, need to assign n/w of 256 hosts

Let us assign: 192.168.0.0/24

B-> 64 hosts, need to assign n/w of 128 hosts

Divide 192.168.1.0/24,

192.168.1.0 to 192.168.1.127 (192.168.1.0/25)

192.168.1.128 to 192.168.1.255 (192.168.1.128/25)

Assign 192.168.1.0/25 to B.

Remaining:

192.168.1.128/25

C->31 hosts, need to assign n/w of 64 hosts

Divide 192.168.1.128/25,

192.168.1.128 to 192.168.1.191 (192.168.1.128/26)

192.168.1.192 to 192.168.1.255 (192.168.1.192/26)

Assign 192.168.1.128/26 to

C. Remaining:

192.168.1.192/26

D-> 15 hosts, need to assign n/w of 32 hosts

Divide 192.168.1.192/26,

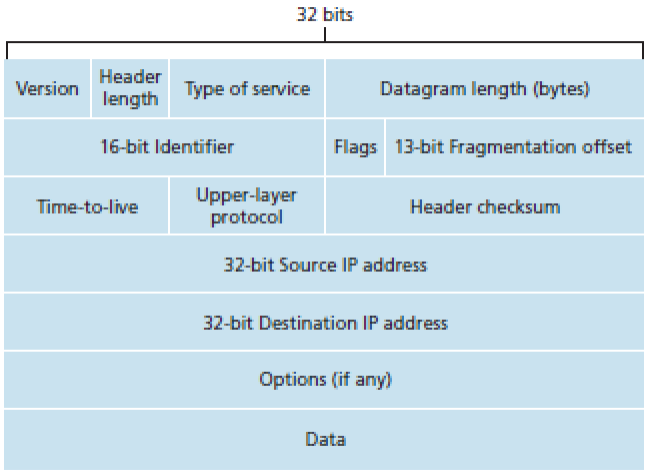
192.168.1.192 to 192.168.1.223 (192.168.1.192/27)

192.168.1.224 to 192.168.1.255 (192.168.1.224/27)

Assign 192.168.1.192/27 to D

Unused: 192.168.1.224/27

IPv4 Header Format:



The key fields in the IPv4 datagram are the following:

- Version number. These 4 bits specify the IP protocol version of the datagram. By looking at the version number, the router can determine how to interpret the remainder of the IP datagram. Different versions of IP use different datagram formats. The datagram format for the current version of IP, IPv4, is shown in Figure.
- Header length. Because an IPv4 datagram can contain a variable number of options (which are included in the IPv4 datagram header), these 4 bits are needed to determine where in the IP datagram the data actually begins. Most IP datagrams do not contain options, so the typical IP datagram has a 20-byte header.
- Type of service. The type of service (TOS) bits were included in the IPv4 header to allow different types of IP datagrams (for example, datagrams particularly requiring low delay, high throughput, or reliability) to be distinguished from each other. For example, it might be useful to distinguish real-time datagrams (such as those used by an IP telephony application) from non-real-time traffic (for example, FTP). The specific level of service to be provided is a policy issue determined by the router's administrator.
- Datagram length. This is the total length of the IP datagram (header plus data), measured in bytes. Since this field is 16 bits long, the theoretical maximum size of the IP datagram is 65,535 bytes. However, datagrams are rarely larger than 1,500 bytes.
- Identifier, flags, fragmentation offset. These three fields have to do with so-called IP fragmentation. Interestingly, the new version of IP, IPv6, does not allow for fragmentation at routers.
- Time-to-live. The time-to-live (TTL) field is included to ensure that datagrams do not circulate forever (due to, for example, a long-lived routing loop) in the network. This field is decremented by one each time the datagram is processed by a router. If the TTL field reaches 0, the datagram must be dropped.
- Protocol. This field is used only when an IP datagram reaches its final destination. The value of this field indicates the specific transport-layer protocol to which the data portion of this IP datagram should be passed. For example, a value of 6 indicates that the data portion is passed to

TCP, while a value of 17 indicates that the data is passed to UDP. Note that the protocol number in the IP datagram has a role that is analogous to the role of the port number field in the transport layer segment. The protocol number is the glue that binds the network and transport layers together, whereas the port number is the glue that binds the transport and application layers together. The link-layer frame also has a special field that binds the link layer to the network layer.

- Header checksum. The header checksum aids a router in detecting bit errors in a received IP datagram. The header checksum is computed by treating each 2 bytes in the header as a number and summing these numbers using 1s complement arithmetic. The 1s complement of this sum, known as the Internet checksum, is stored in the checksum field. A router computes the header checksum for each received IP datagram and detects an error condition if the checksum carried in the datagram header does not equal the computed checksum. Routers typically discard datagrams for which an error has been detected. Note that the checksum must be recomputed and stored again at each router, as the TTL field, and possibly the options field as well, may change.
- Source and destination IP addresses. When a source creates a datagram, it inserts its IP address into the source IP address field and inserts the address of the ultimate destination into the destination IP address field. Often the source host determines the destination address via a DNS lookup.
- Options. The options fields allow an IP header to be extended. Header options were meant to be used rarely—hence the decision to save overhead by not including the information in options fields in every datagram header. However, the mere existence of options does complicate matters—since datagram headers can be of variable length, one cannot determine a priori where the data field will start. Also, since some datagrams may require options processing and others may not, the amount of time needed to process an IP datagram at a router can vary greatly. These considerations become particularly important for IP processing in high-performance routers and hosts. For these reasons and others, IP options were dropped in the IPv6 header.
- Data (payload). Finally, we come to the last and most important field—the raison d'être for the datagram in the first place! In most circumstances, the data field of the IP datagram contains the transport-layer segment (TCP or UDP) to be delivered to the destination. However, the data field can carry other types of data, such as ICMP messages.

Issues with IPv4:

Changes since IPv4 was developed (mid 70's)

- Provider market has changed dramatically
- Immense increase in user and traffic on the Internet
- Rapid technology advancement
- Bandwidth increase from kb/s to

Tb/s IPv4 issues: The major issues in IPv4 are

- Deficiency of address space - The devices connected to the Internet grows exponentially. The size of address space 2^32 is quickly exhausted;
- Too large routing tables

Some more issues are:

- Weak expansibility of the protocol - the insufficient size of heading IPv4 doesn't allow to place demanded quantity of additional parameters in it;
- Problem of safety of communications - it is not stipulated any means for differentiation of access to the information placed in a network;
- Absence of support of quality of service (QoS) - accommodation of the information about throughput, the delays and demanded for normal work of some network appendices is not supported;
- The problems connected with the mechanism of a fragmentation - the size of the maximal block of data transmission on each concrete way is not defined;
- Absence of the auto-configuration IP addresses mechanism.

Overview of IPv6:

To respond to the need for a large IP address space, a new IP protocol, IPv6, was developed. Also, major issues of IPv4 are addressed in this version.

The most important changes introduced in IPv6 are evident in the datagram format:

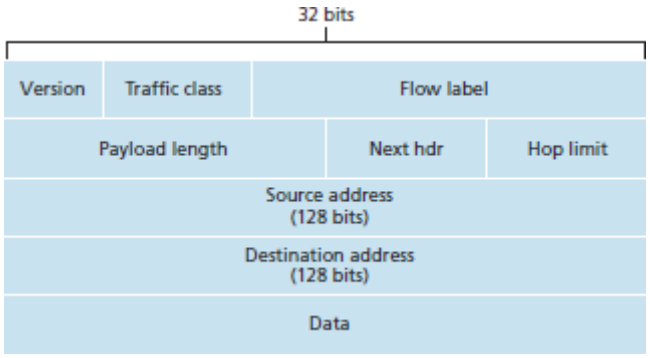
- *Expanded addressing capabilities.* IPv6 increases the size of the IP address from 32 to 128 bits. This ensures that the world won't run out of IP addresses. Now, every grain of sand on the planet can be IP-addressable. In addition to unicast and multicast addresses, IPv6 has introduced a new type of address, called an **any-cast address**, which allows a datagram to be delivered to any one of a group of hosts.
- *A streamlined 40-byte header.* As discussed below, a number of IPv4 fields have been dropped or made optional. The resulting 40-byte fixed-length header allows for faster processing of the IP datagram. A new encoding of options allows for more flexible options processing.
- *Flow labeling and priority.* IPv6 has an elusive definition of a flow. This allows "labeling of packets belonging to particular flows for which the sender requests special handling, such as a non-default quality of service or real-time service." For example, audio and video transmission might likely be treated as a flow.

IPv6 Simplifications:

- Remove header checksum: Because the transport-layer (for example, TCP and UDP) and link-layer (for example, Ethernet) protocols in the Internet layers perform check summing, the designers of IP probably felt that this functionality was sufficiently redundant in the network layer that it could be removed.
- Remove hop-by-hop segmentation: IPv6 does not allow for fragmentation and reassembly at intermediate routers; these operations can be performed only by the source and destination. If an IPv6 datagram received by a router is too large to be forwarded over the outgoing link, the router simply drops the datagram and sends a "Packet Too Big" ICMP error message back to the sender.

- Options. An options field is no longer a part of the standard IP header. However, it has not gone away. Instead, the options field is one of the possible next headers pointed to from within the IPv6 header. The removal of the options field results in a fixed-length, 40-byte IP header.

IPv6 Header:



S.N.	Field & Description
1	Version (4-bits): It represents the version of Internet Protocol, i.e. 0110
2	Traffic Class (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router know what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3	Flow Label (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information.
4	Payload Length (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data.
5	Next Header (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present, then it indicates the Upper Layer PDU.

6	Hop Limit (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0, the packet is discarded.
7	Source Address (128-bits): This field indicates the address of originator of the packet.
8	Destination Address (128-bits): This field provides the address of intended recipient of the packet.

IPv6 Addresses :(IPv6 Format)

IPv6 address is 128 bits long and is arranged in eight groups, each of which is 16 bits. Each group is expressed as four hexadecimal digits and the groups are separated by colons.

An example of a full IPv6 address: FE80:CD00: 0000:0CDE: 1257:0000:211E:729C

IPv6 has three address categories:

- Unicast - identifies exactly one interface
- Multicast - identifies a group; packets get delivered to all members of the group
- Anycast - identifies a group; packets normally get delivered to nearest member of the group

IPv6 Address Abbreviations and CIDR:

Even after converting into Hexadecimal format, IPv6 address remains long. An IPv6 address may be abbreviated to shorter notations by application of the following rules:

Rule 1: Discard leading zero (es)

That address can be shortened because the addressing scheme allows the omission of any leading zero, as well as any sequences consisting only of zeroes.

E.g.: FE80:CD00:0000:0CDE:1257:0000:211E:729C

Here's the short version:

FE80:CD00:0:CDE:1257:0:211E:729C

Rule 2: If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign **::**

2001:0000:3238:DFE1:63:0000:0000:FEFB

can be written as

2001:0000:3238:DFE1:63::FEFB

The IPv6 addressing architecture allows you use the two-colon (::) notation to represent contiguous 16-bit fields of zeros.

CIDR Notation is similar to IPv4 addresses, IPv6 addresses consist of NetworkID + HostID, and use classless notation to identify (distinguish between) the two. Network ID is also referred to as prefix, and the number of bits allocated to Network ID as prefix length. Information on the prefix is provided together with each IPv6 address as a slash (/) at the end of the address followed by the prefix length.

For example, the site prefix of the IPv6 address 2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48 is contained in the leftmost 48 bits, 2001:db8:3c4d. You use the following representation, with zeros compressed, to represent this prefix: 2001:db8:3c4d::/48

IPv6 vs IPv4:

IPv4	**IPv6**
IPv4 addresses are 32 bit length.	IPv6 addresses are 128 bit length.
IPv4 addresses are binary numbers represented in decimals.	IPv6 addresses are binary numbers represented in hexadecimals.
IPSec support is only optional.	Inbuilt IPSec support.
Fragmentation is done by sender and forwarding routers.	Fragmentation is done only by sender.
No packet flow identification	Packet flow identification is available within the IPv6 header using the Flow Label field.
Checksum field is available in IPv4 header	No checksum field in IPv6 header
Options fields are available in IPv4 header	No option fields, but IPv6 Extension headers are available.

Transition from IPv4 to IPv6:

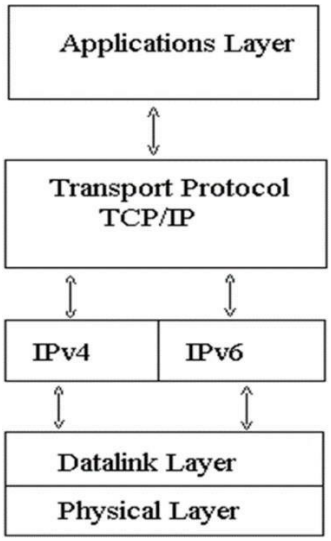
Because of the huge number of systems on the internet, the transition from IPv4 to IPv6 cannot happen suddenly. The transition must be smooth to prevent any problems between IPv4 and IPv6 systems.

Three strategies have been devised to help the transition:

- Dual stack
- Tunneling
- Header translation

Dual Stack:

Dual-stack transition mechanism enables to run both IP stacks (IPv4 and IPv6) in a single node. Maintains both IP protocol stacks that operates parallel and thus allow the end node to use either protocols. Node is capable of handling both kinds of IP (IPv4&IPv6) routing. Flow or routing decisions in the node are based on IP header version's field. Both IPv4 and IPv6 shares common transport layer protocols such as TCP/IP. Many of client and server operating systems provide dual IP protocol stacks. For example: Windows 7, 8, Linux



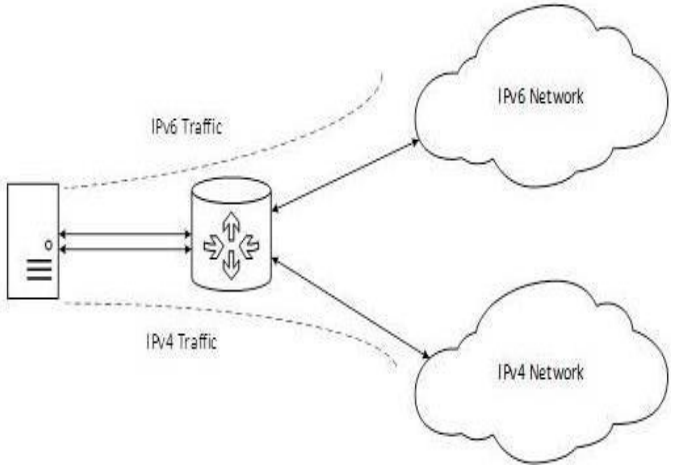


Fig: Dual Stack Router

Fig: Dual stack TCP/IP model

The Dual Stack Router, can communicate with both the networks. It provides a medium for the hosts to access a server without changing their respective IP versions.

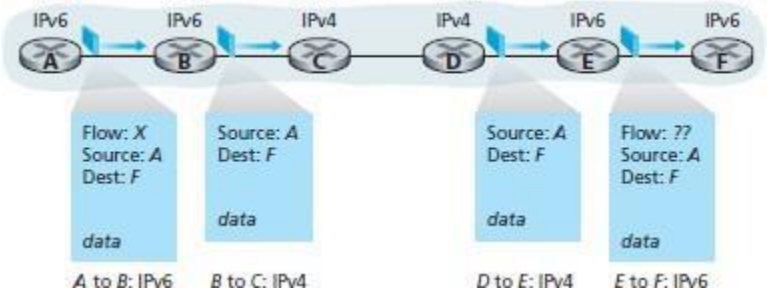
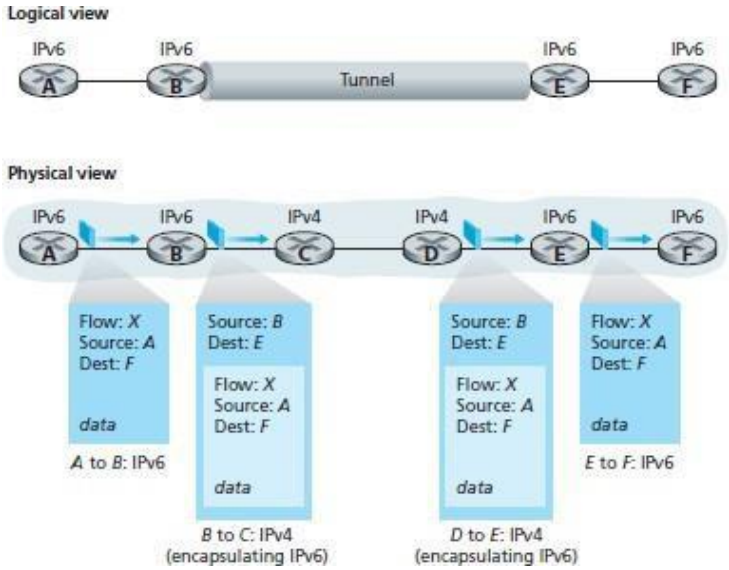


Fig: A dual-stack approach

In the dual-stack approach, if either the sender or the receiver is only IPv4-capable, an IPv4 datagram must be used. As a result, it is possible that two IPv6-capable nodes can end up, in essence, sending IPv4 datagrams to each other. Suppose Node A is IPv6-capable and wants to send an IP datagram to Node F, which is also IPv6-capable. Nodes A and B can exchange an IPv6 datagram. However, Node B must create an IPv4 datagram to send to C. Certainly, the data field of the IPv6 datagram can be copied into the data field of the IPv4 datagram and appropriate address mapping can be done. However, in performing the conversion from IPv6 to IPv4, there will be IPv6-specific fields in the IPv6 datagram (for example, the flow identifier field) that have no counterpart in IPv4. The information in these fields will be lost. Thus, even though E and F can exchange IPv6 datagrams, the arriving IPv4 datagrams at E from D do not contain all of the fields that were in the original IPv6 datagram sent from A.

Tunneling:

Tunneling is a strategy used when two computers using IPv4 want to communicate with each other and the packet must pass through a region that uses IPv6. To pass through this region, the packet must have an IPv6 address. So the IPv4 packet is encapsulated in an IPv6 packet when it enters the region, and it leaves its capsule when it exits the region. Seems as if the IPv4 packet goes through a tunnel at one end and emerges at the other end.

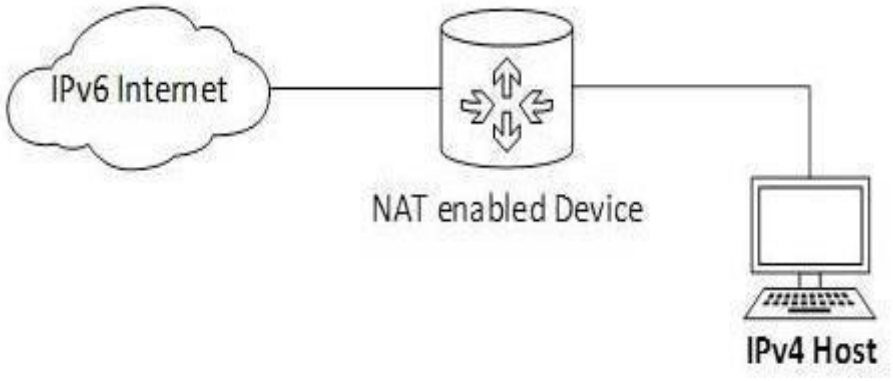


An alternative to the dual-stack approach is known as tunneling. Tunneling can solve the problem noted above, allowing, for example, E to receive the IPv6 datagram originated by A. The basic idea behind tunneling is the following. Suppose two IPv6 nodes (for example, B and E in Figure) want to interoperate using IPv6 datagrams but are connected to each other by intervening IPv4 routers. We refer to the intervening set of IPv4 routers between two IPv6 routers as a tunnel, as illustrated in Figure. With tunneling, the IPv6 node on the sending side of the tunnel (for example, B) takes the entire IPv6 datagram and puts it in the data (payload) field of an IPv4 datagram. This IPv4 datagram is then addressed to the IPv6 node on the receiving side of the tunnel (for example, E) and sent to the first node in the tunnel (for example, C). The intervening IPv4 routers in the tunnel route this IPv4 datagram among themselves, just as they would any other datagram, blissfully unaware that the IPv4 datagram itself contains a complete IPv6 datagram. The IPv6 node on the receiving side of the tunnel eventually receives the IPv4 datagram

(it is the destination of the IPv4 datagram!), determines that the IPv4 datagram contains an IPv6 datagram, extracts the IPv6 datagram, and then routes the IPv6 datagram exactly as it would if it had received the IPv6 datagram from a directly connected IPv6 neighbor.

Header Translation:

Translation mechanism refers the direct conversion of IP protocols. May include transformation of both IPv4 and IPv6 protocol's header and payload according to their IP specifications. Translation mechanisms always need translators that can translate particular IPv4 address to particular IPv6 address and vice versa. A host with IPv4 address sends a request to an IPv6 enabled server on Internet that does not understand IPv4 address. In this scenario, the NAT-PT device can help them communicate. When the IPv4 host sends a request packet to the IPv6 server, the NAT-PT device/router strips down the IPv4 packet, removes IPv4 header, and adds IPv6 header and passes it through the Internet. When a response from the IPv6 server comes for the IPv4 host, the router does vice versa.



Routing:

Routing is the process of selecting a path for traffic in a network, or between or across multiple networks. It refers to establishing the routes that data packets take on their way to a particular destination. In general, routing involves the network topology, or the setup of hardware, that can effectively relay data. Standard protocols help to identify the best routes for data and to ensure quality transmission. Individual pieces of hardware such as routers are referred to as "nodes" in the network. Different algorithms and protocols can be used to figure out how to best route data packets, and which nodes should be used. There are 3 types of routing:
Static routing – Static routing is a process in which we have to manually add routes in routing table.

Advantages –

- No routing overhead for router CPU which means a cheaper router can be used to do routing.
- It adds security because only administrator can allow routing to particular networks only.
- No bandwidth usage between routers.

Disadvantage –

- For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.

- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

Default Routing –This is the method where the router is configured to send all packets towards a single router (next hop). It doesn't matter to which network the packet belongs, it is forwarded out to router which is configured for default routing. It is generally used with stub routers. A stub router is a router which has only one route to reach all other networks.

Fixed Path Routing:

A route is selected for each source and destination pair of nodes in the network. The routes are fixed and changes only if topology of the network changes. It is sometimes also referred to as static routing since the routes are fixed as in static routing.

Flooding:

Flooding adapts the technique in which every incoming packet is sent on every outgoing line expect from which it arrived. One problem with this is that packets may go in a loop and as a result of which a node may receive duplicate packets. These problems can overcome with the help of sequence numbers and hop count. No routing table is required for flooding and no network information like topology, load condition, cost of different paths is required. All possible routes between source and destination is tried, and there will be at least one route which is the shortest.

Unicast vs Multicast Routing:

A Unicast transmission/routing sends IP packets to a single recipient on a network. If the streaming data is to be distributed to a single destination, then we should start a Unicast stream by setting the destination IP address. For example, a device having IP address 10.1.2.0 in a network wants to send the traffic stream (data packets) to the device with IP address 20.12.4.2 in the other network, then unicast comes into the picture. This is the most common form of data transfer over the networks.

A Multicast transmission sends IP packets to a group of hosts on a network. IP multicast requires support of some other protocols like IGMP (Internet Group Management Protocol), Multicast routing for its working. Also, in Classful IP addressing Class D is reserved for multicast groups. If we want to distribute the data at multiple concurrent locations/destinations, then we should set the destination IP address to a valid Multicast IP address (224.0.0.0 – 239.255.255.255). Since Multicasting is a relatively new technology, some legacy devices that are part of the network might not support Multicasting.

Dynamic Routing –Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach it. RIP and OSPF are the best examples of dynamic routing protocol. Automatic adjustment will be made to reach the network destination if one route goes down.

A dynamic protocol has following features:

- The routers should have the same dynamic protocol running in order to exchange routes.
- When a router finds a change in the topology then router advertises it to all other

routers. Advantages –

- Easy to configure.
- More effective at selecting the best route to a destination remote network and also for discovering remote network.

Disadvantage –

- Consumes more bandwidth for communicating with other neighbors.
- Less secure than static routing.

Feature	Static Routing	Dynamic Routing
Hardware support	Supported by all routing hardware	May require special, more expensive routers
Router Memory Required	Minimal	Can require considerable memory for larger tables
Complexity	Simple	Complex
Overhead	None	Varying amounts of bandwidth used for routing protocol updates
Scalability	Limited to small networks	Very scalable, better for larger networks
Robustness	None - if a route fails it has to be fixed manually	Robust - traffic routed around failures automatically
Convergence	None	Varies from good to excellent

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. The cost of routing is a critical factor for all organizations. The least-expensive routing technology is provided by dynamic routing, which automates table changes and provides the best paths for data transmission.

Typically, dynamic routing protocol operations can be explained as follows:

- The router delivers and receives the routing messages on the router interfaces.
- The routing messages and information are shared with other routers, which use exactly the same routing protocol.
- Routers swap the routing information to discover data about remote networks.

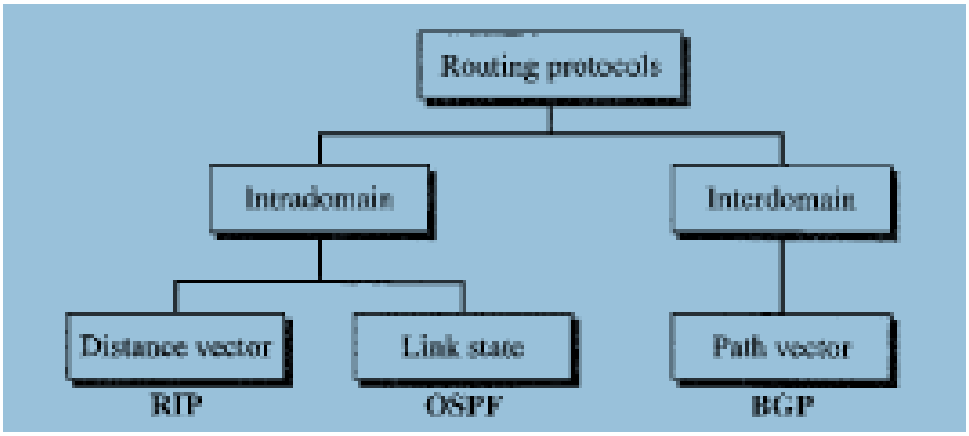
- Whenever a router finds a change in topology, the routing protocol advertises this topology change to other routers.

Dynamic routing is easy to configure on large networks and is more intuitive at selecting the best route, detecting route changes and discovering remote networks. However, because routers share updates, they consume more bandwidth than in static routing; the routers' CPUs and RAM may also face additional loads as a result of routing protocols. Also, dynamic routing is less secure than static routing. Dynamic routing uses multiple algorithms and protocols. The most popular are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

Popular Routing Algorithms:

A routing algorithm is a set of step-by-step operations used to direct Internet traffic efficiently. When a packet of data leaves its source, there are many different paths it can take to its destination. The routing algorithm is used to determine mathematically the best path to take.

Dynamic routing algorithms are basically categorized as follows:



Interior vs Exterior Routing:

Interior routing is a Routing mechanism which is used to find network path information within an Autonomous System. Known Interior Routing Protocols are Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS).

Exterior routing is a Routing mechanism which is used to find network path information between different Autonomous Systems. Exterior Routing Protocols are commonly used in the Internet to exchange routing table information. There is only one Exterior routing protocol exists now and it is Border Gateway Protocol (BGP).

Shortest Path Routing:

Shortest path routing refers to the process of finding paths through a network that have a minimum of distance or other cost metric. Shortest-path routing algorithms have existed since two independent research works by Bellman and Ford, and Dijkstra in 1950's. The difference between these two algorithms is the way information needed for computing the shortest-path is used. In the context of packet-switched networks and Internet routing, in particular, Bellman-Ford's algorithm has enabled the development of

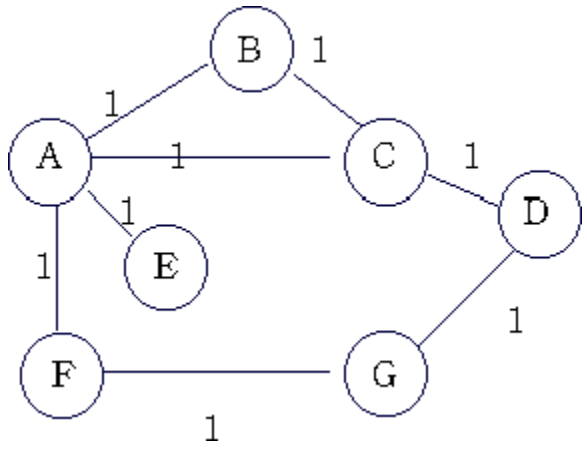
distance-vector routing protocols while Dijkstra's algorithm has paved the way to the introduction of link- state routing protocols.

Distance Vector Routing Algorithm:

A distance-vector routing protocol in data networks determines the best route for data packets based on distance. Distance-vector routing protocols measure the distance by the number of routers a packet has to pass, one router counts as one hop. The vector describes the route of the message over a given set of network nodes. To determine the best route across a network router on which a distance-vector protocol is implemented exchange information with one another, usually routing tables plus hop counts for destination networks and possibly other traffic information. The basic idea here is that each node receives some information from one or more of its directly attached neighbors, performs a calculation, and then distributes the results of its calculation back to its neighbors.

Distance vector routing algorithm is also called **Bellman Ford algorithm**. Each router maintains a Distance Vector table containing the distance between itself and all possible destination nodes. Distances, based on a chosen metric, are computed using information from the neighbors' distance vectors. The starting assumption for distance-vector routing is that each node knows the cost of the link to each of its directly connected neighbors. A link that is down is assigned an infinite cost.

E.g.:



Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	?	1	1	?
B	1	0	1	?	?	?	?
C	1	1	0	1	?	?	?
D	?	?	1	0	?	?	1
E	1	?	?	?	0	?	?
F	1	?	?	?	?	0	1
G	?	?	?	1	?	1	0

Table 1. Initial distances stored at each node(global view).

Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

Table 2. final distances stored at each node (global view).

In practice, each node's forwarding table consists of a set of triples of the form: (Destination, Cost, Next Hop).

For example, Table below shows the complete routing table maintained at node B for the network in figure above.

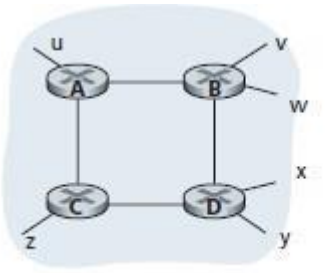
Destination	Cost	NextHop
A	1	A
C	1	C
D	2	C
E	2	A
F	2	A
G	3	A

Table 3. Routing table maintained at node B.

RIP (Routing Information Protocol):

Routing Information Protocol (RIP) is a dynamic protocol used to find the best route or path from end-to-end (source to destination) over a network by using a routing metric/hop count algorithm. This algorithm is used to determine the shortest path from the source to destination, which allows the data to be delivered at high speed in the shortest time. RIP plays an important role providing the shortest and best path for data to take from node to node. The hop is the step towards the next existing device, which could be a router, computer or other device. Once the length of the hop is determined, the information is stored in a routing table for future use. RIP is being used in both local and wide area networks and is generally considered to be easily configured and implemented.

Figure below illustrates an AS with six leaf subnets. The table in the figure indicates the number of hops from the source A to each of the leaf subnets.



Destination	Hops
u	1
v	2
w	2
x	3
y	3
z	2

Figure 4.34 ♦ Number of hops from source router A to various subnets

The maximum cost of a path is limited to 15, thus limiting the use of RIP to autonomous systems that are fewer than 15 hops in diameter. Recall that in DV protocols, neighboring routers exchange distance vectors with each other. The distance vector for any one router is the current estimate of the shortest path distances from that router to the subnets in the AS. In RIP, routing updates are exchanged between

neighbors approximately every 30 seconds using a RIP response message. The response message sent by a router or host contains a list of up to 25 destination subnets within the AS, as well as the sender's distance to each of those subnets. Response messages are also known as RIP advertisements.

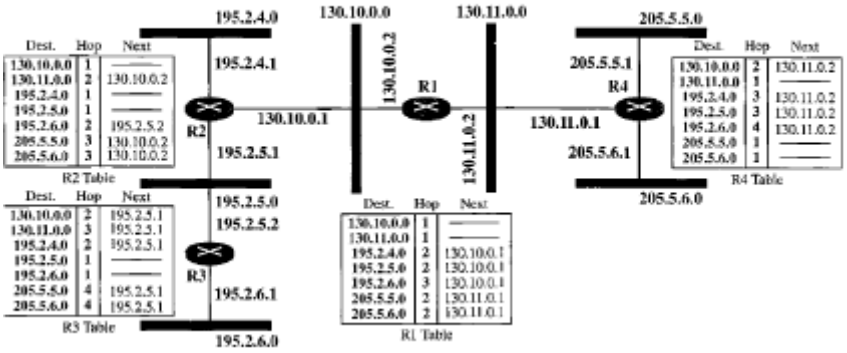
In brief the RIP protocol works as follows:

- Each router initializes its routing table with a list of locally connected networks.
- Periodically, each router advertises the entire contents of its routing table over all of its RIP-enabled interfaces.
  - Whenever a RIP router receives such an advertisement, it puts all of the appropriate routes into its routing table and begins using it to forward packets. This process ensures that every network connected to every router eventually becomes known to all routers.
  - If a router does not continue to receive advertisements for a remote route, it eventually times out that route and stops forwarding packets over it.
- Every route has a property called a metric, which indicates the "distance" to the route's destination.
  - Every time a router receives a route advertisement, it increments the metric.
  - Routers prefer shorter routes to longer routes when deciding which of two versions of a route to program in the routing table.
  - The maximum metric permitted by RIP is 16, which means that a route is unreachable. This means that the protocol cannot scale to networks where there may be more than 15 hops to a given destination.

RIP also includes some optimizations of this basic algorithm to improve stabilization of the routing database and to eliminate routing loops.

- When a router detects a change to its routing table, it sends an immediate "triggered" update. This speeds up stabilization of the routing table and elimination of routing loops.
- When a route is determined to be unreachable, RIP routers do not delete it straightaway. Instead they continue to advertise the route with a metric of 16 (unreachable). This ensures that neighbors are rapidly notified of unreachable routes, rather than having to wait for a soft state timeout.
- When router A has learnt a route from router B, it advertises the route back to B with a metric of 16 (unreachable). This ensures that B is never under the impression that A has a different way of getting to the same destination. This technique is known as "split horizon with poison reverse."
- A "Request" message allows a newly-started router to rapidly query all of its neighbors' routing tables.

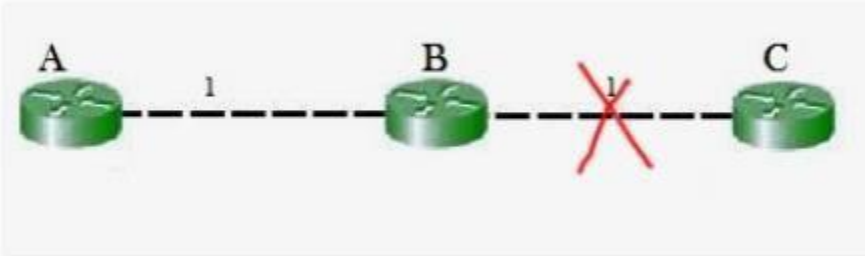
Figure 22.19 *Example of a domain using RIP*



The figure above shows an autonomous system with seven networks and four routers. Table for each router is also shown. Looking at routing table for R1, it has seven entries to show how to reach each network in the autonomous system. Router R1 is directly connected to networks 130.10.0.0 and 130.11.0.0, which means that there are no next hop entries for these two networks. To send a packet to one of the three networks at the far left, router R1 needs to deliver the packet to R2. The next-node entry for these three networks is the interface of router R2 with IP address 130.10.0.1. To send a packet to the two networks at the far right, router R1 needs to send the packet to the interface of router R4 with IP address 130.11.0.1. The other tables can be explained similarly.

The main issue with Distance Vector Routing (DVR) protocols is Routing Loops, since Bellman-Ford Algorithm cannot prevent loops. This routing loop in DVR network causes Count to Infinity Problem. Routing loops usually occur when any interface goes down or two-routers send updates at the same time.

Counting to infinity problem:



So in this example, the Bellman-Ford algorithm will converge for each router, they will have entries for each other. B will know that it can get to C at a cost of 1, and A will know that it can get to C via B at a cost of 2. If the link between B and C is disconnected, then B will know that it can no longer get to C via that link and will remove it from its table. Before it can send any updates it's possible that it will receive an update from A which will be advertising that it can get to C at a cost of 2. B can get to A at a cost of 1, so it will update a route to C via A at a cost of 3. A will then receive updates from B later and update its cost to 4. They will then go on feeding each other bad information toward infinity which is called as Count to Infinity problem.

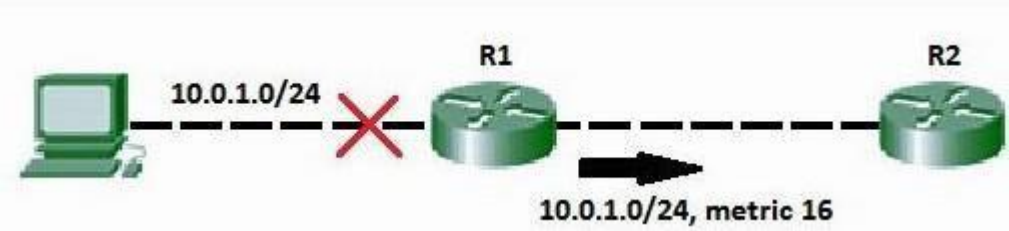
Solution for Count to infinity:

Triggered Update:

A type of Routing Information Protocol (RIP) announcement that occurs when network topology changes is called triggered update. With triggered updates, the update announcing network topology changes is sent almost immediately rather than waiting for the next periodic announcement. Triggered updates deal with count to infinity issues by forcing an update as soon as the link changes. Triggered updates improve the convergence time (the time it takes for a router to update its routing tables) of RIP internetworks, but at the cost of additional broadcast traffic while the triggered updates are propagated.

Route Poisoning:

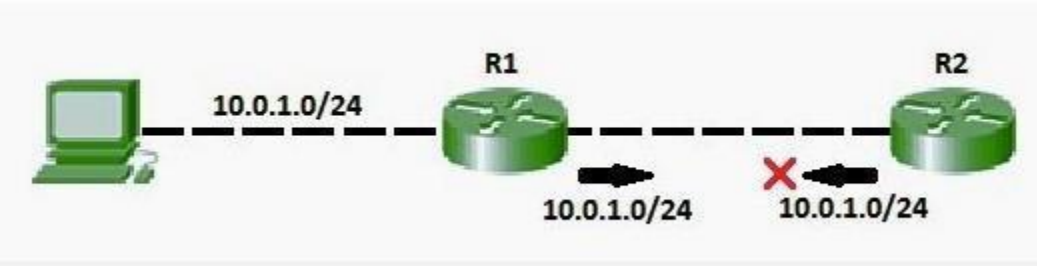
When a route fails, distance vector protocols spread the bad news about a route failure by poisoning the route. Route poisoning refers to the practice of advertising a route, but with a special metric value called Infinity. Routers consider routes advertised with an infinite metric to have failed. Each distance vector routing protocol uses the concept of an actual metric value that represents infinity. RIP defines infinity as 16. The main disadvantage of poison reverse is that it can significantly increase the size of routing announcements in certain fairly common network topologies.



Split horizon:

If the link between B and C goes down, and B had received a route from A , B could end up using that route via A. A would send the packet right back to B, creating a loop. But according to Split horizon Rule, Node A does not advertise its route for C (namely A to B to C) back to B. On the surface, this seems redundant since B will never route via node A because the route costs more than the direct route from B to C.

Consider the following network topology showing Split horizon:



In addition to these, we can also use split horizon with route poisoning where above both technique will be used combinely to achieve efficiency and less increase the size of routing announcements.

Split horizon with Poison reverse technique is used by Routing Information Protocol (RIP) to reduce routing loops. Additionally, **Holddown** timers can be used to avoid the formation of loops. Holddown timer immediately starts when the router is informed that attached link is down. Till this time, router ignores all updates of down route unless it receives an update from the router of that downed link. During the timer, if the down link is reachable again, routing table can be updated.

Disadvantage:

- The primary drawback of this algorithm is its vulnerability to the 'Count-to-Infinity' problem. Many partial solutions have been proposed but none works under all circumstances.
- Another drawback of this scheme is that it does not take into account link bandwidth.
- Yet another problem with this algorithm is that it takes longer time for convergence as network size grows.
- Increased network traffic: RIP checks with its neighboring routers every 30 seconds, which increases network traffic.
- Maximum hop count: RIP has a maximum hop count of 15, which means that on large networks, other remote routers may not be able to be reached.
- Closest may not be shortest: Choosing the closest path by hop count does not necessarily mean that the fastest route was selected. RIP does not consider other factors when calculating best path.
- RIP only updates neighbors so the updates for non-neighboring routers are not first-hand information

Link State Protocols:

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. Each collection of best paths will then form each node's routing table. While distance vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology. Based on this learned topology, each router is then able to compute its routing table by using a shortest path computation.

Features of link state routing protocols:

- Link state packet – A small packet that contains routing information.
- Link state database – A collection information gathered from link state packet.
- Shortest path first algorithm (Dijkstra algorithm) – A calculation performed on the database results into shortest path
- Routing table – A list of known paths and interfaces.

Calculation of shortest path –

To find shortest path, each node need to run the famous **Dijkstra algorithm**. Dijkstra's algorithm is an algorithm for finding the shortest paths between nodes in a graph. This famous algorithm uses the following steps:

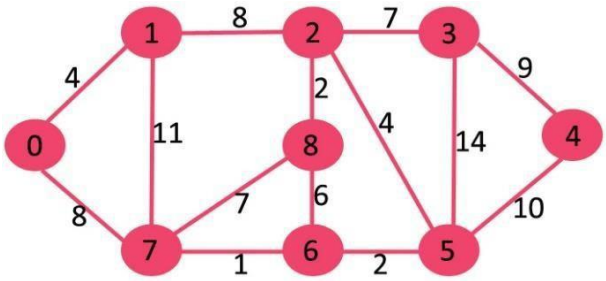
Step-1: The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database

Step-2: Now the node selects one node, among all the nodes not in the tree like structure, which is nearest to the root, and adds this to the tree. The shape of the tree gets changed.

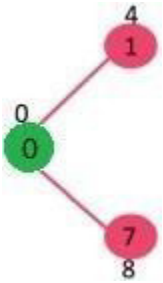
Step-3: After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.

Step-4: The node repeats the Step 2 and Step 3 until all the nodes are added in the tree.

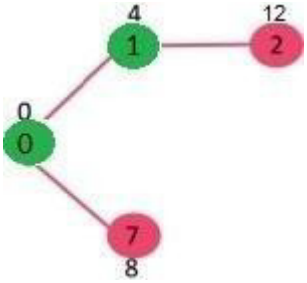
Let us understand with the following example:



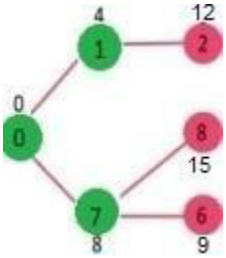
The set sptSet is initially empty and distances assigned to vertices are {0, INF, INF, INF, INF, INF, INF, INF} where INF indicates infinite. Now pick the vertex with minimum distance value. The vertex 0 is picked, include it in sptSet. So sptSet becomes {0}. After including 0 to sptSet, update distance values of its adjacent vertices. Adjacent vertices of 0 are 1 and 7. The distance values of 1 and 7 are updated as 4 and 8. Following subgraph shows vertices and their distance values, only the vertices with finite distance values are shown. The vertices included in SPT are shown in green colour.



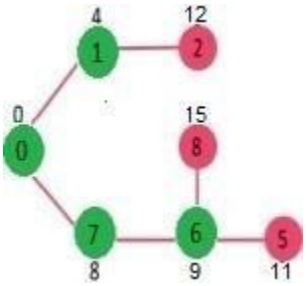
Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). The vertex 1 is picked and added to sptSet. So sptSet now becomes {0, 1}. Update the distance values of adjacent vertices of 1. The distance value of vertex 2 becomes 12.



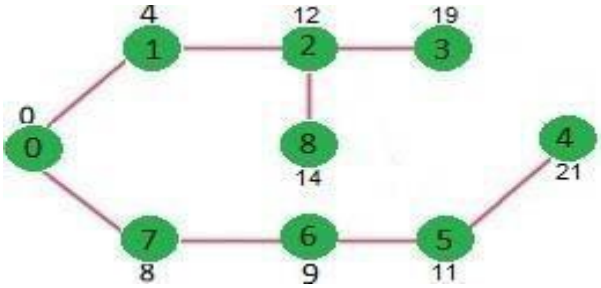
Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 7 is picked. So sptSet now becomes {0, 1, 7}. Update the distance values of adjacent vertices of 7. The distance value of vertex 6 and 8 becomes finite (15 and 9 respectively).



Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 6 is picked. So sptSet now becomes {0, 1, 7, 6}. Update the distance values of adjacent vertices of 6. The distance value of vertex 5 and 8 are updated.

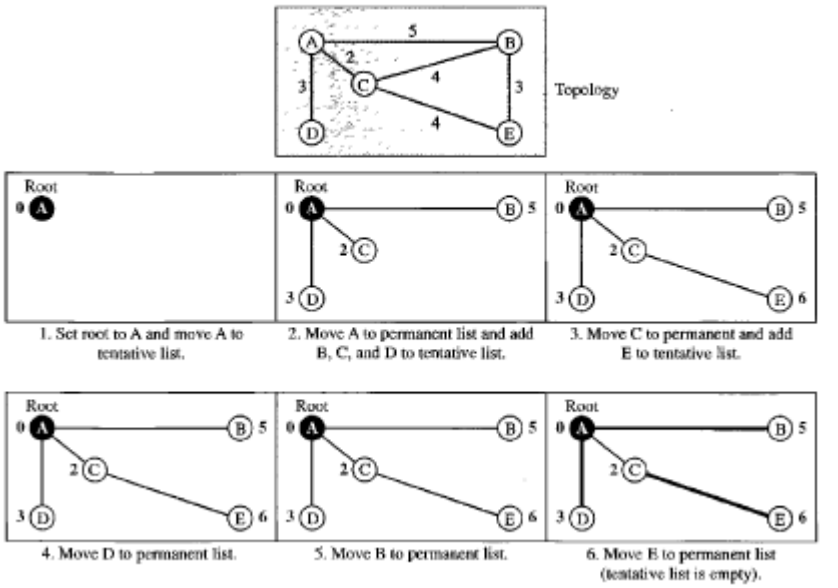


We repeat the above steps until sptSet doesn't include all vertices of given graph. Finally, we get the following Shortest Path Tree (SPT).



Another example for Dijkstra's algorithm is as follows:

Figure 22.23 *Example of formation of shortest path tree*



Overview of OSPF (Open Path Shortest First):

Open Shortest Path First (OSPF) is a link state routing protocol (LSRP) that uses the Shortest Path First (SPF) network communication algorithm (Dijkstra's algorithm) to calculate the shortest connection path between known devices.

The OSPF routing protocol has largely replaced the older Routing Information Protocol (RIP) in corporate networks. Using OSPF, a router that learns of a change to a routing table (when it is reconfigured by network staff, for example) or detects a change in the network immediately multicasts the information to all other OSPF hosts in the network so they will all have the same routing table information. Unlike RIP, which requires routers to send the entire routing table to neighbors every 30 seconds, OSPF sends only the part that has changed and only when a change has taken place. When routes change -- sometimes due to equipment failure -- the time it takes OSPF routers to find a new path between endpoints with no loops (which is called "open") and that minimizes the length of the path is called the convergence time. Rather than simply counting the number of router hops between hosts on a network, as RIP does, OSPF bases its path choices on "link states" that take into account additional network information, including IT-assigned cost metrics that give some paths higher assigned costs. For example, a satellite link may be assigned higher cost than a wireless WAN link, which in turn may be assigned higher cost than a metro Ethernet link.

For example, a person in city A wants to travel to city M and is given two options:

Travel via cities B and C. The route would be ABCM. And the distance (or bandwidth cost in the networking case) for A-B is 10 miles, B-C is 5 miles and C-M is 10 miles.

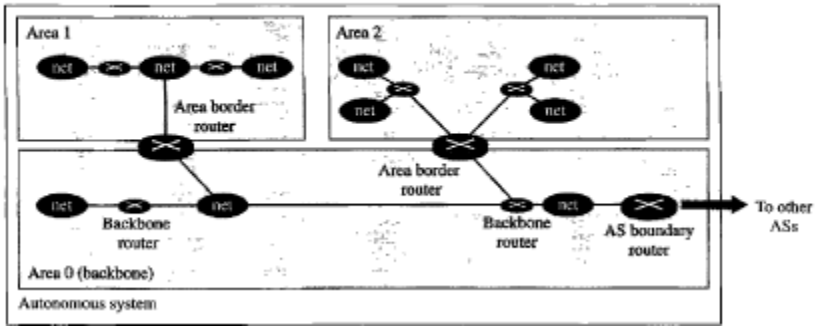
Travel via city F. The route would be AFM. And the distance for A-F is 20 miles and F-M is 10 miles.

The shortest route is always the one with least amount of distance covered in total. Thus, the ABCM route is the better option (10+5+10=25), even though the person has to travel to two cities as the associated total cost to travel to the destination is less than the second option with a single city (20+10=30). OSPF performs a similar algorithm by first calculating the shortest path between the source and destination based on link bandwidth cost and then allows the network to send and receive IP packets via the shortest route.

OSPF Network Topology:

Two routers communicating OSPF to each other exchange information about the routes they know about and the cost for them to get there. When many OSPF routers are part of the same network, information about all of the routes in a network are learned by all of the OSPF routers within that network—technically called an area. Each OSPF router passes along information about the routes and costs they've heard about to all of their adjacent OSPF routers, called neighbors.

Figure 22.24 *Areas in an autonomous system*



An area is a collection of networks, hosts, and routers all contained within an autonomous system. At the border of an area, special routers called area border routers summarize the information about the area and send it to other areas. Among the areas inside an autonomous system is a special area called the backbone; all the areas inside an autonomous system must be connected to the backbone. In other words, the backbone serves as a primary area and the other areas as secondary areas. The routers inside the backbone are called the backbone routers.

OSPF works best in a hierarchical routing environment. When designing an OSPF network, the first and most important task is to determine which routers and links are to be included in the backbone (area 0) and which are to be included in each area. The following are three important characteristics to OSPF to ensure that your OSPF network has a hierarchical routing structure:

- The hierarchical routing structure must exist or be created to effectively use OSPF. The benefits of having a single area include simplicity, ease of troubleshooting, and so on.
- A contiguous backbone area must be present, and all areas must have a connection to the backbone.
- Explicit topology (shortest path) has precedence over any IP addressing schemes that might have been applied; that is, your physical topology takes precedence over a summarized route.

When designing the topology for an OSPF network, consider the following important items:

- Number of routers in an area
- Number of areas connected to an ABR (Area border router)
- Number of neighbors for a router
- Number of areas supported by a router
- Selection of the designated router (DR)
- Size and development of the OSPF LSDB (link state database)

OSPF Protocols (hello, exchange, flooding):

Routers periodically send hello packets on all interfaces to establish and maintain neighbor relationships. Hello packets are multicast on physical networks that have a multicast or broadcast capability, which enables dynamic discovery of neighboring routers. Hello packets are sent out every 10 seconds which helps to detect failed neighbors. RouterDeadInterval (default 40 seconds) is specified for detecting such neighbors. Also, hello message ensures that link between neighbors is bidirectional. Neighboring routers agree on intervals where hello interval is set so that a link is not accidentally brought down.

OSPF uses hello packets and two timers to check if a neighbor is still alive or not:

Hello interval: this defines how often we send the hello packet.

Dead interval: this defines how long we should wait for hello packets before we declare the neighbor dead.

(1) Hello	Discovers neighbors and builds adjacencies between them
(2) Database Description	Checks for database synchronization between routers
(3) Link-State Request	Requests specific link-state records from another router
(4) Link-State Update	Sends specifically requested link-state records
(5) Link-State Acknowledgement	Acknowledges the other packet types

The Hello message contains a list of information needed to form an OSPF neighbor relation between two neighboring routers, the following a list of information contained the Hello messages:

- OSPF Router ID. The router's ID which is configured or automatically selected by OSPF (analyzed below)
- Hello Interval Timer. Frequency upon which Hello packets are sent.
- Dead Interval Timer. Defines how long we should wait for hello packets before we declare the neighbor dead.
- Subnet Mask
- Router Priority. Used to help determine the Designated Router (DR). Higher priority takes precedence. A configured Priority of 0 means the router will not become a DR or BDR.

- List of reachable OSPF neighbors in the network.
- Area ID
- DR & BDR's IP addresses (if exists)
- Authentication Password (if configured)

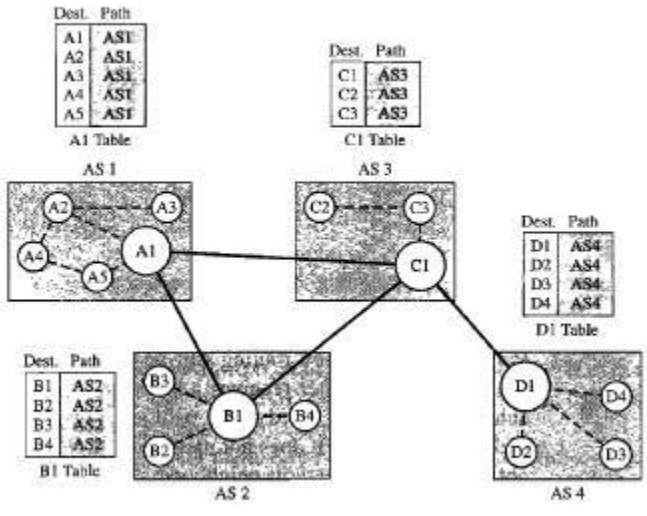
Path Vector:

Distance vector and Link State routing are both intradomain routing protocols. They can be used inside an autonomous system, but not between the autonomous systems. These two protocols are not suitable for interdomain routing mostly because of scalability. Both of these routing protocols become intractable when the domain of operation becomes large. Distance vector routing is subject to instability if there are more than a few hops in the domain of operation. Link state routing needs a huge amount of resources to calculate routing tables. It also creates heavy traffic because of flooding. There is a need for a third routing protocol which we call path vector routing.

Path Vector Routing is a routing algorithm in unicast routing protocol of network layer, and it is useful for interdomain routing. The principle of path vector routing is similar to that of distance vector routing. In path vector routing, we assume that there is one node (there can be more, but one is enough) in each autonomous system that acts on behalf of the entire autonomous system, referred to as speaker node. The speaker node in an AS creates a routing table and advertises it to speaker nodes in the neighboring autonomous systems. A speaker node advertises the path, not the metrics of the nodes, in its autonomous system or other autonomous systems.

Initialization: At the beginning, each speaker node can only know only the reachability of the nodes inside its autonomous system.

Figure 22.30 *Initial routing tables in path vector routing*



Sharing: Just as in distance vector routing, in path vector routing, a speaker in an autonomous system shares its table with immediate neighbors. In figure, node A1 shares its table with nodes B1 and C1.

Node C1 shares its table with nodes D1, B1 and A1. Node B1 shares its table with C1 and A1. Node D1 shares its table with C1.

Updating: When a speaker node receives a two-column table from a neighbor, it updates its own table by adding the nodes that are not in its routing table and adding its own autonomous system and the autonomous system that sent the table. After a while, each speaker has a table and knows how to reach each node in other autonomous systems. Figure below shows the tables for each speaker node after the system is stabilized.

Loop prevention: The instability of distance vector routing and the creation of loops can be avoided in path vector routing. When a router receives a message, it checks to see if its autonomous system is in the path list to the destination. If it is, looping is involved and the message is ignored.

Policy routing: Policy routing can be easily implemented through path vector routing. When a router receives a message, it can check the path. If one of the autonomous systems listed in the path is against its policy, it can ignore that path and that destination. It does not update its routing table with this path, and it does not send this message to its neighbors.

Optimum path: The optimum path in path vector routing is a path to a destination that is the best for the organization that runs the autonomous system. We cannot use metrics in this route because each autonomous system that is included in the path may use a different criterion for the metric. One system may use RIP which defines hop count as the metric, another may use OSPF with the minimum delay (higher link bandwidth) as the metric. The optimum path is the path that fits the organization. In previous figure, each autonomous system may have more than one path to a destination. For eg: a path from AS4 to AS1 can be AS4-AS3-AS2-AS1 or it can be AS4-AS3-AS1. For the tables, we choose the one that had the smaller number of autonomous systems, but this is not always the case. Other criteria, such as security, safety, and reliability can also be applied.

Border Gateway Protocol:

Border gateway protocol (BGP) is an interdomain routing protocol using path vector routing. BGP is protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers. BGP directs packets between autonomous systems (AS) -- networks managed by a single enterprise or service provider. Traffic that is routed within a single network AS is referred to as internal BGP, or iBGP. More often, BGP is used to connect one AS to other autonomous systems, and it is then referred to as an external BGP, or eBGP.

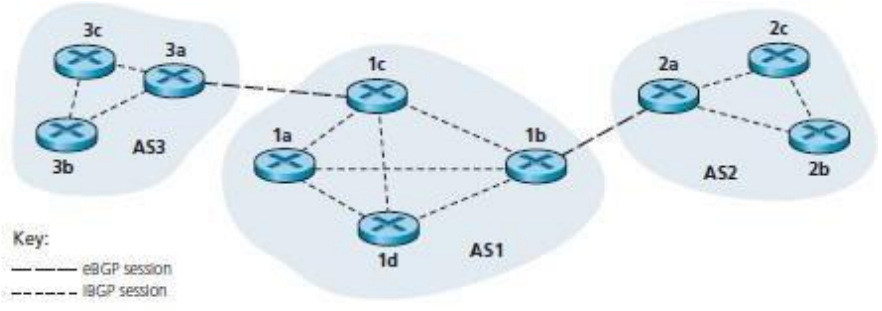


Figure 4.40 ♦ eBGP and iBGP sessions

All other routing protocols are concerned solely with finding the optimal path towards all known destinations. BGP cannot take this simplistic approach because the peering agreements between ISPs almost always result in complex routing policies. To help network operators implement these policies, BGP carries a large number of attributes with each IP prefix: **(BGP Path Attributes)**

- Weight – The BGP weight attribute is Cisco-specific and is used to influence how traffic is routed for a specific BGP device. This value does not pass between internal or external BGP neighbors (peers).
- Local Preference – The local preference attribute is used to dictate how traffic prefers to leave a specific BGP ASN. This attribute is passed between neighbors within the same ASN. The highest local preference gets priority.
- Local Routes – Routes which have been sourced from the local router will be preferred over those sourced from other routers.
- Shortest AS_PATH – With BGP, the path is notated by the ASN of the external BGP networks that must be traversed to reach the destination network; e.g., 10 20 30 means that the traffic must pass through ASNs 10, 20, and 30 to reach the destination. If multiple options exist to a specific network, the one with the shortest AS path will be preferred.
- Origin – With origin, BGP is looking for the source of the initial network advertisement, for example if it was redistributed from an IGP, an EGP or through an unknown source. When analyzing this attribute, routes that have originated from an IGP are preferred to those from an EGP, and routes that have originated by an EGP will be preferred over those originated from an unknown source. I < E <?
- Multi-Exit Discriminator (MED) – The MED is a value that can be injected into a neighboring BGP ASN. This is used when multiple paths exist between two different BGP ASNs. The MED is used to suggest to the neighboring ASN the preferred way to route traffic into their network. The lowest MED value gets priority.
- BGP Neighbor Type – There are two different types of BGP neighborship: internal and external. A BGP neighborship that exists within the same ASN between two devices is considered internal, and a BGP neighborship that exists between devices from different ASNs is considered external. External (or eBGP) routes are preferred to Internal (iBGP) routes.
- IGP metric/next hop – The next attribute uses the IGP metric to the BGP next hop address.
- Oldest External Route – If the contending BGP routes are external then the one which has existed the longest will be preferred
- Lowest Router-ID – The route with the lowest BGP router ID will be preferred
- Lowest Neighbor Address – The route coming through a neighbor with the lowest address will be preferred.

BGP Message (Packet) Types:

BGP communication uses four message types: Open, Update, Keep Alive, Notification.

There is a 5th message type defined in BGP called **Route-Refresh** to support the route refresh capability. 'Route Refresh Capability', which would allow the dynamic exchange of route refresh request between BGP speakers and subsequent re-advertisement. One possible application of this capability is to facilitate non-disruptive routing policy changes.

Type	Name	Functional Overview
1	OPEN	Sets up and establishes BGP adjacency
2	UPDATE	Advertises, updates, or withdraws routes
3	NOTIFICATION	Indicates an error condition to a BGP neighbor
4	KEEPALIVE	Ensures that BGP neighbors are still alive

Open Message:

Once two BGP routers have completed a TCP 3-way handshake they will attempt to establish a BGP session, this is done using open messages. In the open message we will find some information about the BGP router, these have to be negotiated and accepted by both routers before we can exchange any routing information.

Update Message:

Once two routers have become BGP neighbors, they can start exchanging routing information. This is done with the update message. In the update message you will find information about the prefixes that are advertised.

Notification Message:

A Notification message is sent when an error is detected with the BGP session, such as a hold timer expiring, neighbor capabilities change, or a BGP session reset is requested. This causes the BGP connection to close.

Keep Alive Message:

BGP does not rely on the TCP connection state to ensure that the neighbors are still alive. Keepalive messages are exchanged every one-third of the Hold Timer agreed upon between the two BGP routers. Cisco devices have a default Hold Time of 180 seconds, so the default Keepalive interval is 60 seconds. If the Hold Time is set for zero, no Keepalive messages are sent between the BGP neighbors.

Characteristics of Border Gateway Protocol (BGP):

- Inter-Autonomous System Configuration: The main role of BGP is to provide communication between two autonomous systems.
- BGP supports Next-Hop Paradigm.
- Coordination among multiple BGP speakers within the AS (Autonomous System).
- Path Information: BGP advertisement also include path information, along with the reachable destination and next destination pair.

- Policy Support: BGP can implement policies that can be configured by the administrator. For ex:- a router running BGP can be configured to distinguish between the routes that are known within the AS and that which are known from outside the AS.
- Runs Over TCP.
- BGP conserve network Bandwidth.
- BGP supports CIDR.
- BGP also supports Security.

Functionality of Border Gateway Protocol (BGP):

BGP peers performs 3 functions, which are given below.

- The first function consists of initial peer acquisition and authentication. both the peers established a TCP connection and perform message exchange that guarantees both sides have agreed to communicate.
- The second function mainly focus on sending of negative or positive reach-ability information.
- The third function verifies that the peers and the network connection between them are functioning correctly.

BGP Route Information Management Functions:

- Route Storage: Each BGP stores information about how to reach other networks.
- Route Update: In this task, Special techniques are used to determine when and how to use the information received from peers to properly update the routes.
- Route Selection: Each BGP uses the information in its route databases to select good routes to each network on the internet network.
- Route advertisement: Each BGP speaker regularly tells its peer what is knows about various networks and methods to reach them.

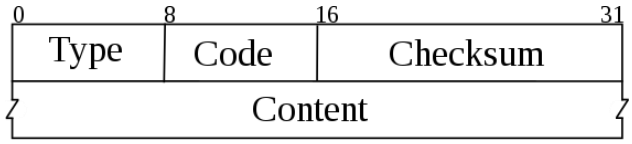
Internet Control Message Protocol (ICMP):

- ICMP is a TCP/IP network layer protocol that provides troubleshooting, control and error message services.
- Internet Control Message Protocol is also known as RFC 792.
- While ICMP is not used regularly in end-user applications, it is used by network administrators to troubleshoot Internet connections in diagnostic utilities.
- An ICMP message is created as a result of errors in an IP datagram. These errors are reported to the originating datagram's source IP address.
- An ICMP message is encapsulated directly within a single IP datagram and reports errors in the processing of datagrams.
- ICMP messages are transmitted as datagrams and consist of an IP header that encapsulates the ICMP data.
- ICMP packets are IP packets with ICMP in the IP data portion. ICMP messages also contain the entire IP header from the original message, so the end system knows which packet failed.

There can be several reasons behind reporting the error like:

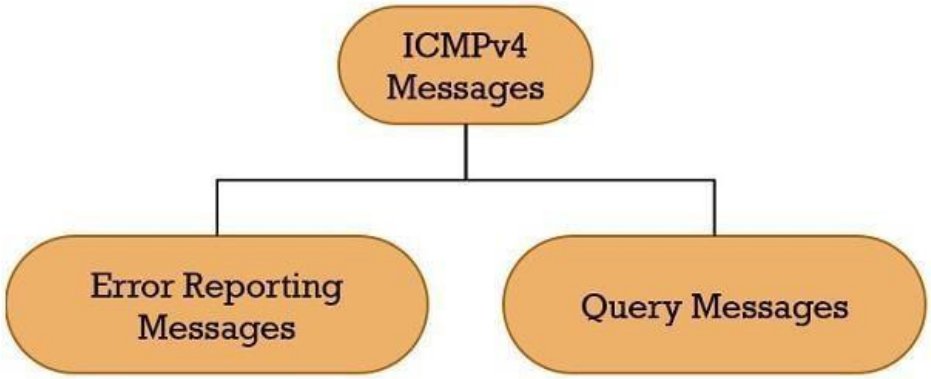
- A router with a datagram for a host in another network, may not find the next hop (router) to the final destination host.
- Datagram's time-to-live field has become zero.
- There may be ambiguity in the header of IP datagram.
- It may happen that all the fragments of datagram if do not arrive within a time limit to the destination host.

ICMP Header Format:



ICMP is available for both IPv4 and IPv6. The header format is similar for both versions of ICMP. ICMPv4 is the messaging protocol for IPv4. ICMPv6 provides these same services for IPv6 but includes additional functionality.

ICMPv4: ICMP for IPv4



Error Reporting Messages: (Report the error)

- Destination unreachable
- Source Quench
- Time Exceeded
- Parameter Problem (header field parameters corrupted)
- Redirection (when packet being routed wrongly, informed by intermediate

router) Query Messages: (identify network problems)

- Echo Request and Reply
- Timestamp Request and Reply

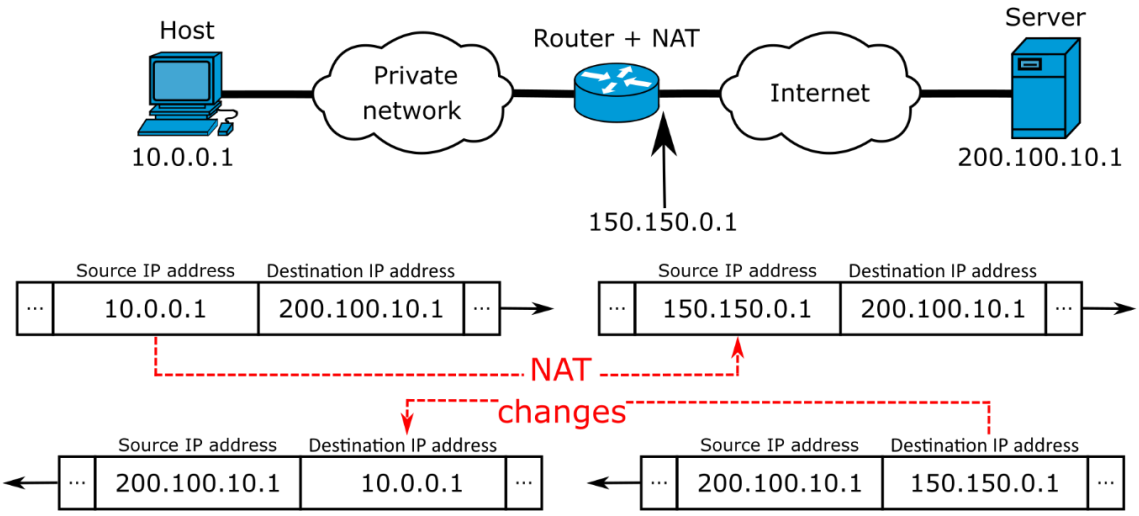
ICMPv6:

- Internet Control Message Protocol version 6 (ICMPv6) is the implementation of the Internet Control Message Protocol (ICMP) for Internet Protocol version 6 (IPv6).
- ICMPv6 is defined in RFC 4443.
- ICMPv6 plays a far more important role in the operation of IPv6 than ICMPv4 does for IPv4.
- ICMPv6 is an integral part of IPv6 and performs error reporting and diagnostic functions (e.g., ping).
- ICMPv6 has a framework for extensions to implement future changes. Several extensions have been published, defining new ICMPv6 message types as well as new options for existing ICMPv6 message types.
- For example, Neighbor Discovery Protocol (NDP) is a node discovery protocol based on ICMPv6 which replaces and enhances functions of ARP.
- Secure Neighbor Discovery (SEND) is an extension of NDP with extra security.
- Multicast Listener Discovery (MLD) is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like Internet Group Management Protocol (IGMP) is used in IPv4.
- Multicast Router Discovery (MRD) allows the discovery of multicast routers.

Network Address Translation (NAT):

NAT is a technique to map multiple local private addresses to a public one before transferring the information. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.

The most common form of network translation involves a large private network using addresses in a private range (10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, or 192.168.0 0 to 192.168.255.255).



NAT Types:

There are three different types of NATs.

1. Static NAT

When the local address is converted to a public one, this NAT chooses the same one. This means there will be a consistent public IP address associated with that router or NAT device.

2. Dynamic NAT

Instead of choosing the same IP address every time, this NAT goes through a pool of public IP addresses. This results in the router or NAT device getting a different address each time the router translates the local address to a public address.

3. PAT

PAT stands for port address translation. It's a type of dynamic NAT, but it bands several local IP addresses to a singular public one. Organizations that want all their employees' activity to use a singular IP address use a PAT, often under the supervision of a network administrator.

Why use NAT?

IP Conservation: IP addresses identify each device connected to the internet. The existing IP version 4 (IPv4) uses 32-bit numbered IP addresses, which allows for 4 billion possible IP addresses, which seemed like more than enough when it launched in the 1970s.

However, the internet has exploded, and while not all 7 billion people on the planet access the internet regularly, those that do often have multiple connected devices: phones, personal desktop, work laptop, tablet, TV, even refrigerators.

Therefore, the number of devices accessing the internet far surpasses the number of IP addresses available. Routing all of these devices via one connection using NAT helps to consolidate multiple private IP addresses into one public IP address. This helps to keep more public IP addresses available even while private IP addresses proliferate.

Network Traffic Analysis:

Network traffic analysis (NTA) is a method of monitoring network availability and activity to identify anomalies, including security and operational issues.

In other words, Network traffic analysis (NTA) is the process of intercepting, recording and analyzing network traffic communication patterns in order to detect and respond to security threats.

Network traffic analysis is primarily done to get in-depth insight into what type of traffic/network packets or data is flowing through a network.

Typically, network traffic analysis is done through a network monitoring or network bandwidth monitoring software/application. The traffic statistics from network traffic analysis helps in:

- Understanding and evaluating the network utilization
- Download/upload speeds
- Type, size, origin and destination and content/data of packets
- Collecting a real-time and historical record of what's happening on your network
- Detecting malware activity
- Detecting the use of vulnerable protocols and ciphers
- Troubleshooting a slow network
- Improving internal visibility and eliminating blind spots

Network security staff uses network traffic analysis to identify any malicious or suspicious packets within the traffic. Similarly, network administrations seek to monitor download/upload speeds, throughput, content, etc. to understand network operations.

Network traffic analysis is also used by attackers/intruders to analyze network traffic patterns and identify any vulnerabilities or means to break in or retrieve sensitive data.

Security Concepts: Firewall & Router Access Control

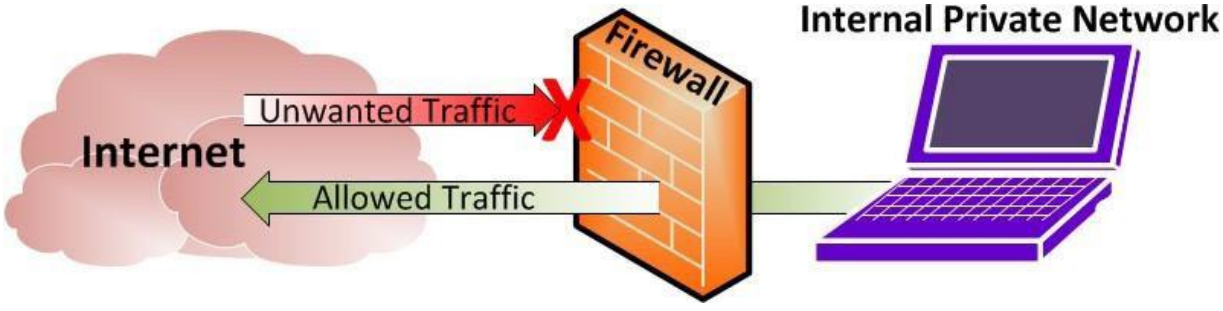
Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

Firewall:

A firewall is a software or a hardware device that examines the data from several networks and then either permits it or blocks it to communicate with your network and this process is governed by a set of predefined security guidelines.

In other words, a firewall is a hardware device or software application installed on the borderline of secured networks to examine and control incoming and outgoing network communications.

A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the internet.



Hardware firewalls can be purchased as a stand-alone product but are also typically found in routers, and should be considered as an important part of system and network set-up.

Software firewalls are installed on your computer (like any software) and we can customize it; allowing us some control over its function and protection features.

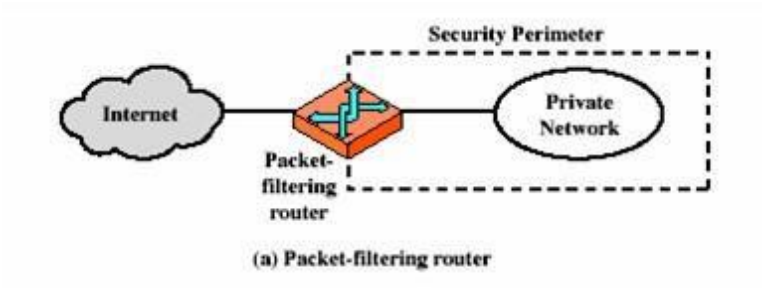
Types of Firewall:

There are four basic types of firewalls:

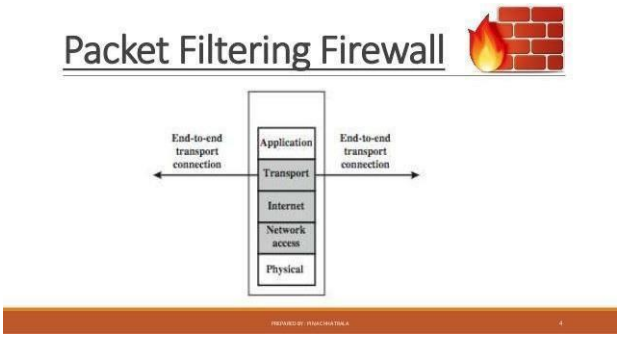
- Packet Filtering Firewall
- Stateful Inspection Firewall
- Circuit-Level Gateway
- Application-Level Gateway

Packet Filtering Firewall:

- A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.
- The firewall is typically configured to filter packets going in both directions (from and to the internal network).
- Filtering rules are based on information contained in a network packet.
- Two default policies are possible:
    - Default = discard: That which is not expressly permitted is prohibited.
    - Default = forward: That which is not expressly prohibited is permitted.
- Advantage of a packet filtering firewall is its simplicity. Also, packet filters typically are transparent to users and are very fast.

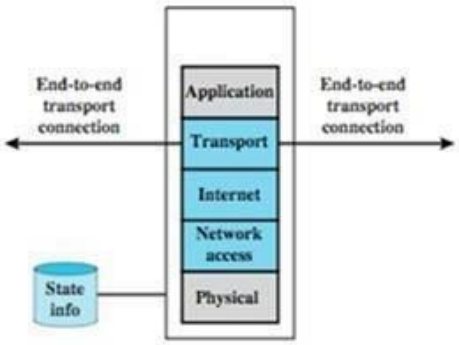


(a) Packet-filtering router



State-full Inspection Firewall:

- State-full packet filtering is a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.
- It is also known as dynamic packet filtering and Stateful inspection filtering.
- Only packets matching a known active connection are allowed to pass the firewall.
- It is a security feature often included in business networks.



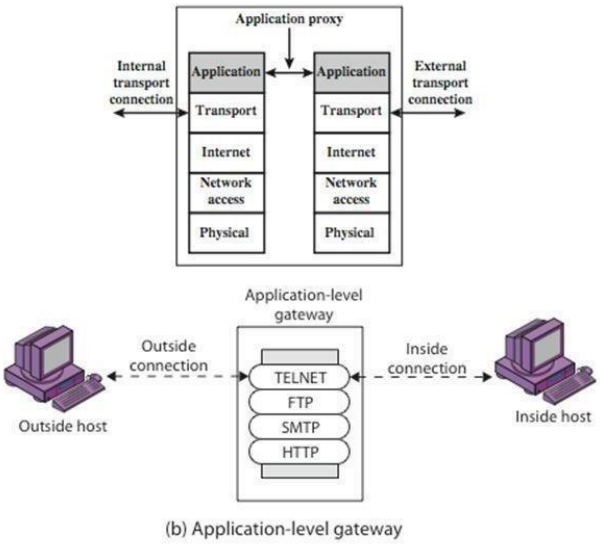
(c) Stateful inspection firewall

- A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections.
- There is an entry for each currently established connection.
- The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.
- By recording session information such as IP addresses and port numbers, a dynamic packet filter can implement a much tighter security posture than a static packet filter can.

Application-Level Gateway:

- An application-level gateway, also called an application proxy, acts as a relay of application-level traffic.
- The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.
- When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.
- If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall.
- Application proxy filters incoming node traffic to certain specifications which mean that only transmitted network application data is filtered.
- Application-level gateways tend to be more secure than packet filters.
- In addition, it is easy to log and audit all incoming traffic at the application level.
- Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application-level gateway need only examine a few allowable applications.

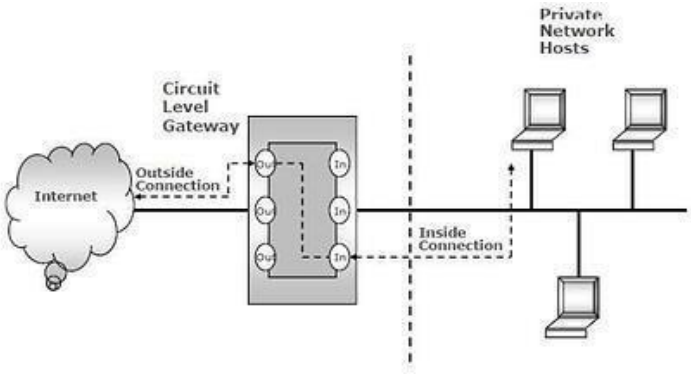
Firewalls - Application Level Gateway (or Proxy)



(b) Application-level gateway

Circuit Level Gateway:

- A fourth type of firewall is the circuit-level gateway or circuit-level proxy.
- The circuit level gateway firewalls work at the transport and session layer of the OSI model. They monitor TCP handshaking between the packets to determine if a requested session is legitimate.
- As with an application gateway, a circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host.
- Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents.
- The security function consists of determining which connections will be allowed.
- A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users.



Router Access Control (ACL):

- ACLs are a network filter utilized by routers and some switches to permit and restrict data flows into and out of network interfaces.
- When an ACL is configured on an interface, the network device analyzes data passing through the interface, compares it to the criteria described in the ACL, and either permits the data to flow or prohibits it.
- There are a variety of reasons we use ACLs. The primary reason is to provide a basic level of security for the network.
- ACLs are not as complex and in depth of protection as firewalls, but they do provide protection on higher speed interfaces where line rate speed is important and firewalls may be restrictive. Also, ACLs do offer a significant amount of firewall capability.
- ACLs are also used to restrict updates for routing from network peers and can be instrumental in defining flow control for network traffic.
- ACLs should be placed on external routers to filter traffic against less desirable networks and known vulnerable protocols.
- One of the most common methods in this case is to setup a DMZ, or de-militarized buffer zone in your network.
- This architecture is normally implemented with two separate network devices:

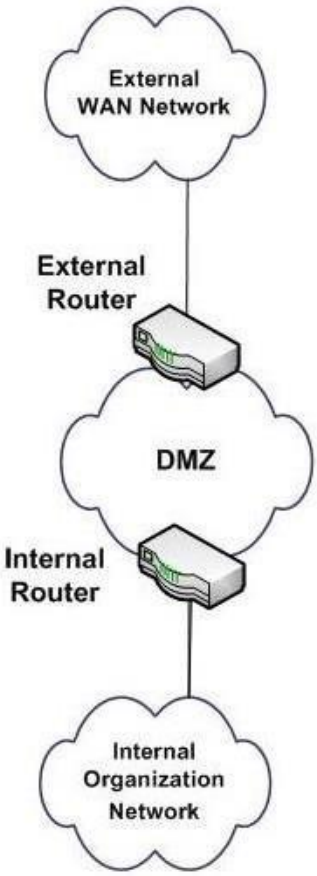


Fig: External Network Configuration with DMZ

Unit 4: Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. A process is a network application running on a host. Whereas the network layer oversees source-to-destination delivery of packets, it does not recognize any relationship between those packets. The transport layer ensures that the whole message arrives at the host application.

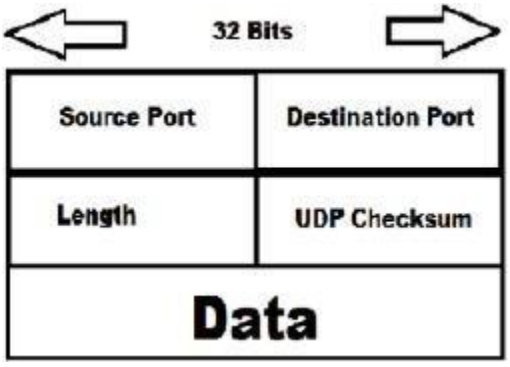
Transport Layer Services & Responsibilities:

- Process to Process Delivery
- Multiplexing and Demultiplexing – simultaneous use of different applications
- Segmentation and reassembly
- Congestion Control
- Connection Control – TCP or UDP
- Flow Control
- Error Control

User Datagram Protocol (UDP):

The user datagram protocol (UDP) is called a connectionless, unreliable transport protocol. It does not add anything to the services of IP except to provide process-to-process communication instead of host-to-host communication.

The UDP packet structure is as follows:



UDP Operations:

UDP uses concepts common to the transport layer.

Connectionless Services: UDP provides connectionless service which means that each user datagram sent by UDP is an independent datagram. There is no relationship between the different user datagrams even if they are coming from the same source process and going to the same destination process. The user

datagrams are not numbered and there is no connection establishment and no connection termination, which means each user datagram can travel on a different path. Stream of data cannot be sent; it should get fragmented.

Flow and Error Control: UDP is a very simple, unreliable transport protocol which does not provide flow control. The receiver may overflow with incoming messages. There is error control mechanism in UDP except checksum, which means the sender does not know if a message has been lost or duplicated. When the receiver detects an error through the checksum, the user datagram is silently discarded.

Encapsulation and Decapsulation: To send a message from one process to another, the UDP protocol encapsulates and decapsulates messages in an IP datagram.

Queuing: Queuing in UDP simply refers to requesting port number for client processes and using that port number for process-to-process delivery of messages.

UDP Characteristics and Applications:

- UDP allows very simple data transmission without any error detection. So, it can be used in networking applications like VOIP, streaming media, etc. where loss of few packets can be tolerated and still function appropriately.
- UDP is suitable for multicasting since multicasting capability is embedded in UDP software but not in TCP software.
- UDP is used for management processes such as SNMP.
- UDP is used for some route updating protocols such as RIP.
- UDP is used by Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to systems dynamically.
- UDP is an ideal protocol for network applications where latency is critical such as gaming and voice and video communications.

Transmission Control Protocol (TCP):

TCP is a transport layer protocol for process-to-process communication like UDP. It is a connection oriented, reliable transport protocol. TCP creates a virtual connection between two TCP clients to send data. In addition, TCP uses flow and error control mechanisms at the transport level.

TCP Operations:

Various services and operations of TCP are as follows:

Process to Process Communication: Like UDP, TCP provides process-to-process communication using port numbers.

Stream Delivery Service: TCP is a stream-oriented protocol. It allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes. TCP creates an environment in which the two processes seem to have a dedicated connection that carries their data across the internet. For flow control, TCP uses sending and receiving buffer that provides some storage for data packets in case of overflow. This prevents the loss of packets by synchronizing the flow rate.

Full-Duplex Communication: TCP offers full-duplex services in which data can flow in both directions at the same time. Each TCP then has sending and receiving buffer, and segments move in both directions.

Connection-Oriented Service: When a process at site A wants to send and receive data from another process at site B, the following occurs:

- The two TCPs establish a connection between them.
- Data are exchanged in both directions.
- The connection is terminated.

Note that this a virtual connection, not a physical connection.

Reliable Service: TCP is a reliable transport protocol. It uses an acknowledgement mechanism to check the safe arrival of data. This is possible due to efficient error control mechanisms.

TCP Features and Characteristics:

To support the services of TCP, following are some features:

Numbering System: TCP keeps track of segments being transmitted or received. There are two fields called the sequence number and the acknowledgement number for numbering the bytes within the segments and acknowledgements respectively.

Flow control: TCP provides flow control mechanism. The receiver of the data controls the amount of data that are to be sent by the sender. This is done to prevent the receiver from being overloaded with data. The numbering system allows TCP to use a byte-oriented flow control.

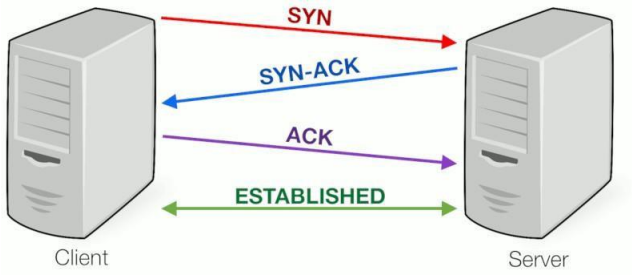
Error Control: To provide reliable service, TCP implements an error control mechanism. Although error control mechanism considers a segment as the unit of data for error detection (loss or corrupted segments), error control is byte-oriented.

Congestion Control: TCP takes into account about the congestion in the network. The amount of data sent by a sender is not only controlled by the receiver (flow control), but is also determined by the level of congestion in the network.

Three-Way Handshaking:

Since TCP is a connection-oriented service, it requires three phases: connection establishment, data transfer, and connection termination.

The connection establishment in TCP is called three-way handshaking. The figure below shows the handshaking process.



Similarly, three-way handshaking can also be used for connection termination.

Key Differences Between TCP and UDP:

- TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol.
- The speed for TCP is slower while the speed of UDP is faster.
- TCP is reliable as it guarantees the data delivery while UDP is not reliable.
- TCP uses handshake protocol like SYN, SYN-ACK, ACK while UDP uses no handshake protocols.
- TCP does error checking and also makes error recovery, on the other hand, UDP performs error checking, but it discards erroneous packets.
- TCP has acknowledgment segments, but UDP does not have any acknowledgment segment.
- TCP is heavy-weight, and UDP is lightweight.
- Data packets arrive in order at the receiver in TCP while no sequencing in UDP.
- TCP doesn't support broadcasting while UDP does.
- TCP is used by HTTP, HTTPS, FTP, SMTP and TELNET while UDP is used by DNS, DHCP, SNMP, RIP and VoIP.

Connection Oriented Services:

A connection-oriented service needs an established connection between peers before data can be sent between the connected terminals. This method is often called a "reliable" network service. This handles real-time traffic more efficiently than connectionless protocols because data arrives in the same order as it was sent. Connection-oriented protocols are also less error-prone. There is a sequence of operation to be followed by the users of connection-oriented service.
These are:
1. Connection is established.
2. Information is sent.
3. Connection is released.

In connection-oriented service, we have to establish a connection before starting the communication. When connection is established, we send the message or the information and then we release the connection. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

Virtual Circuits:

- A virtual circuit (VC) is a means of transporting data over a packet switched computer network in such a way that it appears as though there is a dedicated physical layer link between the source and destination end systems of this data.
- In all major computer network architectures to date (Internet, ATM, frame relay, and so on), the network layer provides either a host-to-host connectionless service or a host-to-host connection service, but not both.
- Computer networks that provide only a connection-oriented service at the network layer are called **virtual-circuit** (VC) networks; computer networks that provide only a connectionless service at the network layer are called datagram networks.

- While the Internet is a datagram network, many alternative network architectures— including those of ATM and frame relay—are virtual-circuit networks and, therefore, use connections at the network layer. These network-layer connections are called **virtual circuits (VCs)**.

There are three identifiable phases in a virtual circuit: VC Setup, Data Transfer, VC Teardown

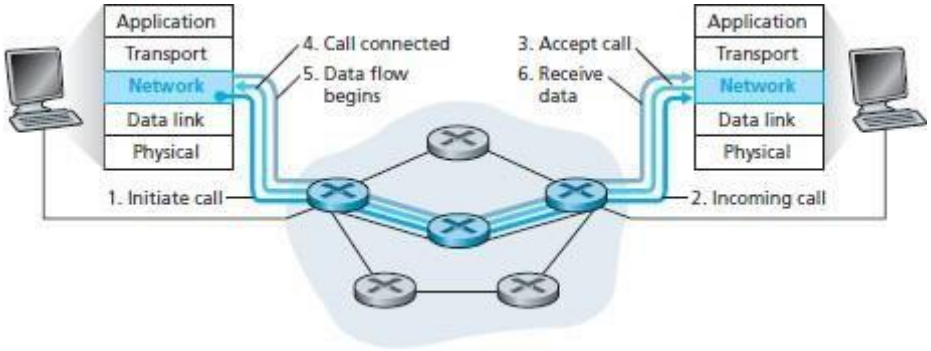


Fig: Virtual Circuit Setup

Connection less Services:

Connectionless service means that a terminal or node can send data packets to its destination without establishing a connection to the destination. A session connection between the sender and the receiver is not required, the sender just starts sending the data. The message or datagram is sent without prior arrangement, which is less reliable but faster transaction than a connection-oriented service. This works because of error handling protocols, which allow for error correction like requesting retransmission. It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.
LANs are actually connectionless systems with each computer able to transmit data packets as soon as it can access the network. The Internet is a large connectionless packet network in which all packet delivery is handled by Internet providers. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

The connectionless services at the network layer are called datagram networks. In a datagram network, each time an end system wants to send a packet, it stamps the packet with the address of the destination end system and then pops the packet into the network. As shown in Figure, there is no VC setup and routers do not maintain any VC state information (because there are no VCs).

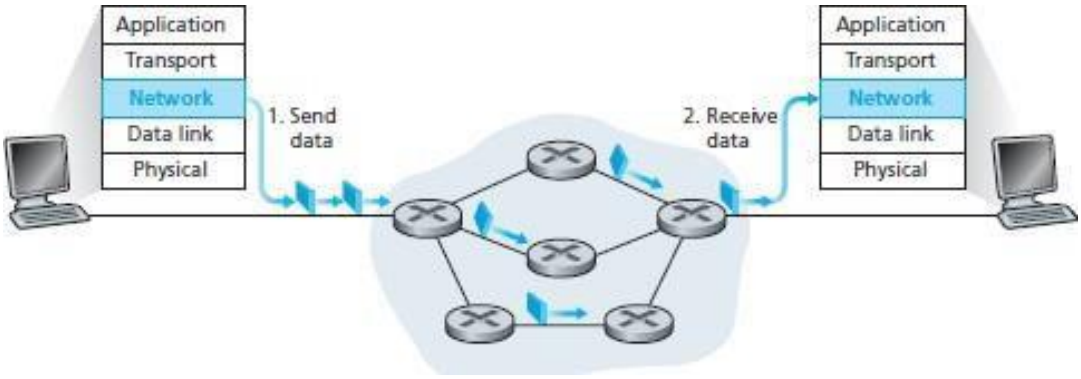


Fig: Datagram Network

Congestion Control:

Too many packets present in (a part of) the network causes packet delay and loss that degrades performance. This situation is called congestion. In other words, congestion in a network may occur if the load on the network, the number of packets sent to the network, is greater than the capacity of the network (the number of packets a network can handle).

The network and transport layers share the responsibility for handling congestion. Since congestion occurs within the network, it is the network layer that directly experiences it and must ultimately determine what to do with the excess packets. However, the most effective way to control congestion is to reduce the load that the transport layer is placing on the network. Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

Effects of Congestion:

- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation even worse

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.

The General Principles of Congestion Control are as follows:

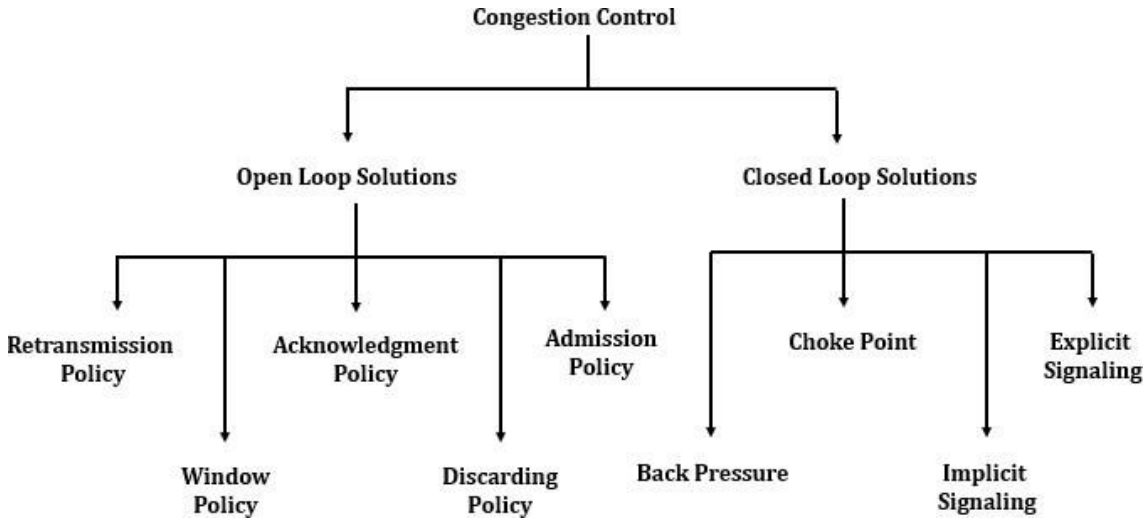
Open Loop Principle:

- attempt to prevent congestion from happening
- after system is running, no corrections made

Closed Loop Principle:

- monitor system to detect congestion

- pass information to where action is taken
- adjust system operation to correct problem



Open Loop Congestion Control:

In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination.

The list of policies that can prevent congestion are:

Retransmission Policy:

It is the policy in which retransmission of the packets are taken care. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network.

To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency

Window Policy

The type of window at the sender side may also affect the congestion. Several packets in the Go-back-n window are resent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and making it worse.

Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.

Acknowledgement Policy

Since acknowledgement are also the part of the load in network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment.

The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send an acknowledgment only if it has to send a packet or a timer expires.

Discarding Policy

A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discards the corrupted or less sensitive package and also able to maintain the quality of a message.

In case of audio file transmission, routers can discard fewer sensitive packets to prevent congestion and also maintain the quality of the audio file.

Admission Policy

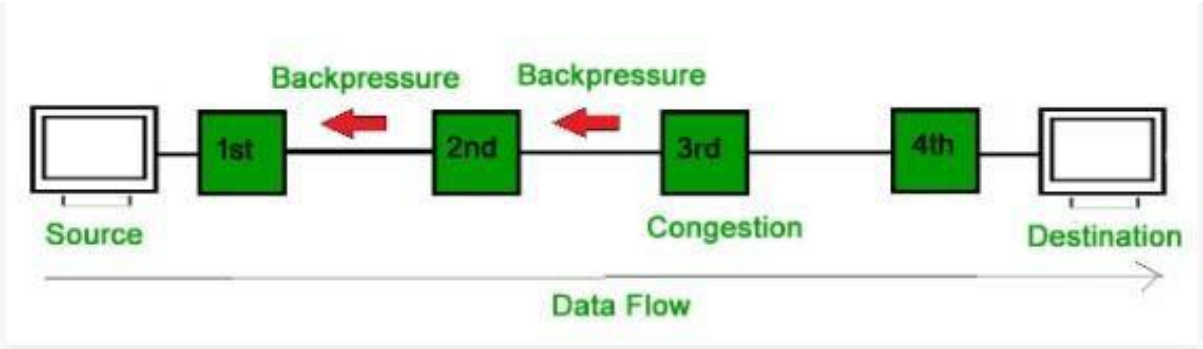
In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

Closed Loop Congestion Control

Closed-Loop congestion control mechanisms try to reduce effects of congestion after it happens.

Back Pressure:

Backpressure is a technique in which a congested node stops receiving packet from upstream node. This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow. The backpressure technique can be applied only to virtual circuit where each node has information of its above upstream node.

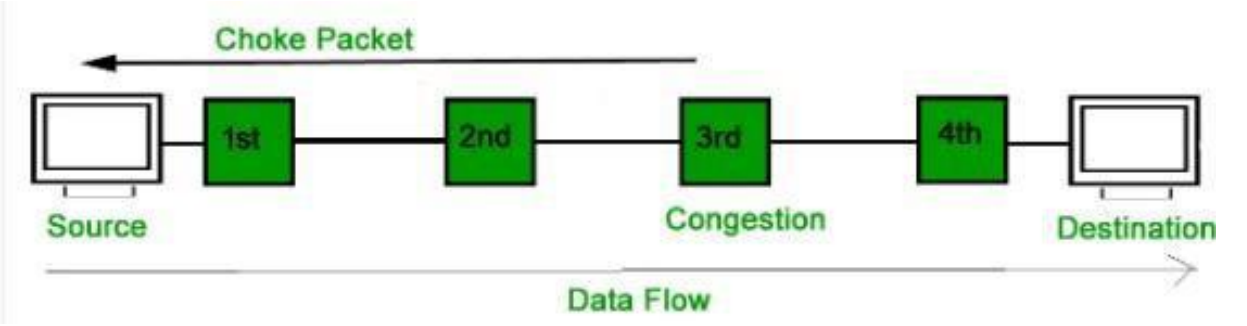


In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly, 1st node may get congested and informs the source to slow down.

Choke Packet:

Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitors its resources and the utilization at each of its output lines. whenever the resource utilization exceeds the threshold value

which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets have traveled are not warned about congestion.



Implicit Signaling:

In this method, there is no communication between congested node or nodes and the source. The source guesses that there is congestion somewhere in the network from other symptoms. For example, when source sends several packets and there is no acknowledgment for a while, one assumption is that network is congested and source should slow down.

Explicit Signaling:

In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating different packet as in case of choke packet technique.

Explicit signaling can occur in either forward or backward direction.

Forward Signaling: In forward signaling signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopts policies to prevent further congestion.

Backward Signaling: In backward signaling signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

TCP Congestion Control:

Congestion Control in TCP (Virtual-Circuit Subnet) is closed loop-based design for connection-oriented services which can be done during connection set up. The basic principle is that when setting up a virtual circuit, we have to make sure that congestion be avoided.

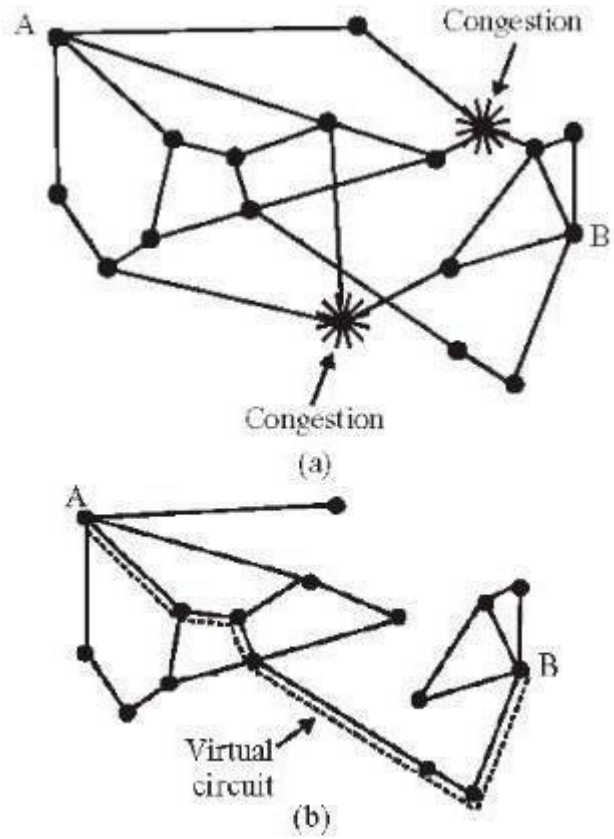
The following method is used for congestion control in TCP:

- Admission Control

- Once the congestion has been signaled, no newer virtual circuits can be set up until the problem has been solved.
- This type of approach is often used in normal telephone networks. When the exchange is overloaded, then no new calls are established.

- Another Approach: Alternative routes
  - To allow new virtual connections, route these carefully so that none of the congested router (or none of the problem area) is a part of this route i.e., to avoid the part of the network that is overloaded.
  - Yet another approach can be: To negotiate different parameters between the host and the network, when the connection is setup. During the setup time itself, Host specifies the volume and shape of traffic, quality of service, maximum delay and other parameters, related to the traffic it would be offering to the network. Once the host specifies its requirement, the resources needed are reserved along the path, before the actual packet follows.

    In the figure below, Normally when router A sets a connection to B, it would pass through one of the two congested routers, as this would result in a minimum-hop route. To avoid congestion, a temporary subnet is redrawn by eliminating congested routers. A virtual circuit can then be established to avoid congestion.



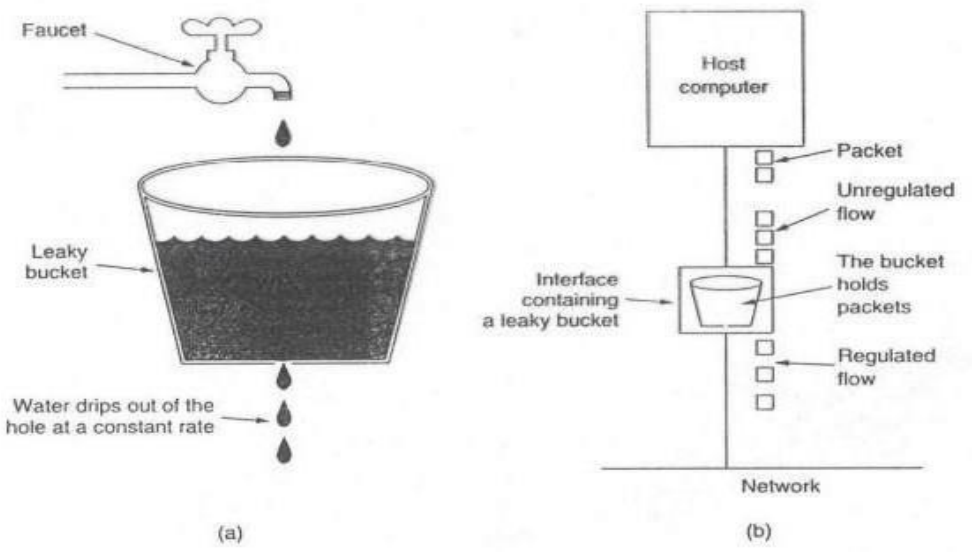
Traffic Shaping:

It is a mechanism to control the amount and the rate of the traffic sent to the network.

Two techniques can shape traffic: Leaky bucket and Token bucket.

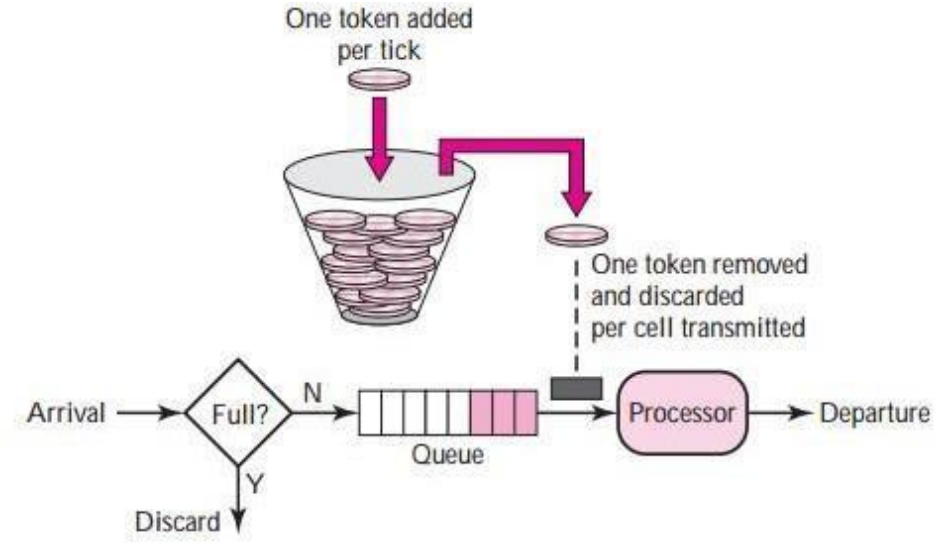
Leaky bucket algorithm:

- Each host is connected to the network by an interface containing a leaky bucket, a finite internal queue.
- If a packet arrives at the queue when it is full, the packet is discarded.
- In fact, it is nothing other than a single server queuing system with constant service time.



Token bucket algorithm:

- The leaky bucket holds tokens, generated by a clock at the rate of one token every T second.
- For a packet to be transmitted, it must capture and destroy one token.
- The token bucket algorithm allows idle hosts to save up permission to the maximum size of bucket n for burst traffic latter.



Parameter	Leaky Bucket	Token Bucket
Token Dependency	Token independent.	Dependent on Token.
Filled bucket for token	When bucket is full, data or packets are discarded.	If bucket is full, token are discard not packets.
Packet transmission	Leaky bucket sends packets at constant rate.	Token bucket can send large burst of packets at faster rate.
Condition for packet transmission	In Leaky bucket algorithm, Packets are transmitted continuously.	In Token bucket algorithm, Packets can only transmit when there is enough token.
Token saving	It does not save any token.	It saves token for the burst of packet transmission.
Restrictive Algorithm	Leaky bucket algorithm is more restrictive as compared to Token bucket algorithm.	Token bucket algorithm is less restrictive as compared to Leaky bucket algorithm.

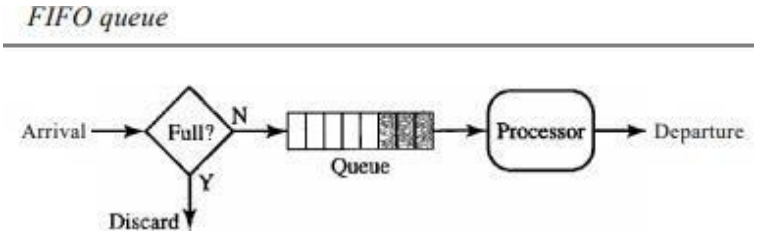
Queuing Techniques for Scheduling:

QoS traffic scheduling is a scheduling methodology of network traffic based upon QoS (Quality of Service).

Packets from different flows arrive at a switch or router for processing. A good scheduling technique treats the different flows in a fair and appropriate manner. Several scheduling techniques are designed to improve the quality of service. Major scheduling techniques are: FIFO Queuing, Priority Queuing and Weight Fair Queuing.

FIFO Queuing:

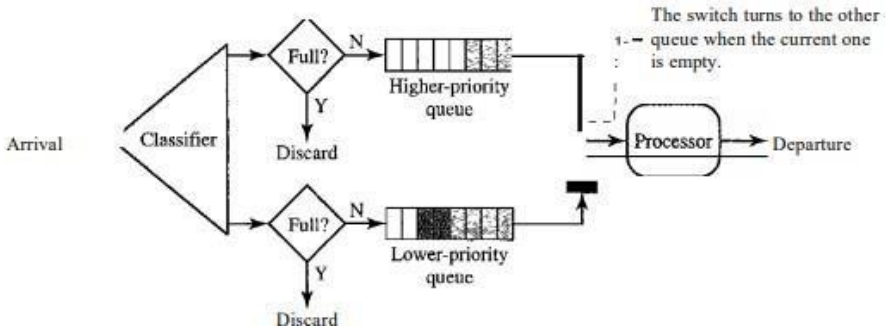
In first- in first-out (FIFO) queuing, packets wait in a buffer (queue) until the node (router or switch) is ready to process them. If the average arrival rate is higher than the average processing rate, the queue will fill up and new packets will be discarded. A FIFO queue is familiar to those who have had to wait for a bus at a bus stop.



Priority Queuing:

In priority queuing, packets are first assigned to a priority class. Each priority class has its own queue. The packets in the highest-priority queue are processed first. Packets in the lowest-priority queue are processed last. Note that the system does not stop serving a queue until it is empty.

Figure 24.17 *Priority queuing*

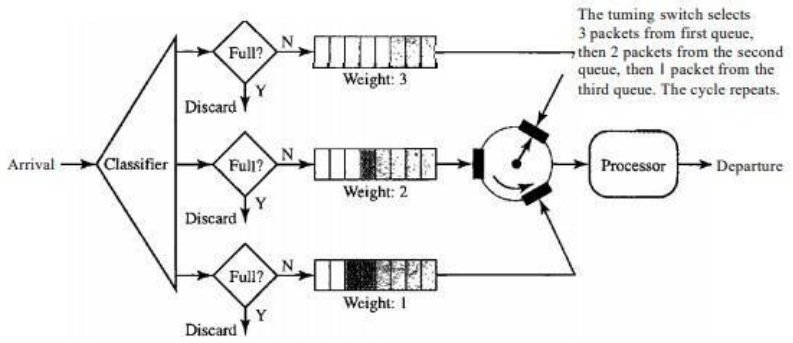


A priority queue can provide better QoS than the FIFO queue because higher priority traffic, such as multimedia, can reach the destination with less delay. However, there is a potential drawback. If there is a continuous flow in a high-priority queue, the packets in the lower-priority queues will never have a chance to be processed. This is a condition called starvation.

Weighted Fair Queuing:

A better scheduling method is weighted fair queuing. In this technique, the packets are still assigned to different classes and admitted to different queues. The queues, however, are weighted based on the priority of the queues; higher priority means a higher weight. The system processes packets in each queue in a round-robin fashion with the number of packets selected from each queue based on the corresponding weight. For example, if the weights are 3, 2, and 1, three packets are processed from the first queue, two from the second queue, and one from the third queue. If the system does not impose priority on the classes, all weights can be equal. In this way, we have fair queuing with priority.

Figure 24.18 *Weighted fair queuing*



Introduction to Ports and Sockets: (Port Addressing/Socket Addressing)

The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet. A system that sends nothing but data from one computer to another is not complete.

Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process.

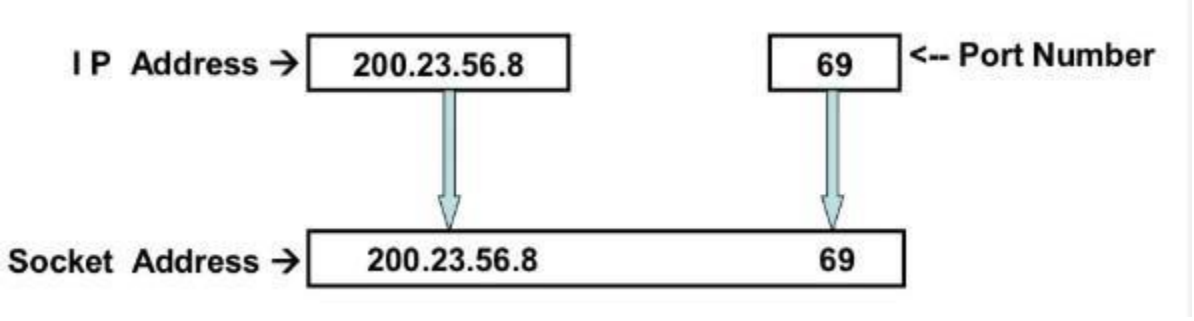
For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes.

In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a port address. A port address in TCP/IP is 16 bits in length.

Source and destination addresses are found in the IP packet, belonging to the network layer. A transport layer datagram or segment that uses port numbers is wrapped into an IP packet and transported by it.

The network layer uses the IP packet information to transport the packet across the network (routing). Arriving at the destination host, the host's IP stack uses the transport layer information (port number) to pass the information to the application.

Port Number	Assignment
21	File Transfer Protocol (FTP)
23	TELNET remote login
25	SMTP
80	HTTP
53	DNS



IP address and Port Number is combinedly called Socket Address that identifies the host along with the networking application running in the host.

A socket is one endpoint of a two-way communication link between two programs running on the network. A socket is bound to a port number so that the TCP layer can identify the application that data is destined to be sent to. An endpoint is a combination of an IP address and a port number.

Socket Programming:

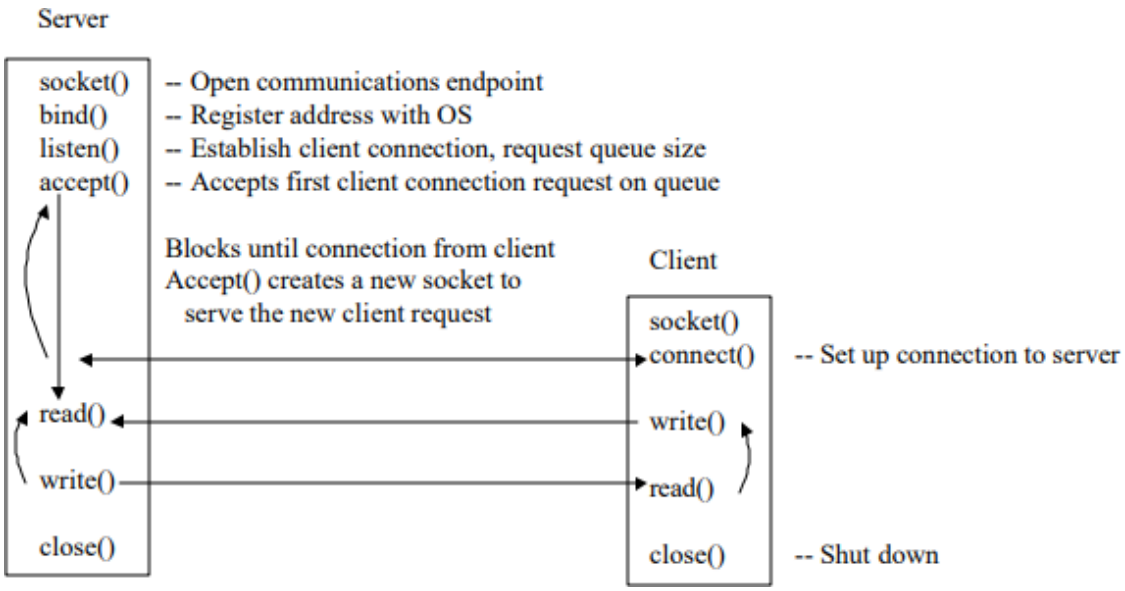
A typical network application consists of a pair of programs—a client program and a server program—residing in two different end systems. When these two programs are executed, a client process and a server process are created, and these processes communicate with each other by reading from, and writing to, sockets. When creating a network application, the developer's main task is therefore to write the code for both the client and server programs, called socket programming.

There are two types of network applications. One type is an implementation whose operation is specified in a protocol standard, such as an RFC or some other standards document; such an application is sometimes referred to as "open," since the rules specifying its operation are known to all. For such an implementation, the client and server programs must conform to the rules dictated by the RFC.

The other type of network application is a proprietary network application. In this case the client and server programs employ an application-layer protocol that has not been openly published in an RFC or elsewhere. A single developer (or development team) creates both the client and server programs, and the developer has complete control over what goes in the code. But because the code does not implement an open protocol, other independent developers will not be able to develop code that interoperates with the application.

During the development phase, one of the first decisions the developer must make is whether the application is to run over TCP or over UDP.

When a web page is opened, automatically a socket program is initialized to receive/send to the process. The socket program at the source communicates with the socket program at the destination machine with the associated source port/destination port numbers. When a web page is terminated, automatically the socket programs will be terminated.



The following sequence of events occur in the client-server application using socket programming for both TCP and UDP:

- The client reads a line of characters (data) from its keyboard and sends the data to the server.
- The server receives the data and converts the characters to uppercase.
- The server sends the modified data to the client.
- The client receives the modified data and displays the line on its screen.

BSD Socket API is the well-known socket programming API that defines a set of standard function calls made available at the application level.

BSD- Berkeley Software Distribution, API-Applications Programming Interface

These functions allow programmers to include Internet communications capabilities in their products. BSD Sockets generally relies upon client/server architecture. For TCP communications, one host listens for incoming connection requests. When a request arrives, the server host will accept it, at which point data can be transferred between the hosts. UDP is also allowed to establish a connection, though it is not required. Data can simply be sent to or received from a host. The Sockets API makes use of two mechanisms to deliver data to the application level: ports and sockets.

Unit 5: Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
Specific services provided by the application layer include the following:

- **Network virtual terminal.** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
- **File transfer, access, and management.** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **Mail services.** This application provides the basis for e-mail forwarding and storage.
- **Directory services**. This application provides distributed database sources and access for global information about various objects and services.

Web:

Web services are information exchange systems that use the Internet for direct application-to-application interaction. These systems can include programs, objects, messages, or documents. A web service is a collection of open protocols and standards used for exchanging data between applications or systems.

The World Wide Web (WWW) is a repository of information linked together from points all over the world. The WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet.

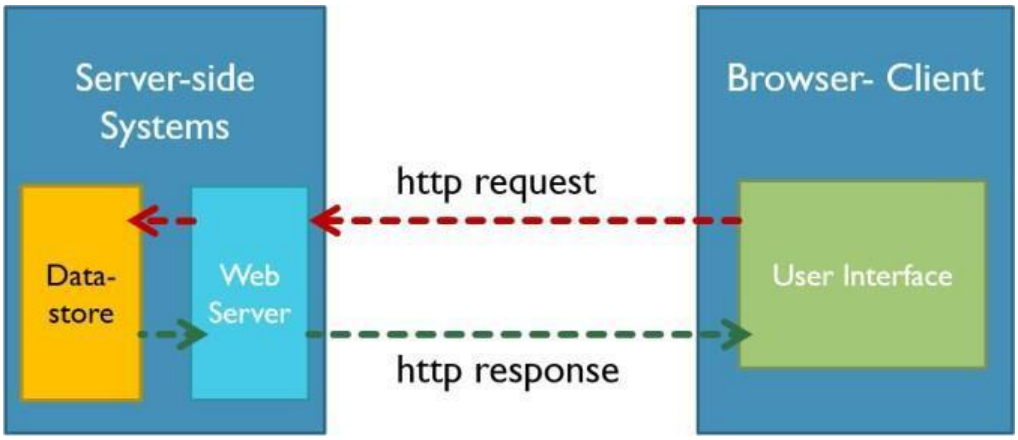
The World Wide Web (WWW), commonly known as the Web, is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs, such as https://www.example.com/), which may be interlinked by hypertext, and are accessible over the Internet. The resources of the WWW may be accessed by users by a software application called a web browser. The World Wide Web is what most people think of as the Internet. It is all the Web pages, pictures, videos and other online content that can be accessed via a Web browser. The Internet, in contrast, is the underlying network connection that allows us to send email and access the World Wide Web.

HTTP:

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

An HTTP session is a sequence of network request-response transactions. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a server (typically port 80, occasionally port 8080). An HTTP server listening on that port waits for a client's request message. Upon receiving the request, the server sends back a status and a message of its own. The body of this message is typically the requested resource, although an error message or other information may also be returned. HTTP is also called stateless protocol because the sessions between the HTTP browser

and HTTP client are not saved for later reference. The session is information is only valid until the session exists.



HTTP Methods and Their Meaning

Method	Meaning
GET	Read data
POST	Insert data
PUT or PATCH	Update data, or insert if a new id
DELETE	Delete data

lynda.com

HTTPS:

Hypertext Transfer Protocol Secure (HTTPS) is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit through a secure socket layer (SSL) or transport layer security (TLS) protocol connection.

HTTPS enables encrypted communication and secure connection between a remote user and the primary web server. HTTPS is primarily designed to provide enhanced security layer over the unsecured HTTP protocol for sensitive data and transactions such as billing details, credit card transactions and user login etc. HTTPS encrypts every data packet in transition using SSL or TLS encryption technique to avoid intermediary hackers and attackers to extract the content of the data; even if the connection is compromised.

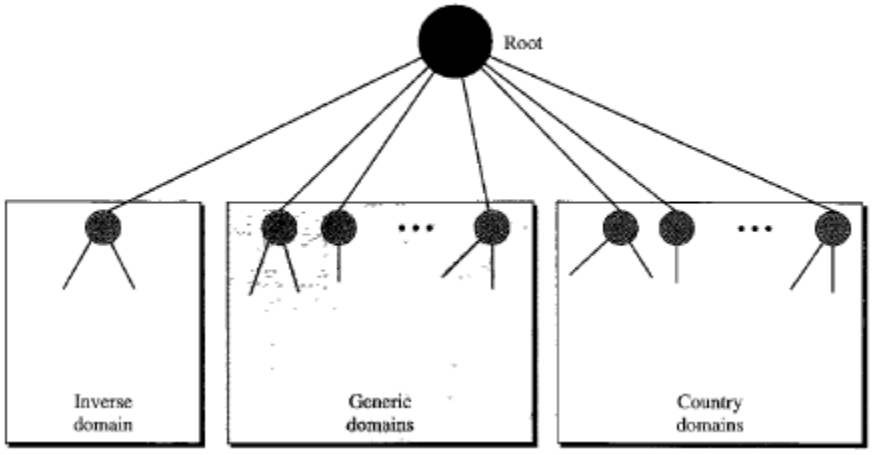
HTTPS is configured and supported by default in most web browsers and initiates a secure connection automatically if the accessed web server requests secure connection. HTTPS works in collaboration with certificate authorities that evaluates the security certificate of the accessed website.

Domain Naming System (DNS):

The domain name system (DNS) is a naming database in which internet domain names are located and translated into internet protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate a website. For example, if someone types example.com into a web browser, a server behind the scenes will map that name to the corresponding IP address. Facebook.com will be mapped to 66.220.144.0. Web browsing and most other internet activities rely on DNS to quickly provide the information necessary to connect users to remote hosts.

Although it's possible to enter an IP address into a web browser into order to get to a website, it's a lot easier to enter its domain name instead. However, computers, servers and other devices are unable to make heads or tails of domain names - they strictly rely on binary identifiers. The DNS's job, then, is to take domain names and translate them into the IP addresses that allow machines to communicate with one another. Every domain name has at least one IP address associated with it.

Figure 25.8 *DNS used in the Internet*



Generic domain labels

Com-commercial organizations

Gov- Government institutions

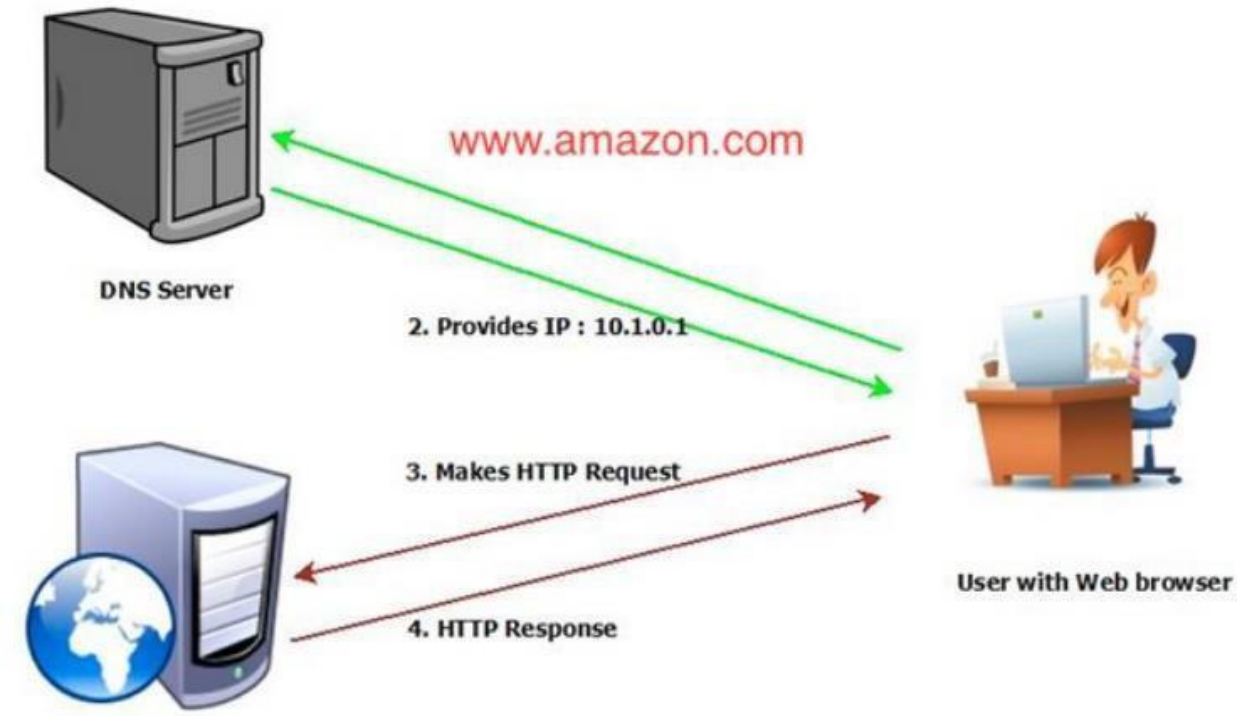
Net- network support centers

Org- nonprofit organizations

Name- personal names (individual) etc.

Inverse Domain: Used to map an ip address to a domain name.

Country Domains: .np, .in, .jp, .au, .uk, etc



There are three types of queries in the DNS system:

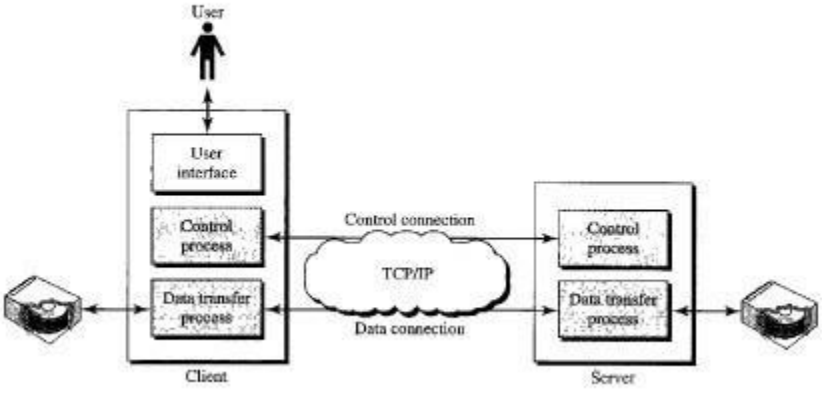
- **Recursive Query**
  In a recursive query, a DNS client provides a hostname, and the DNS Resolver “must” provide an answer—it responds with either a relevant resource record, or an error message if it can't be found. The resolver starts a recursive query process, starting from the DNS Root Server, until it finds the Authoritative Name Server that holds the IP address and other information for the requested hostname.
- **Iterative Query**
  In an iterative query, a DNS client provides a hostname, and the DNS Resolver returns the best answer it can. If the DNS resolver has the relevant DNS records in its cache, it returns them. If not, it refers the DNS client to the Root Server, or another Authoritative Name Server which is nearest to the required DNS zone. The DNS client must then repeat the query directly against the DNS server it was referred to.
- **Non-Recursive Query**
  A non-recursive query is a query in which the DNS Resolver already knows the answer. It either immediately returns a DNS record because it already stores it in local cache, or queries a DNS Name Server which is authoritative for the record, meaning it definitely holds the correct IP for that hostname. In both cases, there is no need for additional rounds of queries (like in recursive or iterative queries). Rather, a response is immediately returned to the client.

FTP:

File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.

FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for control information (commands and responses) and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, also known as anonymous FTP. FTP uses two well-known TCP ports: Port 21 for control connection and Port 20 for the data connection.

Figure 26.21 *FTP*



The control connection remains connected during the entire interactive FTP session. The data connection is opened and then closed for each file transfer. It opens each time commands that involve transferring files are used, and it closes when the file is transferred. In other words, when a user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred.

SFTP:

SFTP, which stands for SSH File Transfer Protocol, or Secure File Transfer Protocol, is a separate protocol packaged with SSH that works in a similar way but over a secure connection. The advantage is the ability to leverage a secure connection to transfer files and traverse the filesystem on both the local and remote system.

In almost all cases, SFTP is preferable to FTP because of its underlying security features and ability to rely on an SSH connection. FTP is an insecure protocol that should only be used in limited cases or on networks you trust.

SSH or Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH.

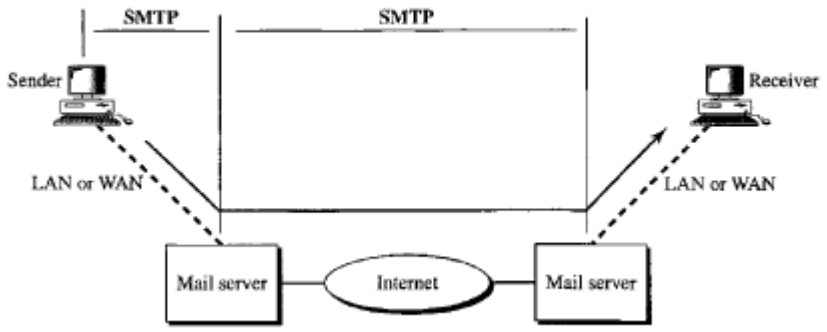
By default, SFTP uses the SSH protocol to authenticate and establish a secure connection. Because of this, the same authentication methods are available that are present in SSH.

SFTP also protects against password sniffing and man-in-the-middle attacks. It protects the integrity of the data using encryption and cryptographic hash functions, and authenticates both the server and the user.

Simple Mail Transfer Protocol (SMTP):

It is a standard protocol used for sending e-mail efficiently and reliably over the internet.

Figure 26.16 *SMTP range*



Key Points:

- SMTP is application level protocol.
- SMTP is connection-oriented protocol.
- SMTP is text-based protocol.
- It handles exchange of messages between e-mail servers over TCP/IP network.
- Apart from transferring e-mail, SMTP also provides notification regarding incoming mail.
- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

S.N.	Command Description
1	**HELLO** This command initiates the SMTP conversation.

2	**EHELLO** This is an alternative command to initiate the conversation. ESMTP indicates that the sender server wants to use extended SMTP protocol.
3	**MAIL FROM** This indicates the sender's address.
4	**RCPT TO** It identifies the recipient of the mail. In order to deliver similar message to multiple users this command can be repeated multiple times.
5	**SIZE** This command let the server know the size of attached message in bytes.
6	**DATA** The **DATA** command signifies that a stream of data will follow. Here stream of data refers to the body of the message.
7	**QUIT** This command is used to terminate the SMTP connection.
8	**VERFY** This command is used by the receiving server in order to verify whether the given username is valid or not.
9	**EXPN** It is same as VRFY, except it will list all the users name when it used with a distribution list.

IMAP:

IMAP stands for Internet Message Access Protocol. It is a standard protocol for accessing e-mail from the local server. IMAP is a client/server protocol in which e-mail is received and held by the Internet server. As this requires only a small data transfer, this works well even over a slow connection. Only if we request to read a specific email, message will it be downloaded from the server. We can also create and manipulate folders or mailboxes on the server, delete messages etc.

Key Points:

- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.

- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail. It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.
- It allows concurrent access to multiple mailboxes on multiple mail servers.

POP:

POP stands for Post Office Protocol. It is generally used to support a single client. There are several versions of POP but the POP 3 is the current standard.

Key Points

- POP is an application layer internet standard protocol.
- Since POP supports offline access to the messages, thus requires less internet usage time.
- POP does not allow search facility.
- In order to access the messages, it is necessary to download them.
- It allows only one mailbox to be created on server.
- It is not suitable for accessing non-mail data.

Overview of Application Server Concepts:

Application Server is a type of server designed to install, operate, and host applications. An application server is a program that resides on the server-side, and it's a server programmer providing business logic behind any application. This server can be a part of the network or the distributed network. Ideally, server programs are used to provide their services to the client program that either resides on the same machine or lies on a network.

Proxy Server:

In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server. The proxy server evaluates the request as a way to simplify and control their complexity.

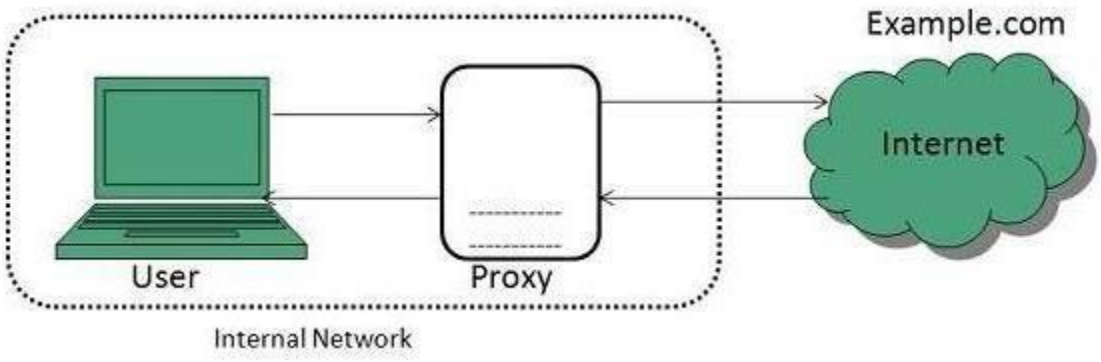
Thus, Proxy server is an intermediary server between client and the internet. Proxy servers allow to hide, conceal and make your network id anonymous by hiding your IP address.

Functionalities and Benefits of Proxy Servers:

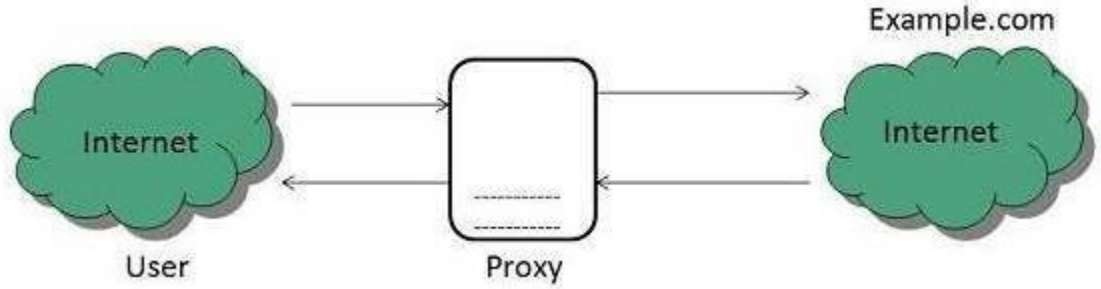
- Firewall, Network data Monitoring and filtering.
- Network connection sharing
- Data caching, Improving Performance
- Translation of Content
- Accessing Services Anonymously
- Enhanced Security

Types of Proxies:

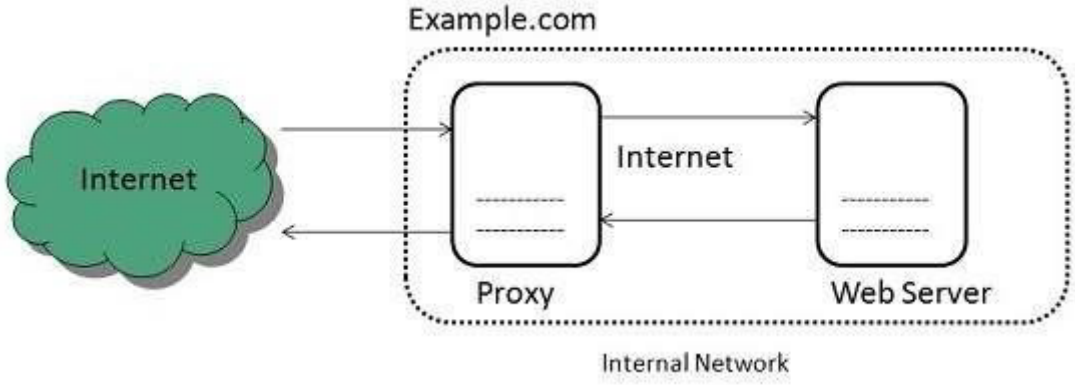
1. Forward Proxies: In this the client requests its internal network server to forward to the internet.



2. Open Proxies: Open Proxies helps the clients to conceal their IP address while browsing the web.



3. Reverse Proxies: In this the requests are forwarded to one or more proxy servers and the response from the proxy server is retrieved as if it came directly from the original Server.



Web Server:

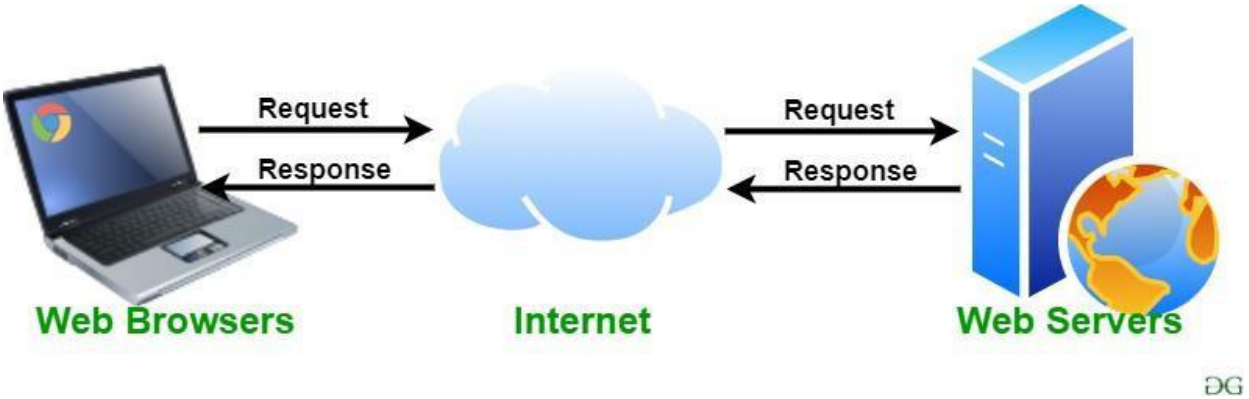
Web server can refer to either the hardware (the computer) or the software (the computer application) that helps to deliver Web content that can be accessed through the Internet. The most common use of web servers is to host websites, but there are other uses such as gaming, data storage or running enterprise applications. The primary function of a web server is to deliver web pages on the request to clients using the Hypertext Transfer Protocol (HTTP).

A user agent, commonly a web browser, initiates communication by making a request for a specific resource using HTTP and the server responds with the content of that resource or an error message if

unable to do so. The resource is typically a real file on the server's secondary memory, but this is not necessarily the case and depends on how the web server is implemented. While the primary function is to serve content, a full implementation of HTTP also includes ways of receiving content from clients.

Web server respond to the client request in either of the following two ways:

- Sending the file to the client associated with the requested URL.
- Generating response by invoking a script and communicating with database



Key Points:

- When client sends request for a web page, the web server search for the requested page if requested page is found then it will send it to client with an HTTP response.
- If the requested web page is not found, web server will the send an HTTP response: Error 404 Not found.
- If client has requested for some other resources then the web server will contact to the application server and data store to construct the HTTP response.

Mail Server:

A mail server (or email server) is a computer system that sends and receives email. In many cases, web servers and mail servers are combined in a single machine. However, large ISPs and public email services (such as Gmail and Hotmail) may use dedicated hardware for sending and receiving email.

In order for a computer system to function as a mail server, it must include mail server software. This software allows the system administrator to create and manage email accounts for any domains hosted on the server. For example, if the server hosts the domain name "example.com," it can provide email accounts ending in "@example.com."

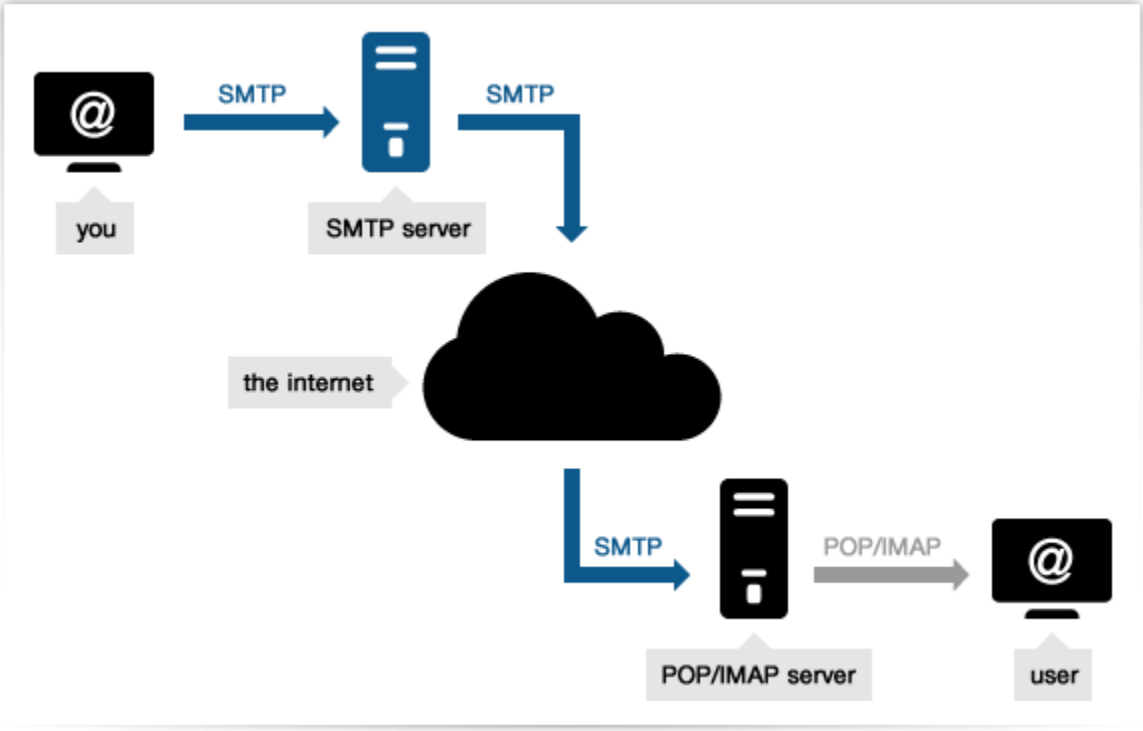
Mail servers send and receive email using standard email protocols. For example, the SMTP protocol sends messages and handles outgoing mail requests. The IMAP and POP3 protocols receive messages and are used to process incoming mail. When you log on to a mail server using a webmail interface or email client, these protocols handle all the connections behind the scenes.

Webmail: example.com/webmail

Email Client: Email applications and interfaces like Gmail, Outlook, Yandex etc.

Mail servers can be broken down into two main categories: outgoing mail servers and incoming mail servers.

- Outgoing mail servers are known as SMTP, or Simple Mail Transfer Protocol, servers.
- Incoming mail servers come in two main varieties.
    - POP3, or Post Office Protocol version 3, servers are best known for storing sent and received messages on PCs' local hard drives.
    - IMAP, or Internet Message Access Protocol, servers always store copies of messages on servers. Most POP3 servers can store messages on servers, too, which is a lot more convenient.



Network Management: SNMP

We can define network management as monitoring, testing, configuring, and troubleshooting network components to meet a set of requirements defined by an organization. These requirements include the smooth, efficient operation of the network that provides the predefined quality of service for users.

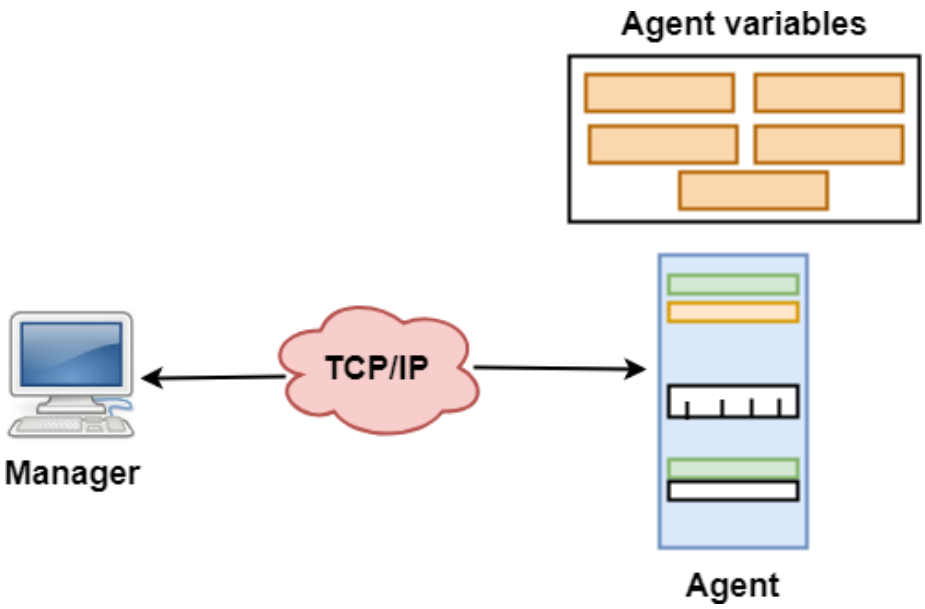
Network Management Functions:

- **Performance management** deals with monitoring and managing the various parameters that measure the performance of the network. Performance management is an essential function that enables a service provider to provide quality-of-service guarantees to their clients and to ensure that clients comply with the requirements imposed by the service provider.

- **Fault management** is the function responsible for detecting failures when they happen and isolating the failed component. The network also needs to restore traffic that may be disrupted due to the failure, but this is usually considered a separate function.
- **Configuration management** deals with the set of functions associated with managing orderly changes in a network. The basic function of managing the equipment in the network, connection management, network adaptation belongs to this category.
- **Security management** includes administrative functions such as authenticating users and setting attributes such as read and write permissions on a per-user basis

Simple Network Management Protocol (SNMP) is the application layer protocol that is used to perform the above-mentioned network management functions.

SNMP uses the concept of manager and agent. That is, a manager, usually a host, controls and monitors a set of agents, usually routers. A few manager stations control a set of agents. The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks.



Managers and Agents:

- A manager is a host that runs the SNMP client program while the agent is a router that runs the SNMP server program.
- Management of the internet is achieved through simple interaction between a manager and agent.
- The agent is used to keep the information in a database while the manager is used to access the values in the database. For example, a router can store the appropriate variables such as a number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.
- Agents can also contribute to the management process. A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manage.