UNIVERSITY OF GONDAR

COLLEGE OF INFORMATICS

DEPARTMENT OF INFORMATION SYSTEMS

DATA COMMUNICATIONS AND NETWORKING

History and overview of networking

Computer networking's past

A computer network is a collection of computers capable of transmitting, receiving, and exchanging voice, data, and video traffic. A network link may be established using either wired or wireless media. In today's world, where information technology is expanding at a rapid rate, computer networks are of paramount importance. As the evolution of technology is dependent on the system, including devices, the network and data transfer are crucial to the growth of information technology worldwide. ARPANET initiated networking decades ago.

ARPANET − Advanced Research Projects Agency Network − the granddad of Internet was a network established by the US Department of Defense (DOD). The work for establishing the network started in the early 1960s and DOD sponsored major research work, which resulted in development on initial protocols, languages and frameworks for network communication.

It had four nodes at University of California at Los Angeles (UCLA), Stanford Research Institute (SRI), University of California at Santa Barbara (UCSB) and University of Utah. On October 29, 1969, the first message was exchanged between UCLA and SRI. E-mail was created by Roy Tomlinson in 1972 at Bolt Beranek and Newman, Inc. (BBN) after UCLA was connected to BBN.

Internet ARPANET was expanded to connect the Department of Defense with US colleges conducting defense-related research. It included the majority of the country's major universities. When the University College of London (UK) and the Royal Radar Network (Norway) joined to the ARPANET, a network of networks was developed.

Stanford University's Vinton Cerf, Yogen Dalal, and Carl Sunshine invented the word "Internet" to characterize this network of networks. They also collaborated on protocols to facilitate information flow across the Internet. Transmission Control Protocol (TCP) is still the foundation of networking.

Telnet was the first commercial ARPANET adaption, launched in 1974. This also created the notion of Internet Service Provider (ISP). An ISP's primary function is to provide its clients with reliable Internet access at reasonable prices.

The World Wide Web With the commercialization of the internet, an increasing number of networks were built in various parts of the world. For communication over the network, each network employed a separate protocol. This prevented different networks from seamlessly integrating. Tim Berners-Lee

led a group of computer scientists at CERN in Switzerland in the 1980s to establish the World Wide Web, a seamless network of disparate networks (WWW).

The World Wide Web is a sophisticated network of websites and web pages linked together by hypertext links. A word or collection of words that links to another web page on the same or different website is referred to as hypertext. When the hypertext link is clicked, another web page is launched.

The transition from ARPANET to WWW was made possible by numerous new discoveries made by researchers and computer scientists all across the world. Here are a few examples of recent advancements.

In today's world, through the use of networks, we are connected like never before. People with ideas can communicate instantly with others to make those ideas a reality. News events and discoveries are known worldwide in seconds. Individuals can even connect and play games with friends separated by oceans and continents. Networks connect people and promote unregulated communication. Everyone can connect, share, and make a difference

The Network as a Platform (1.3)

The network has become a platform for distributing a wide range of services to end users in a reliable, efficient, and secure manner. Modern networks are constantly evolving to meet user demands. Early data networks were limited to exchanging character-based information between connected computer systems. Traditional telephone, radio, and television networks were maintained separately from data networks. In the past, every one of these services required a dedicated network, with different communication channels and different technologies to carry a particular communication signal. Each service had its own set of rules and standards to ensure successful communication.

Advances in technology are enabling us to consolidate these different kinds of networks onto one platform, referred to as the ***converged network***. Unlike dedicated networks, converged networks are capable of delivering voice, video streams, text, and graphics among many different types of devices over the same communication channel and network structure. Previously separate and distinct communication forms have converged onto a common platform. This platform provides access to a wide range of alternative and new communication methods that enable people to interact directly with each other almost instantaneously.

In a converged network, there are still many points of contact and many specialized devices, such as personal computers, phones, TVs, and tablet computers, but there is one common network infrastructure. This network infrastructure uses the same set of rules, agreements, and implementation standards.

Network Architecture Characteristics

Network Architecture is the way network services and devices are structured together to serve the connectivity needs of client devices and applications. The following are four basic network architectures characteristic.

1. Fault Tolerance. A fault-tolerant network is one that limits the number of devices that are impacted by faults, as the Internet will fail at times. It's built to recover quickly and utilize multiple paths between the source and destination, so if one faults, another steps in.

2. Scalability. A scalable network can expand quickly to support its new clients and applications without impacting the performance of the service being delivered to already existing users.

3. Quality of Service (QoS). The quality of service is a requirement of networks in the modern multi-cloud era. Services need to be dependable, measurable, and at times, guaranteed without fear of compromised quality, which includes the controls to manage congested network traffic and network bandwidth.

4. Security. A high-level of security is a non-negotiable for an impactful network architecture as it serves as one of the fundamentals. Security is addressed in the network infrastructure and in information security, which means physically securing a network is necessary and the information being transmitted, stored, and utilized in cloud-native environments.

Data communications are the exchange of data between two devices via some form of transmission medium 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).

A data communications system has five components

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.

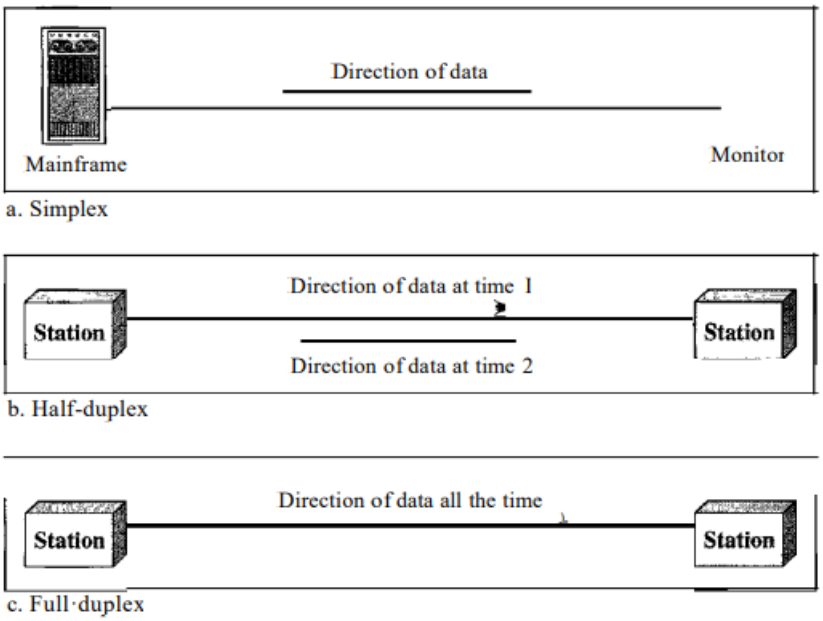
5. Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data communications system depends on four fundamental characteristics:

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. For example, let us assume that video packets are sent every 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure 1.1.



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 (see Figure 1.1a). 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 (see Figure 1.1b). 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 mode (also called duplex), both stations can transmit and receive simultaneously (see Figure 1.1c). In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions. 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.

What is communication?

TRANSMISSION MODES

Of primary concern when we are considering the transmission of data from one device to another is the wiring, and of primary concern when we are considering the wiring is the data stream. Do we send 1 bit at a time; or do we group bits into larger groups and, if so, how? The transmission of binary data across a link can be accomplished in either parallel or serial mode. In parallel mode, multiple bits are sent with each clock tick. In serial mode, 1 bit is sent with each clock tick. While there is only one way to send parallel data, there are three subclasses of serial transmission: asynchronous, synchronous, and isochronous.

Asynchronous Transmission is so named because the timing of a signal is unimportant. Instead, information is received and translated by agreed upon patterns. As long as those patterns are followed, the receiving device can retrieve the information without regard to the rhythm in which it is sent. Patterns are based on grouping the bit stream into bytes. Each group, usually 8 bits, is sent along the link as a unit. The sending system handles each group independently, relaying it to the link whenever ready, without regard to a timer.

Synchronous Transmission, the bit stream is combined into longer "frames," which may contain multiple bytes. Each byte, however, is introduced onto the transmission link without a gap between it and the next one. It is left to the receiver to separate the bit stream into bytes for decoding purposes. In other words, data are transmitted as an unbroken string of 1s and Os, and the receiver separates that string into the bytes, or characters, it needs to reconstruct the information.

Isochronous In real-time audio and video, in which uneven delays between frames are not acceptable, synchronous transmission fails. For example, TV images are broadcast at the rate of 30 images per second; they must be viewed at the same rate. If each image is sent by using one or more frames, there should be no delays between frames. For this type of application, synchronization between characters is not enough; the entire stream of bits must be synchronized. The isochronous transmission guarantees that the data arrive at a fixed rate.

Data can be analog or digital. The term analog data refers to information that is continuous; digital data refers to information that has discrete states. For example, an analog clock that has hour, minute, and

second hands gives information in a continuous form; the movements of the hands are continuous. On the other hand, a digital clock that reports the hours and the minutes will change suddenly from 8:05 to 8:06. Analog data, such as the sounds made by a human voice, take on continuous values. When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal. Digital data take on discrete values. For example, data are stored in computer memory in the form of Os and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.

Analog and Digital Signals Like the data they represent, signals can be either analog or digital. An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path. A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and O. The simplest way to show signals is by plotting them on a pair of perpendicular axes. The vertical axis represents the value or strength of a signal. The horizontal axis represents time. Figure 3.1 illustrates an analog signal and a digital signal. The curve representing the analog signal passes through an infinite number of points. The vertical lines of the digital signal, however, demonstrate the sudden jump that the signal makes from value to value.

Analog and digital transmission

A computer network is designed to send information from one point to another. This information needs to be converted to either a digital signal or an analog signal for transmission.

TRANSMISSION IMPAIRMENT'S

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are attenuation, distortion, and noise.

Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal. To show that a signal has lost or gained strength, engineers use the unit of the decibel. The decibel (dB) measures the relative strengths of two signals or one signal at two different points. Note that the decibel is negative if a signal is attenuated and positive if a signal is amplified.

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed (see the next section) through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration. In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same. Figure 3.28 shows the effect of distortion on a composite signal.

Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal. Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter. Induced noise comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna. Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna. Impulse noise is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on. Figure 3.29 shows the effect of noise on a signal.

Components of the network

End devices and their role

The network devices that people are most familiar with are called end devices, or hosts. These devices form the interface between users and the underlying communication network. Some examples of end devices are:

- ✓ Computers (work stations, laptops, file servers, web servers)
- ✓ Network printers
- ✓ VoIP phones
- ✓ Tele Presence endpoint
- ✓ Security cameras
- ✓ Mobile handheld devices (such as smartphones, tablets, PDAs, and wireless debit/credit card readers and barcode scanners)

A host device is either the source or destination of a message transmitted over the network, as shown in the animation. In order to distinguish one host from another, each host on a network is identified by an

address. When a host initiates communication, it uses the address of the destination host to specify where the message should be sent.

2.1.1. Intermediary Devices & their role

Intermediary devices interconnect end devices. These devices provide connectivity and work behind the scenes to ensure that data flows across the network. Intermediary devices connect the individual hosts to the network and can connect multiple individual networks to form an internetwork.

The intermediary devices for the management of the data flowing through them use various addressing systems such as IP Address, MAC Address, and Port Numbers (or Port Address) along with the information about the network interconnections. Further various types of switching in the computer networks determine the path that messages take through the network during the communication.

HUB

A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.

The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

Switch

A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

Router

A router is a device that connects two or more packet-switched networks or sub-networks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

- A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.
- A router works in a **Layer 3 (Network layer)** of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.

Modem

A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line. It is not integrated with the motherboard rather than it is installed on the PCI slot found on the motherboard. It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

Based on the differences in speed and transmission rate, a modem can be classified as Standard PC modem or Dial-up modem, Cellular Modem and Cable modem.

Repeater

Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters. Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss. So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN.

Bridges

Bridges are used to connect two sub networks that use interchangeable protocols. It combines two LANs to form an extended LAN. The main difference between the bridge and repeater is that the bridge has a penetrating efficiency. A bridge accepts all the packets and amplifies all of them to the other side. The bridges are intelligent devices that allow the passing of only selective packets from them. A bridge only passes those packets addressed from a node in one network to another node in the other network.

Network Media

Network media refers to the communication channels used to interconnect nodes on a computer network. Communication across a network is carried on a medium. The medium provides the channel over which the message travels from source to destination.

Different types of network media have different features and benefits. Not all network media has the same characteristics and is appropriate for the same purpose. The criteria for choosing network media are:

- The distance the media can successfully carry a signal
- The environment in which the media is to be installed
- The amount of data and the speed at which it must be transmitted
- The cost of the media and installation

In telecommunications, transmission media can be divided into two broad categories: guided and unguided. Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable. Unguided medium is free space.

GUIDED MEDIA

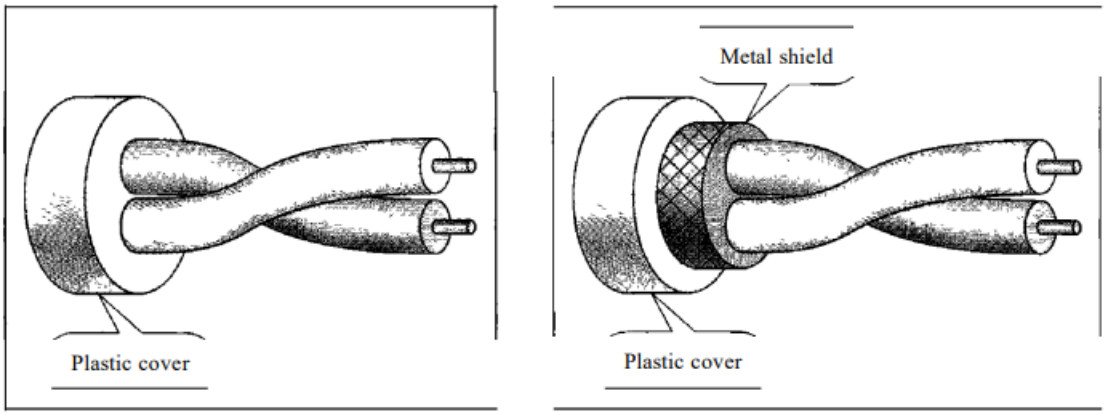
Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) 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.

Twisted pair cable

Twisted pair cables have two conductors that are generally made up of copper and each conductor has insulation. These two conductors are twisted together, thus giving the name twisted pair cables. One of the conductors is used to carry the signal and the other is used as a ground reference only. The receiver uses the difference of signals between these two conductors. The noise or crosstalk in the two parallel conductors is high but this is greatly reduced in twisted pair cables due to the twisting characteristic. In the first twist, one conductor is near to noise source and the other is far from the source but in the next twist the reverse happens and the resultant noise is very less and hence the balance in signal quality is maintained and the receiver receives very less or no noise. The quality of signal in twisted pair cables greatly depends upon the number of twists per unit length of the cable.

Unshielded Versus Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP). STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive. The following figure shows the difference between UTP and STP.



a.UTP b.STP

Connectors

The most common UTP connector is RJ45 (RJ stands for registered jack), as shown in Figure. The RJ45 is a keyed connector, meaning the connector can be inserted in only one way

RJ45 female

Rj 45 male

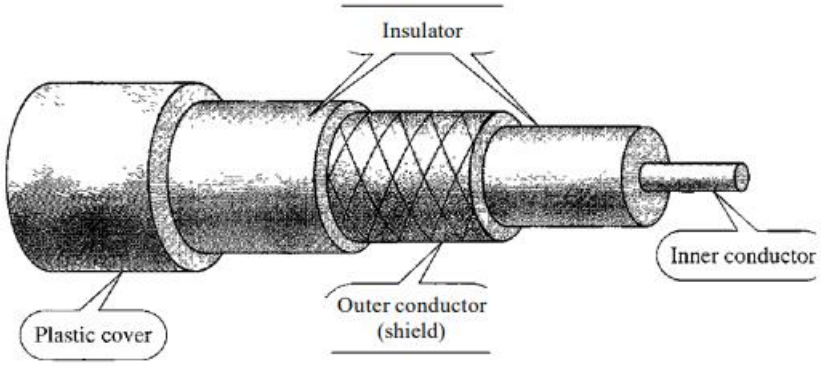
Categories

The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories. Categories are determined by cable quality, with 1 as the lowest and 7 as the highest. Each EIA category is suitable for specific uses.

Category	*Specification*	*Data Rate (Mbps)*	*Use*
I	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-llines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
SE	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk: and increases the data rate.	600	LANs

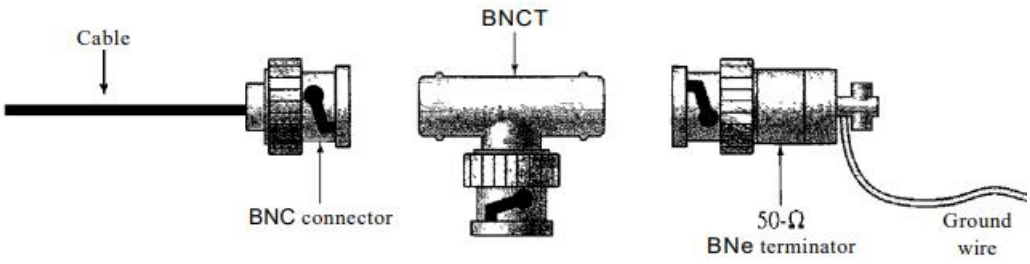
Coaxial Cable

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.



Coaxial Cable Connectors

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-Neill-Concelman (BNe), connector. Figure 7.8 shows three popular types of these connectors: the BNC connector, the BNC T connector, and the BNC terminator. The BNC connector is used to connect the end of the cable to a device, such as a TV set. The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device. The BNC terminator is used at the end of the cable to prevent the reflection of the signal.



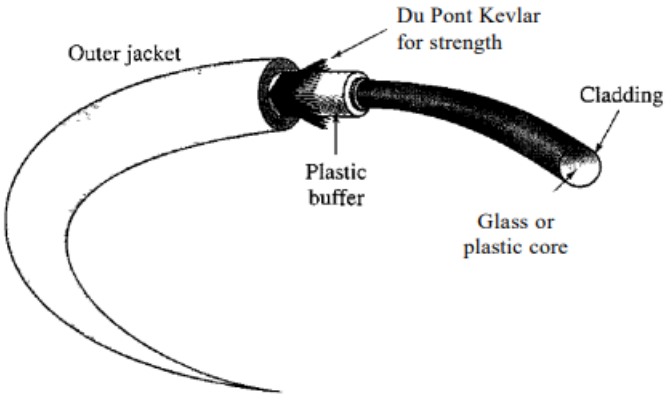
Fiber-Optic Cable

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 substance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction.

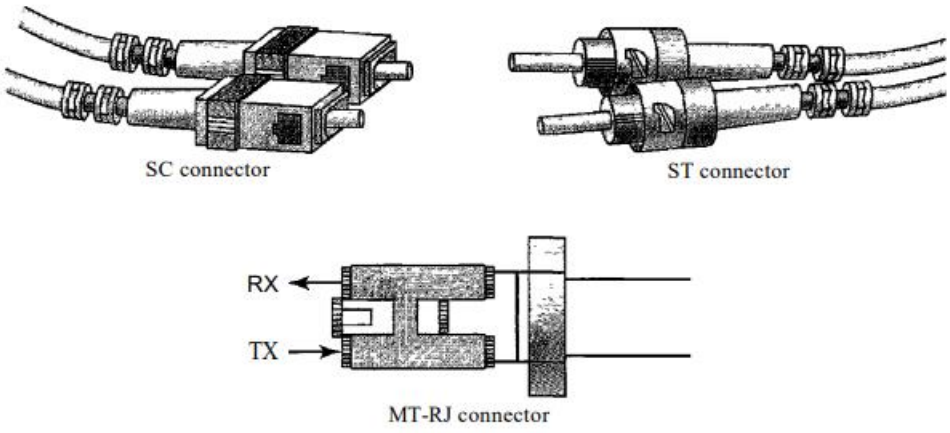
Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted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

The figure 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.



Fiber-Optic Cable Connectors

There are three types of connectors for fiber-optic cables, as shown in Figure. The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system. The straight-tip (ST) connector is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC. MT-RJ is a connector that is the same size as RJ45.



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.

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 (the layer of atmosphere where particles exist as ions) 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.

Chapter 3: Network Types

Categories of Networks

Today when we speak of networks, we are generally referring to two primary categories: local-area networks and wide-area networks. The category into which a network falls is determined by its size.

A local area network (LAN)

Is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers.

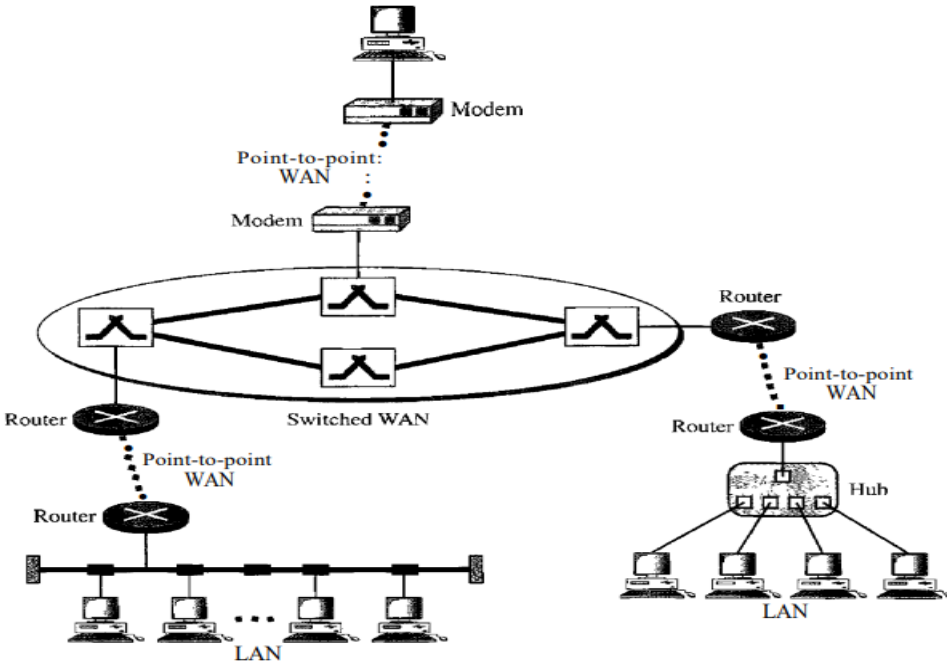
In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.

A wide area network (WAN)

Provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN. The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (lSP). This type of WAN is often used to provide Internet access.

Interconnection of Networks: Internetwork

Today, it is very rare to see a LAN, a MAN, or a LAN in isolation; they are connected to one another. When two or more networks are connected, they become an internetwork, or internet.



3.1. Peer to peer versus Server based Networks

What is a Client-Server Network?

A client-server network acts as a medium via which consumers access services and resources from a central computer, with the help of WAN (wide-area network) or LAN (local area network). The Client-server network is mainly used for game hosting, web services, and personal networks operated in organizations.

What is Peer to Peer Network?

A peer-to-peer network authorizes you to link two or more computers to a single system. It is basically a circulated application architecture that splits tasks between peers. In the networking world, a peer is a node that delivers the exact functionality as another. For example, two PCs in a network are peers.

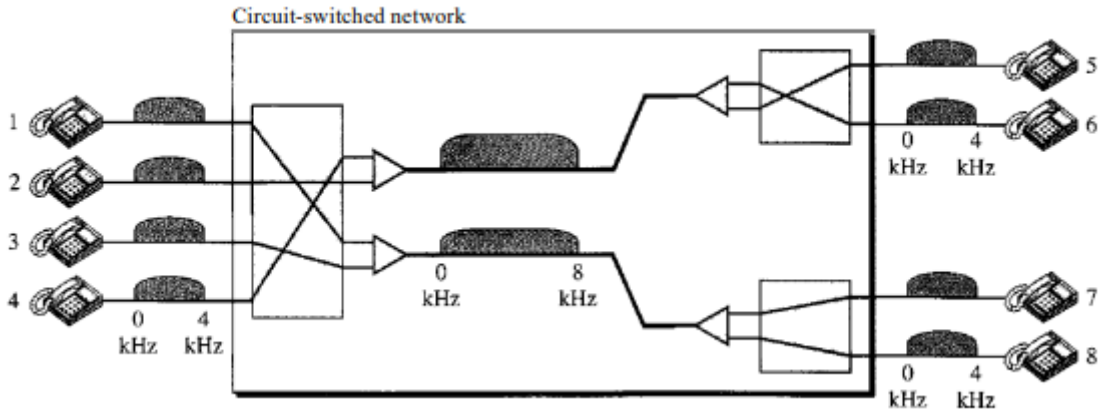
S.NO	Client-Server Network	Peer-to-Peer Network
1.	When it comes to a Client-Server Network, clients and servers are distinguished because of the distinctive servers and clients present.	When it comes to the Peer-to-Peer Network, both clients and servers are not distinguished.
2.	It majorly concentrates on sharing the information.	It majorly concentrates on the connectivity part.
3.	Here, we mainly prefer the centralised server to keep the data.	Here, every peer stores its own data.
4.	In the case of the Client-Server network, the server replies to the services which are asked by the client.	In the case of a Peer-to-Peer network, every node can accomplish both request and response.
5.	The Client-Server network is expensive as compared to the Peer-to-Peer network.	The Peer-to-Peer network is affordable as compared to the Client-Server network.
6.	They are a more stable network form.	They are comparatively less stable.
7.	These can be used both in small and large networks.	It is mostly preferred for short networks.

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 (a mesh topology) or between a central device and every other device (a star topology). These methods, however, are impractical and wasteful when applied to very large networks. The number and length of the links require too much infrastructure to be cost-efficient, and the majority of those links would be idle most of the time. Other topologies employing multipoint connections, such as a bus, are ruled out because 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. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing.

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. A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels.

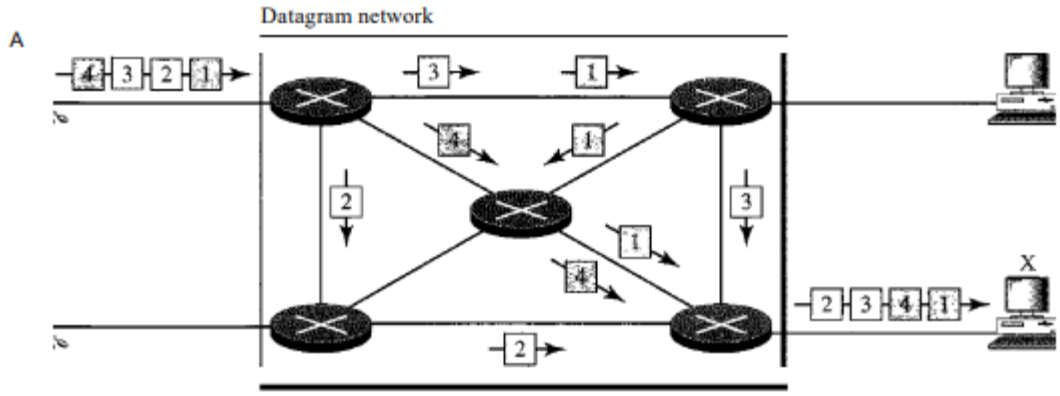


As shown in the above figure As a trivial example, let us use a circuit-switched network to connect eight telephones in a small area. Communication is through 4-kHz voice channels. We assume that each link uses FDM to connect a maximum of two voice channels. The bandwidth of each link is then 8 kHz. Figure 8.4 shows the situation. Telephone 1 is connected to telephone 7; 2 to 5; 3 to 8; and 4 to 6. Of course, the situation may change when new connections are made. The switch controls the connections.

- 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, as we will see shortly.

Packet switching (Datagram networks)

In data communications, we need to send messages from one end system to another. If the message is going to pass through a packet-switched network, it needs to be divided into packets of fixed or variable size. The size of the packet is determined by the network and the governing protocol. 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-served 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. As with other systems in our daily life, this lack of reservation may create delay.



In this example, all four packets (or 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. In most protocols, it is the responsibility of an upper-layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application.

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

Network cabling and topologies

The term ***topology*** *refers to the way in which a network is laid out physically.* Two 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.

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 nodes, 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 duplex-mode links. To accommodate that many links, every device on the network must have n - 1 input/output (VO) ports to be connected to the other n - 1 stations.

$$n(n -1) /2$$

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 . A star topology is less expensive than a mesh topology.

The star topology is used in local-area networks (LANs).

Bus Topology

The preceding examples all describe point-to-point connections. A bus topology, on the other hand, 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.

Ring Topology

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. 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.

Topology	Advantage	Disadvantage
Mesh	- use of dedicated links (carry its own data load) - If one link becomes unusable, it does not incapacitate the entire system - privacy or security since every message travel along a dedicated line, only the intended recipient sees it. - point-to-point links make fault identification and fault isolation easy	- requires more cabling and the number of I/O ports. (Every device must be connected to every other device) - difficult for installation and maintenance - hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.
Star	- easy to install and reconfigure - less cabling needs to be housed, and additions, moves, and deletions involve only one connection - easy fault identification and fault isolation - it easy to trouble shoot and manage the network. -A node can fail without affecting other nodes	- If the hub goes down, the whole system is dead. - more cable is required - expensive since it requires hub and more cables
Bus	-It is cheap -it uses small amount of cable. -More computers can be added without disruption.	- With a lot of users, the network will be slow as data has to travel through the same central cable. - Failure of the central cable will stop the network from working. - Difficult to trouble shoot because no central distribution points exist.
Ring	They are cheap to expand. The data flows around the network in one direction so it is fast. There is no reliance on a central computer. Easier to manage; easier to locate a defective node or cable problem Well-suited for transmitting signals over long distances on a LAN Handles high-volume network traffic Enables reliable communication	If there are a lot of users on the network, it could slow down as all the data is sent along a single line. If one computer in the ring stops working, the whole network stops. Requires more cable and network equipment at the start Not used as widely as bus topology

Chapter four & Five protocols

A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

- Syntax. The term syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
- Semantics. The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?
- Timing. The term timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

The rules

Protocols are necessary for effective communication and include:

- An identified sender and receiver
- Common language and grammar
- Speed and timing of delivery
- Confirmation or acknowledgment requirements

Protocols used in network communications also define:

• Message encoding, Message delivery options, Message Formatting and Encapsulation, Message Timing, Message Size.

Protocol suit and standards

As stated previously, a protocol suite is a set of protocols that work together to provide comprehensive network communication services. Protocols must be able to work with other protocols.

Protocol suites is A group of inter-related protocols necessary to perform a communication

Function in addition it works together to help solve a problem

The protocols are viewed in terms of layers either Higher Layers or Lower Layers- concerned with moving data and provide services to upper layers

There are several protocol suites.

Internet Protocol Suite or TCP/IP- The most common protocol suite and maintained by the Internet Engineering Task Force (IETF)

Open Systems Interconnection (OSI) protocols- Developed by the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU)

AppleTalk- Proprietary suite release by Apple Inc.

Novell NetWare- Proprietary suite developed by Novell Inc.

Standards

Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications. Data communication standards fall into two categories: de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation").

o De facto. Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology. o De jure. Those standards that have been legislated by an officially recognized body are de jure standards.

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies like International Organization for Standardization (ISO), International Telecommunication Union-Telecommunication Standards Sector (ITU-T), American National Standards Institute (ANSI), Institute of Electrical and Electronics Engineers (IEEE) and Electronic Industries Association (EIA).

Layered models

An *architectural model* provides a common frame of reference for discussing Internet communications. It is used not only to explain communication protocols but to develop them as well. It separates the functions performed by communication protocols into manageable layers stacked on top of each other. Each layer in the stack performs a specific function in the process of communicating over a network.

In an architectural model, a layer does not define a single protocol--it defines a data communication function that may be performed by any number of protocols. Because each layer defines a function, it can contain multiple protocols, each of which provides a service suitable to the function of that layer.

Every protocol communicates with its peer. A *peer* is an implementation of the same protocol in the equivalent layer on a remote computer. Peer-level communications are standardized to ensure that successful communications take place. Theoretically, each protocol is only concerned with communicating to its peer--it does not care about the layers above or below it.

A dependency, however, exists between the layers. Because every layer is involved in sending data from a local application to an equivalent remote application, the layers must agree on how to pass data between themselves on a single computer. The upper layers rely on the lower layers to transfer the data across the underlying network.

TCP/IP model

The name TCP/IP refers to a suite of data communication protocols. The name is misleading because TCP and IP are only two of dozens of protocols that compose the suite. Its name comes from two of the more important protocols in the suite: the *Transmission Control Protocol* (TCP) and the *Internet Protocol* (IP).

TCP/IP originated out of the investigative research into networking protocols that the Department of Defense (DoD) initiated in 1969. In 1968, the DoD Advanced Research Projects Agency (ARPA) began researching the network technology that is now called *packet switching*.

The original focus of this research was to facilitate communication among the DoD community. However, the network that was initially constructed as a result of this research, then called ARPANET, gradually became known as the Internet. The TCP/IP protocols played an important role in the development of the Internet. In the early 1980s, the TCP/IP protocols were developed. In 1983, they became standard protocols for ARPANET.

Because of the history of the TCP/IP protocol suite, it is often referred to as the *DoD protocol suite* or the *Internet protocol suite*.

TCP/IP model basically contains four layers

Network Access Layer

The design of TCP/IP hides the function of this layer from users--it is concerned with getting data across a specific type of physical network (such as Ethernet, Token Ring, etc.). This design reduces the need to rewrite higher levels of a TCP/IP stack when new physical network technologies are introduced (such as ATM and Frame Relay).

The functions performed at this level include encapsulating the IP datagrams into *frames* that are transmitted by the network. It also maps the IP addresses to the physical addresses used by the network. One of the strengths of TCP/IP is its addressing scheme, which uniquely identifies every computer on the network. This IP address must be converted into whatever address is appropriate for the physical network over which the datagram is transmitted.

Data to be transmitted is received from the internetwork layer. The network access layer is responsible for routing and must add its routing information to the data. The network access layer information is added in the form of a header, which is appended to the beginning of the data.

In Windows NT, the protocols in this layer appear as NDIS drivers and related programs. The modules that are identified with network device names usually encapsulate and deliver the data to the network, while separate programs perform related functions such as address mapping.

Internetwork Layer

The best-known TCP/IP protocol at the internetwork layer is the *Internet Protocol (*IP*),* which provides the basic packet delivery service for all TCP/IP networks. In addition to the physical node addresses used at the network access layer, the IP protocol implements a system of logical host addresses called IP addresses. The IP addresses are used by the internetwork and higher layers to identify devices and to perform internetwork routing. The Address Resolution Protocol (ARP) enables IP to identify the physical address that matches a given IP address.

IP is used by all protocols in the layers above and below it to deliver data, which means all TCP/IP data flows through IP when it is sent and received, regardless of its final destination.

Internet Protocol

IP is a *connectionless protocol*, which means that IP does not exchange control information (called a *handshake*) to establish an end-to-end connection before transmitting data. In contrast, a *connection-oriented protocol* exchanges control information with the remote computer to verify that it is ready to receive data before sending it. When the handshaking is successful, the computers are said to have established a *connection*. IP relies on protocols in other layers to establish the connection if connection-oriented services are required.

IP also relies on protocols in another layer to provide error detection and error recovery. Because it contains no error detection or recovery code, IP is sometimes called an *unreliable protocol*.

The functions performed at this layer are as follows:

- **Define the datagram, which is the basic unit of transmission in the Internet.** The TCP/IP protocols were built to transmit data over the ARPANET, which was a *packet switching network*. A *packet* is a block of data that carries with it the information necessary to deliver it--in a manner similar to a postal letter that has an address written on its envelope. A packet switching network uses the addressing information in the packets to switch packets from one physical network to another, moving them toward their final destination. Each packet travels the network independently of any other packet. The *datagram* is the packet format defined by IP.

- **Define the Internet addressing scheme.** IP delivers the datagram by checking the destination address in the header. If the destination address is the address of a host on the directly attached network, the packet is delivered directly to the destination. If the destination address is not on the local network, the packet is passed to a gateway for delivery. *Gateways* and *routers* are devices that switch packets between the different physical networks. Deciding which gateway to use is called *routing*. IP makes the routing decision for each individual packet.

- **Move data between the Network Access Layer and the Host-to-Host Transport Layer.** When IP receives a datagram that is addressed to the local host, it must pass the data portion of the datagram to the correct host-to-host transport layer protocol. This selection is done by using the *protocol number* in the datagram header. Each host-to-host transport layer protocol has a unique protocol number that identifies it to IP.

- **Route datagrams to remote hosts.** Internet gateways are commonly (and perhaps more accurately) referred to as IP routers because they use IP to route packets between networks. In traditional TCP/IP jargon, there are only two types of network devices: gateways and hosts. Gateways forward packets between networks and hosts do not. However, if a host is connected to more than one network (called a *multi-homed host*), it can forward packets between the networks. When a multi-homed host forwards packets, it acts like any other gateway and is considered to be a gateway.

- **Fragment and reassemble datagrams.** As a datagram is routed through different networks, it may be necessary for the IP module in a gateway to divide the datagram into smaller pieces. A datagram received from one network may be too large to be transmitted in a single packet on a different network. This condition only occurs when a gateway interconnects dissimilar physical networks.

Each type of network has a *maximum transmission unit (MTU)*, which is the largest packet it can transfer. If the datagram received from one network is longer than the other network's MTU, it is necessary to divide the datagram into smaller fragments for transmission. This division process is called *fragmentation*.

Internet Control Message Protocol

The *Internet Control Message Protocol* (ICMP) is part of the internetwork layer and uses the IP datagram delivery facility to send its messages. ICMP sends messages that perform the following control, error reporting, and informational functions for the TCP/IP protocol suite:

- **Flow control**. When datagrams arrive too quickly for processing, the destination host or an intermediate gateway sends an ICMP *source quench message* back to the sender. This message instructs the source to stop sending datagrams temporarily.
- **Detect unreachable destinations.** When a destination is unreachable, the computer detecting the problem sends a *destination unreachable message* to the datagram's source. If the unreachable destination is a network or host, the message is sent by an intermediate gateway. But if the destination is an unreachable port, the destination host sends the message.
- **Redirect routes.** A gateway sends the ICMP *redirect message* to tell a host to use another gateway, presumably because the other gateway is a better choice. This message can only be used when the source host is on the same network as both gateways.
- **Check remote hosts.** A host can send the ICMP *echo message* to see if a remote computer's IP is up and operational. When a computer receives an echo message, it sends the same packet back to the source host.

Host-to-Host Transport Layer

The protocol layer just above the internetwork layer is the *host-to-host layer*. It is responsible for end-to-end data integrity. The two most important protocols employed at this layer are the *Transmission Control Protocol* (TCP) and *User Datagram Protocol* (UDP).

TCP provides reliable, full-duplex connections and reliable service by ensuring that data is resubmitted when transmission results in an error (end-to-end error detection and correction). Also, TCP enables hosts to maintain multiple, simultaneous connections. When error correction is not required, UDP provides unreliable datagram service (connectionless) that enhances network throughput at the host-to-host transport layer.

Both protocols deliver data between the *application layer* and the *internetwork layer*. Applications programmers can choose the service that is most appropriate for their specific applications.

User Datagram Protocol

The *User Datagram Protocol* gives application programs direct access to a datagram delivery service, like the delivery service that IP provides. This direct access allows applications to exchange messages over the network with a minimum of protocol overhead.

UDP is an unreliable, connectionless datagram protocol. "Unreliable" merely means that the protocol has no technique for verifying that the data reached the other end of the network correctly. Within your computer, UDP will deliver data correctly.

Why do applications programmers choose UDP as a data transport service? A number of good reasons exist. If the amount of data being transmitted is small, the overhead of creating connections and ensuring reliable delivery may be greater than the work of retransmitting the entire data set. In this case, UDP is the most efficient choice for a host-to-host transport layer protocol.

Applications that fit a "query-response" model are also excellent candidates for using UDP. The response can be used as a positive acknowledgment to the query. If a response is not received within a certain time period, the application just sends another query. Still other applications provide their own techniques for reliable data delivery and do not require that service from the transport layer protocol. Imposing another layer of acknowledgment on any of these types of applications is redundant.

Transmission Control Protocol

Applications that require the host-to-host transport protocol to provide reliable data delivery use TCP because it verifies that data is delivered across the network accurately and in the proper sequence. TCP is a *reliable, connection-oriented, byte-stream* protocol.

Application Layer

The most widely known and implemented TCP/IP application layer protocols are listed below:

- **File Transfer Protocol (FTP).** Performs basic interactive file transfers between hosts.
- **Telnet.** Enables users to execute terminal sessions with remote hosts.
- **Simple Mail Transfer Protocol (SMTP).** Supports basic message delivery services.

- **HyperText Transfer Protocol (HTTP).** Supports the low-overhead transport of files consisting of a mixture of text and graphics. It uses a stateless, connection- and object-oriented protocol with simple commands that support selection and transport of objects between the client and the server.

In addition to widely known protocols, the application layer includes the following protocols:

- **Domain Name Service (DNS).** Also called *name service*; this application maps IP addresses to the names assigned to network devices.
- **Routing Information Protocol (RIP).** Routing is central to the way TCP/IP works. RIP is used by network devices to exchange routing information.
- **Simple Network Management Protocol (SNMP).** A protocol that is used to collect management information from network devices.
- **Network File System (NFS).** A system developed by Sun Microsystems that enables computers to mount drives on remote hosts and operate them as if they were local drives.

Some protocols, such as Telnet and FTP, can only be used if the user has some knowledge of the network. Other protocols, like RIP, run without the user even knowing that they exist.

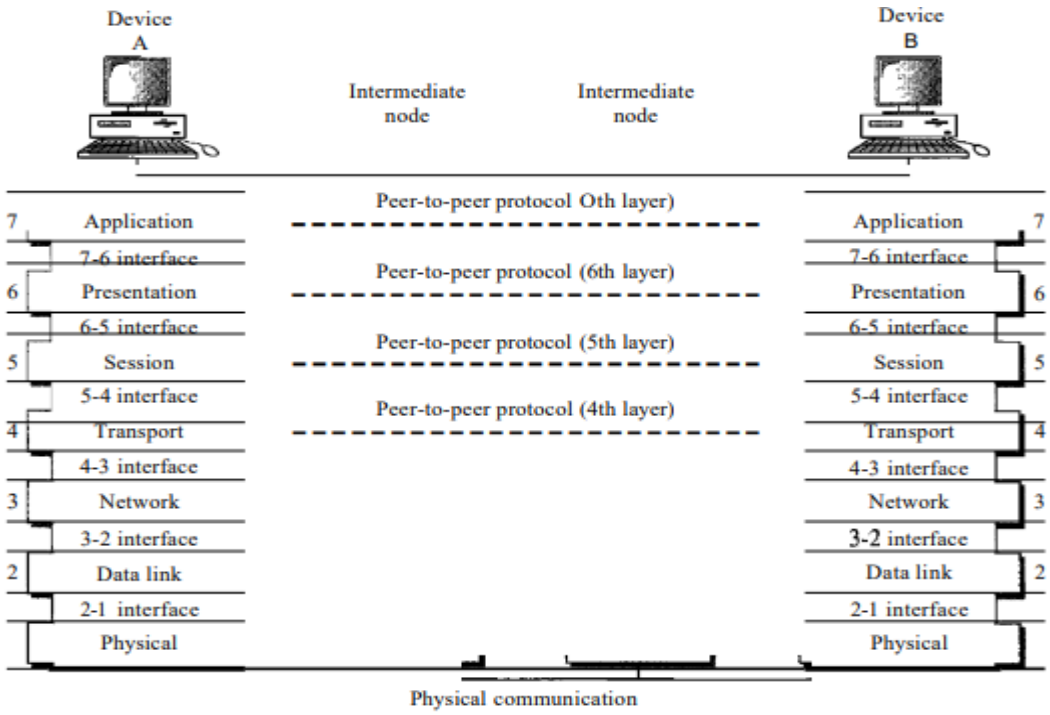
OSI reference model

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. ISO is the organization. OSI is the model.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network . An understanding of the fundamentals of the OSI model provides a solid basis for exploring data communications.

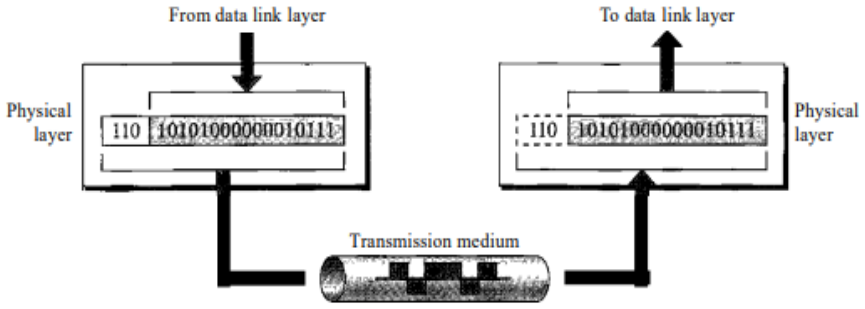
In developing the model, the designers distilled the process of transmitting data to its most fundamental elements. They identified which networking functions had related uses and collected those functions into discrete groups that became the layers. Each layer defines a family of functions distinct from those of the other layers. By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible. Most importantly, the OSI model allows complete interoperability between otherwise incompatible systems.



Layers in OSI model

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.



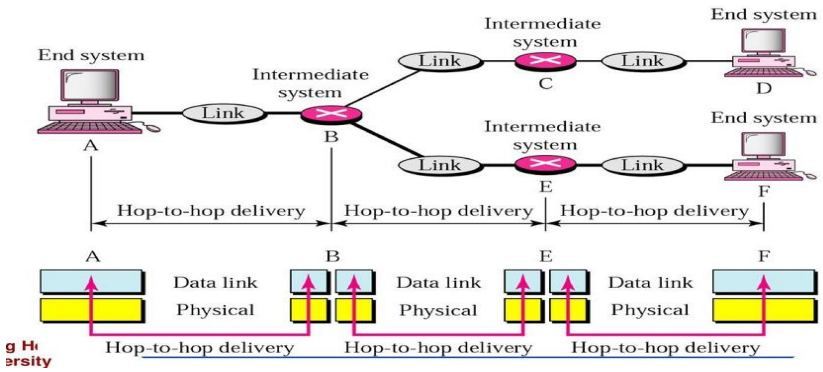
The physical layer is also concerned with the following:

- Physical characteristics of interfaces and medium. The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
- Representation of bits. The physical layer data consists of a stream of bits (sequence of 0 s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how 0 s and 1s are changed to signals).
- Data rate. The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts. o Synchronization of bits. The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.
- Line configuration. The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.
- Physical topology. The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).
- Transmission mode. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). Figure 2.6 shows the relationship of the data link layer to the network and physical layers.

Responsibilities of the data link layer include the following

- Framing. The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- Physical addressing. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
- Flow control. 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.
- Error control. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
- Access control. 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.
- The data link layer is responsible for moving frames from one hop (node) to the next.eg to send data from A to F , First, the data link layer at A sends a frame to the data link layer at B (a router). Then B to E finally E sends the frame to F.



The data link layer in the IEEE standard is divided into two sublayers: LLC and MAC. Logical Link Control (LLC

Network Layer

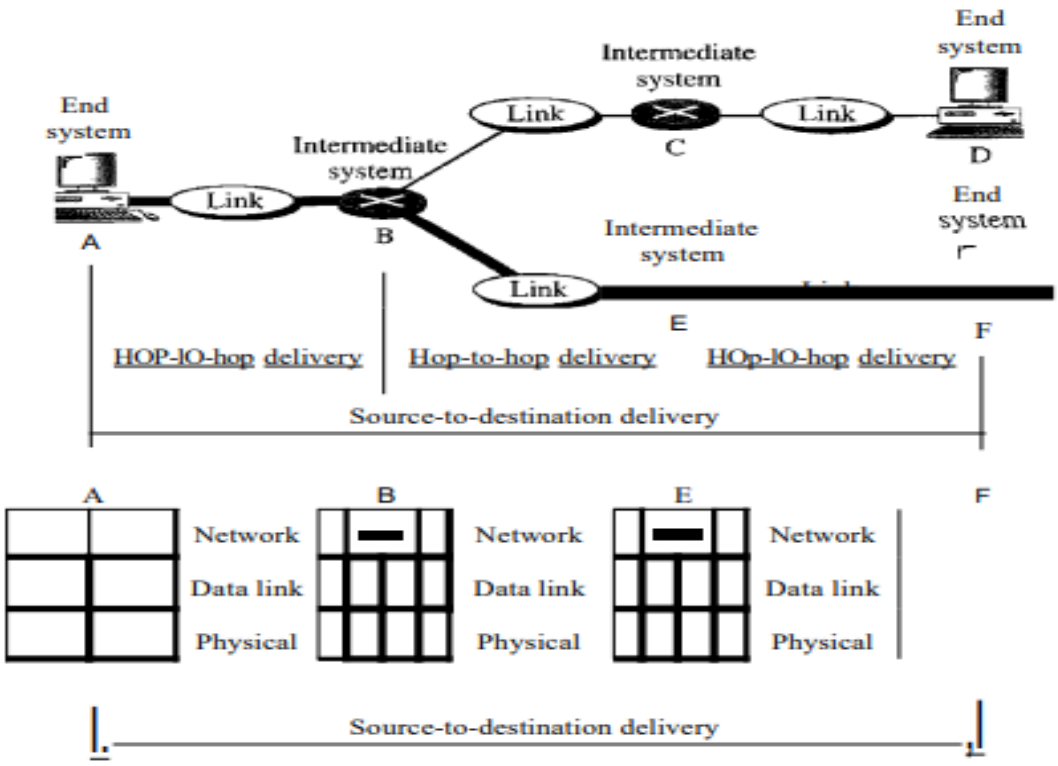
The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two

systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination. If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. Figure 2.8 shows the relationship of the network layer to the data link and transport layers.

Responsibilities of the network layer include the following:

- The network layer is responsible for the delivery of individual packets from the source host to the destination host.
- Logical addressing. The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver. We discuss logical addresses later in this chapter.
- Routing. When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism. Figure 2.9 illustrates end-to-end delivery by the network layer.

As the following figure shows, now we need a source-to-destination delivery. The network layer at A sends the packet to the network layer at B. When the packet arrives at router B, the router makes a decision based on the final destination (F) of the packet. As we will see in later chapters, router B uses its routing table to find that the next hop is router E. The network layer at B, therefore, sends the packet to the network layer at E. The network layer at E, in tum, sends the packet to the network layer at F.



Transport Layer

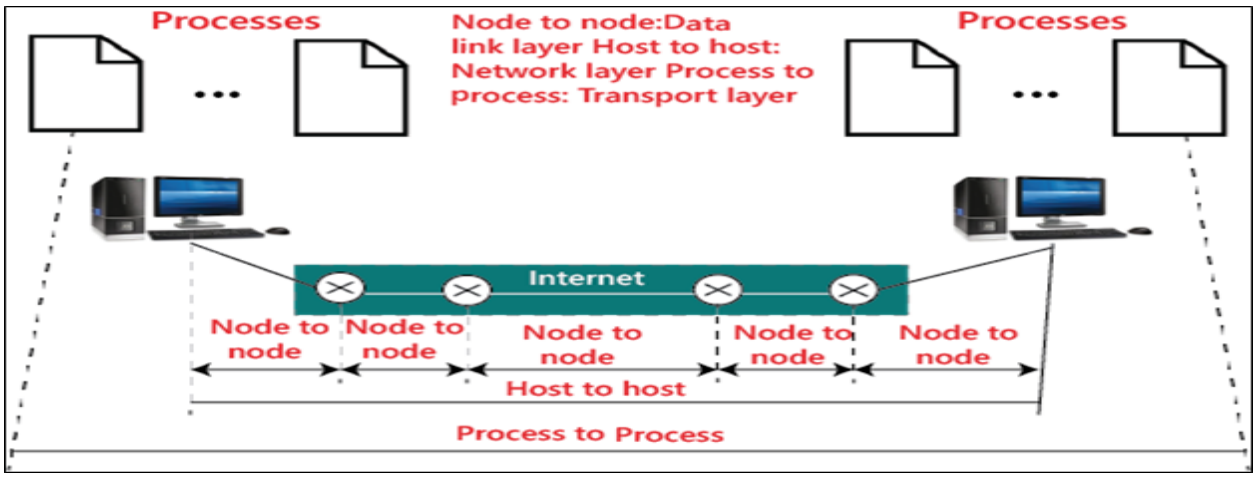
The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level. Figure 2.10 shows the relationship of the transport layer to the network and session layers.

Responsibilities of the transport layer include the following

- The transport layer is responsible for the delivery of a message from one process to another.
- Service-point addressing. Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to

the correct computer; the transport layer gets the entire message to the correct process on that computer.

- Segmentation and reassembly. A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
- Connection control. The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
- Flow control. Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- Error control. Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.



Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems. The session layer is responsible for dialog control and synchronization. Specific responsibilities of the session layer include the following:

- Dialog control. The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
- Synchronization. The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. Specific responsibilities of the presentation layer include the following:

- Translation. The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
- Encryption. To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- Compression. Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

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. Of the many application services available, the figure shows only three: XAOO (message-handling services), X.500 (directory

services), and file transfer, access, and management (FTAM). The user in this example employs XAOO to send an e-mail message.

Specific services provided by the application layer include the following:

- The application layer is responsible for providing services to the user.
- 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. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
- 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.

OSI vs TCP/IP model

TCP/IP and OSI are the two most widely use networking models for communication. There are some similarities and dissimilarities between them. One of the major difference is that OSI is a conceptual model which is not practically used for communication, whereas, TCP/IP is used for establishing a connection and communicating through the network.

OSI	**TCP/IP**
OSI represents **Open System Interconnection**.	TCP/IP model represents the Transmission Control Protocol / Internet Protocol.
OSI is a generic, protocol independent standard. It is acting as an interaction gateway between the network and the final-user.	TCP/IP model depends on standard protocols about which the computer network has created. It is a connection protocol that assigns the network of hosts over the internet.

OSI	TCP/IP
The OSI model was developed first, and then protocols were created to fit the network architecture's needs.	The protocols were created first and then built the TCP/IP model.
It provides quality services.	It does not provide quality services.
The OSI model represents defines administration, interfaces and conventions. It describes clearly which layer provides services.	It does not mention the services, interfaces, and protocols.
The protocols of the OSI model are better unseen and can be returned with another appropriate protocol quickly.	The TCP/IP model protocols are not hidden, and we cannot fit a new protocol stack in it.
It is difficult as distinguished to TCP/IP.	It is simpler than OSI.
It provides both connection and connectionless oriented transmission in the network layer; however, only connection-oriented transmission in the transport layer.	It provides connectionless transmission in the network layer and supports connecting and connectionless-oriented transmission in the transport layer.

Some familiar protocols

Internetworking Protocol (IP)

The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol-a best-effort delivery service. The term best effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees. IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination. The limited functionality of IP

should not be considered a weakness, however. IP provides bare-bones transmission functions that free the user to add only those facilities necessary for a given application and thereby allows for maximum efficiency.

Address Resolution Protocol The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known.

Reverse Address Resolution Protocol

The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

Internet Control Message Protocol the Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

Internet Group Message Protocol the Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

User Datagram Protocol the User Datagram Protocol (UDP) is the simpler of the two standard TCPIIP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

Transmission Control Protocol the (TCP) provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data. At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

Stream Control Transmission Protocol the Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

What is Protocol Data Unit (PDU) in networking?

A protocol data unit (PDU) is a single unit of information or a specific block of information transferred over a network. It is composed of protocol-specific control information and user data.

It is used in the reference of the OSI model, which defines the data state when it is transferred from one layer to another layer. In other words, we can say that protocol data unit (PDU) is used as a generic term for the block of information in the OSI model.

Encapsulation

For application data to travel uncorrupted from one host to another, header (or control data), which contains control and addressing information, is added to the data as it moves down the layers. The process of adding control information as it passes through the layered model is called encapsulation. Decapsulation is the process of removing the extra information and sending only the original application data up to the destination application layer. Each layer adds control information at each step. The generic term for data at each level is protocol data unit (PDU), but a PDU is different at each layer.

PDU Name	Layer
Data	Application layer PDU
Segment	Transport layer PDU
Packet	Internetwork layer PDU
Frame	Network access layer PDU
Bits	PDU used for the physical transmission of binary data over media

Sending and Receiving Process

The common task of sending an e-mail has many steps in the process. Using the proper terms for PDUs and the TCP/IP model, the process of sending the e-mail is as follows:

1. An end user, using an e-mail application, creates data. The application layer codes the data as e-mail and sends the data to the transport layer.

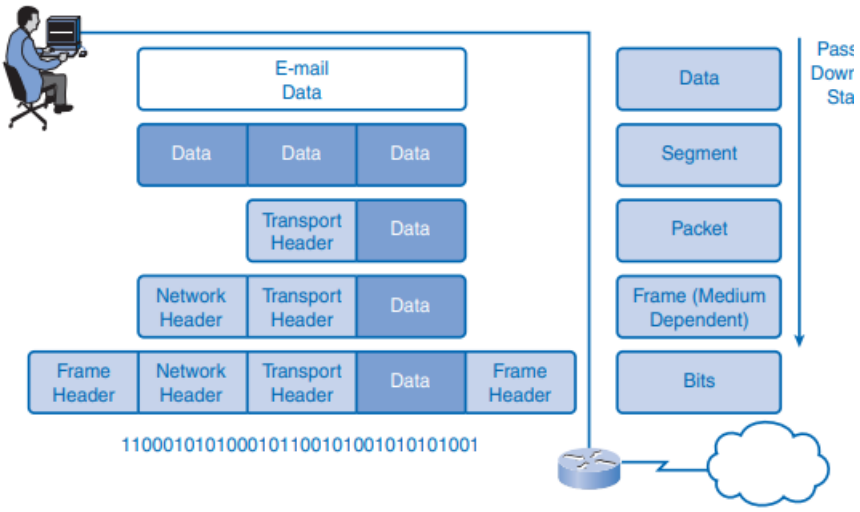
2. The message is segmented, or broken into pieces, for transport. The transport layer adds control information in a header so that it can be assigned to the correct process and all segments put into proper order at the destination. The segment is sent down to the internetwork layer.

3. The internetwork layer adds IP addressing information in an IP header. The segment is now an addressed packet that can be handled by routers en route to the destination. The internetwork layer sends the packet down to the network access layer.

4. The network access layer creates an Ethernet frame with local network physical address information in the header. This enables the packet to get to the local router and out to the web. The frame also contains a trailer with error-checking information. After the frame is created, it is encoded into bits and sent onto the media to the destination.

5. At the destination host, the process is reversed. The frame is DE capsulated to a packet, then to a segment, and then the transport layer puts all segments into the proper order.

6. When all data has arrived and is ready, it is sent to the application layer, and then the original application data goes to the receiver's e-mail application. The message is successful



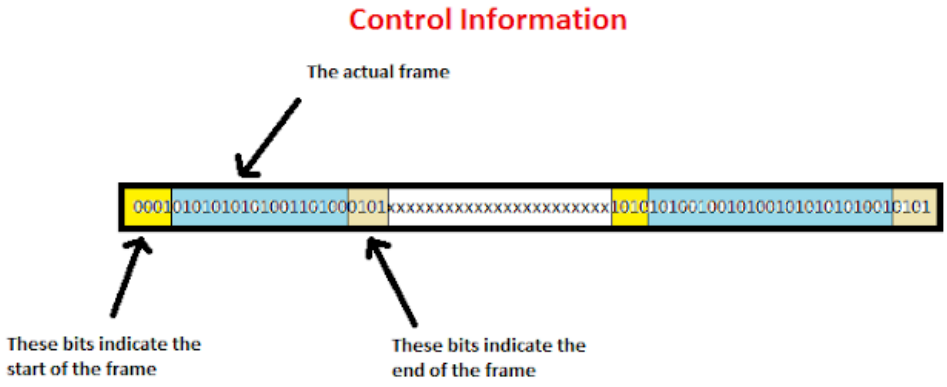
Encoding and signaling

Encoding and signaling are the main functions of layer one of the OSI reference model, physical layer. At the data-link layer, frames are in the form of bits (zeros and ones), but when they get down to the physical layer, they get turned into other formats that the physical layer understands ; in this case they are transformed into signals, because they need to be carried through cables and

In order for data to be recognized by both sender and receiver, it must be put in a specific order, or grouped, or encoded into patters. Devices must adhere to some rules when encoding data so that when it is received at the destination, it would be easily understandable by means of being subjected to the same rules, or decoding process. Thus, data is accumulated at the data-link layer as a frame, encoded

into patterns recognized by layer 1 devices, travels as signals onto media (e.g. cables, wireless), then received by the layer 1 of the destination and decoded so as to be handed up to the upper layer as a frame again.

In addition to grouping data bits into patterns, encoding has got another function which is control information. As you know, a cable, on which bits in the form of signals are transmitted, is busy with signals containing zeros and ones, and to distinguish between what bits are the actual traveled data and what bits are non-wanted noise is very difficult; so a method to tell the difference is required. For that reason, control information is utilized. This information is in the form of zeros and ones that indicate where a frame start and where the frame ends. The following figure clarifies how frames are distinguished from other extra bits.



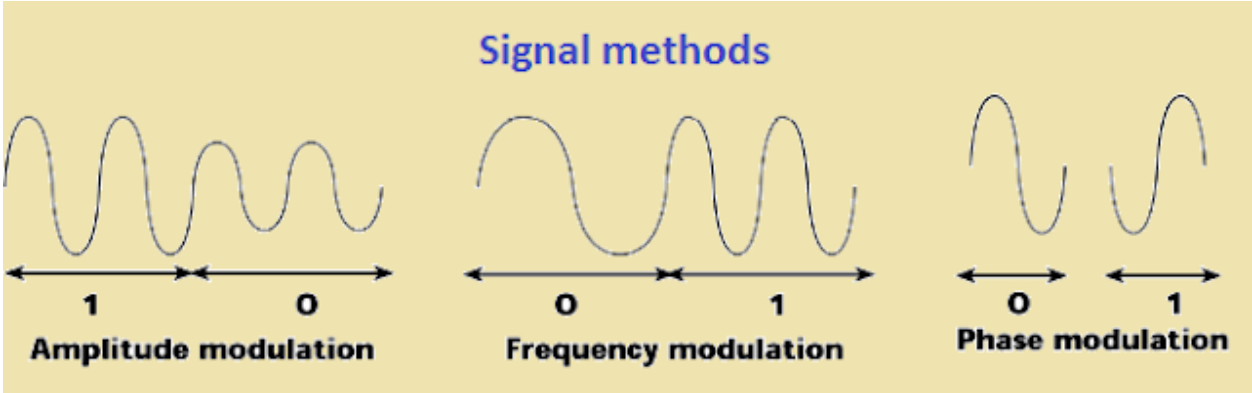
Therefore, frames are put in a string of binary bits, comprising the control information that informs where the actual data is located within a stream of bits, as well as acting as a means of guiding the bits up to the destination by virtue of signals, whose function is to carry the bits patterns. So signaling is another function of the physical layer.

Source machine and destination machine do the same thing in terms of encoding and signaling. When encoded and signaled frames get out the source machine heading towards the destination, this latter picks the frames in the form of signals and reverses the process. In other words, the destination apply the same mechanism to convert the patterns of physical energy into binary bits, then decoding the encoded bits to get the actual frame to be handed up to the upper layers.

Representing bits on media

The methods of representing binary digits on physical media is converting a pulse of energy into a defined amount of time referred to as a bit time. This latter means how much time a given Network Interface Card at the OSI model takes generate 1 bit of data and put it onto media in the form a signal. So the way binary bits are represented onto media as a signal indicates whether it is 0 or 1 at a time.

This is achieved by virtue of three possible variations which are amplitude, frequency, and phase. Take a look at this figure to have an idea.



Manchester encoding

This signaling method makes use of whether the amplitude is in a high or a low position. If a voltage (amplitude) drops from low to high within the bit time, it represents a 1 ; whereas, in case a voltage (amplitude) moves from high to low, it represents a 0. If a value is repeated such 1111 or 0000, it is represented by repeating the same movement of the amplitude. In addition, moving from one position to another (from high to low, or vice versa), happens at the edge of the time bit. The following figure shows how Manchester encoding occurs in a rather simplified way.

This signaling method is not suitable for higher-speed links. It is rather fitted for lower-speed links such as 10Base-T Ethernet whose speed is 10 megabits per second.

Nonreturn To Zero (NRZ)

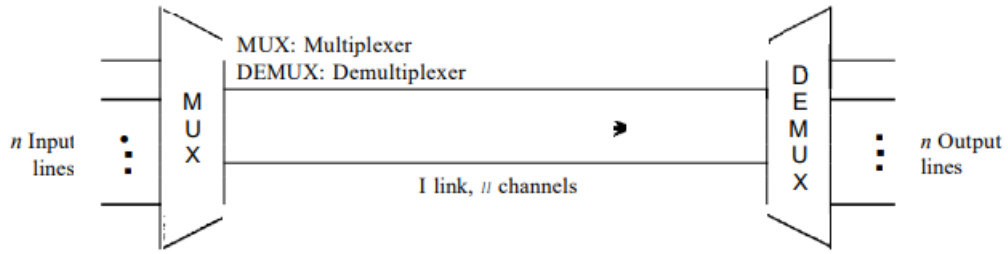
NRZ stands for Nonreturn to Zero. It is another signaling method in which bits representation lies in the voltage level within a bit time. The level of the voltage can either be a 0 or a 1. More specifically, If the the level of the voltage is high, then the voltage represents 1. Contrariwise, if the level of the voltage is low, or rather remaining steady, it is in this case a 0.

But this signaling methods has also some weaknesses which prevent it from being used in higher-speed links. It is not inherently a self-clocking signal. Simply put, a string of 0's or 1's in NRZ prevent the sender and the receiver clocks from being synchronized.

Chapter SIX Multiplexing

Multiplexing is the set 5wrtfgscaAs data and telecommunications use increases, so does traffic. We can accommodate this increase by continuing to add individual links each time a new channel is needed; or we can install higher-bandwidth links and use each to carry multiple signals.

In a multiplexed system, n lines share the bandwidth of one link. Figure 6.1 shows the basic format of a multiplexed system. The lines on the left direct their transmission streams to a multiplexer (MUX), which combines them into a single stream (many-toone). At the receiving end, that stream is fed into a demultiplexer (DEMUX), which separates the stream back into its component transmissions (one-to-many) and directs them to their corresponding lines. In the figure, the word link refers to the physical path. The word channel refers to the portion of a link that carries a transmission between a given pair of lines. One link can have many (n) channels.



Categories of multiplexing

Frequency-Division Multiplexing

FDM is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted. In FOM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal. These bandwidth ranges are the channels through which the various signals travel. Channels can be separated by strips of unused bandwidth-guard bands-to prevent signals from overlapping. In addition, carrier frequencies must not interfere with the original data frequencies. FDM is an analog multiplexing technique that combines analog signal but it also can be used for digital signal since a digital signal can be converted to analog signal.

Wavelength-Division Multiplexing

WDM is designed to use the high-data-rate capability of fiber-optic cable. The optical fiber data rate is higher than the data rate of metallic transmission cable. Using a fiber-optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.

WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve optical signals transmitted through fiber-optic channels. The idea is the same: We are combining different signals of different frequencies. The difference is that the frequencies are very high.

Synchronous Time-Division Multiplexing

Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a linle Instead of sharing a portion of the bandwidth as in FDM, time is shared. Each connection occupies a portion of time in the link. TDM is a digital multiplexing technique for combining several low-rate channels into one high-rate one. We can divide TDM into two different schemes: synchronous and statistical. In synchronous TDM, each input connection has an allotment in the output even if it is not sending data.

STANDARD ETHERNET

It was standardized in IEEE 802.3 in 1980. Ethernet is network technology which shares media. Network which uses shared media has high probability of data collision. Ethernet uses CSMA/CD technology to detect collisions. CSMA/CD stands for Carrier Sense Multi Access/Collision Detection. When a collision happens in Ethernet, all its host rolls back and waits for some random amount of time and then retransmit data

The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations: Standard Ethernet (lot Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (l Gbps), and Ten-Gigabit Ethernet (l0 Gbps), as shown in Figure 13.3. We briefly discuss all these generations starting with the first, Standard (or traditional) Ethernet.

Ethernet connector, i.e. Network Interface cards are equipped with 48-bits MAC address. This help other Ethernet devices to identify and communicate with remote devices in Ethernet. Traditional Ethernet uses 10BASE-T specifications. 10 is for 10mpbs speed, BASE stands for using baseband and T stands for Thick net or Thick Ethernet. 10BASE-T Ethernet provides transmission speed up to 10mbps and uses Coaxial cable or Cat-5 Twisted Pair cable with RJ-5 connector. Ethernet follows Star Topology with segment length up to 100 meters. All devices are connected to a Hub/Switch in a Star Fashion.

Fast-Ethernet

To encompass need of fast emerging software and hardware technologies, Ethernet extends itself as Fast-Ethernet. It can run on UTP, Optical Fiber and can be wireless too. It can provide speed up to 100 mbps. This standard is named as 100BASE-T in IEEE 803.2 using Cat-5 Twisted pair cable. It uses CSMA/CD technique for wired media sharing among Ethernet hosts and CSMA/CA (Collision Avoidance) technique for wireless Ethernet LAN. Fast Ethernet on fiber is defined under 100BASE-FX standard which provides speed up to 100mbps on fiber. Ethernet over Fiber can be extended up to 100 meters in half-duplex mode and can reach maximum of 2000 meters in full-duplex over multimode fibers.

Giga-Ethernet

After being introduced in 1995, Fast-Ethernet could enjoy its high speed status only for 3 years till Giga-Ethernet introduced. Giga-Ethernet provides speed up to 1000 megabits/seconds. IEEE802.3ab standardize Giga-Ethernet over UTP using Cat-5, Cat-5e and Cat-6 cables. IEEE802.3ah defines Giga-Ethernet over Fiber.

Virtual LAN

LAN uses Ethernet which in turn works on shared media. Shared media in Ethernet create one single Broadcast domain and one single Collision domain. Introduction of switches to Ethernet has removed single collision domain issue and each device connected to switch works in its separate collision domain. But even Switches cannot divide a network into separate Broadcast domain. Virtual LAN is a method to divide a single Broadcast domain into more than one Broadcast domains. Host in one VLAN cannot speak to a host in another. By default, all hosts are placed into same VLAN.

Wireless network

Wireless communication is one of the fastest-growing technologies. The demand for connecting devices without the use of cables is increasing everywhere. Wireless LANs can be found on college campuses, in office buildings, and in many public areas.

Wireless network is a grouping, or network, of multiple devices where data is sent and received over radio frequencies.

Wireless networks differ from wired networks, which require each end of a data connection to be physically connected by a cable in order for communication to take place. Wireless networks make it possible for organizations to eliminate the dedicated wired cabling required to connect endpoint

computing devices -- such as tablets, laptops and smartphones -- to embedded and peripheral devices. Wireless backhaul is often part of large service provider networks.

Wireless networks generally include some form of radio transmission for broadcasting and receiving wireless signals across a specified range of electromagnetic radiation spectrum, commonly referred to simply as *spectrum*. The transmission of data across a wireless network is typically done with antennas, which are often small, embedded pieces of hardware within a given device. Different wireless networks use various frequency ranges of spectrum. Within the spectrum, different channels help reduce the risk of congestion within a given spectrum frequency.

Chapter Seven Introduction to IP addressing and sub-netting

Logical Addressing

Logical addressing is a function of the Network layer of the OSI Model (Layer-3), and provides a hierarchical structure to separate networks. Logical addresses are never hardcoded on physical network interfaces, and can be dynamically assigned and changed freely. A logical address contains two components:

• Network ID – identifies which network a host belongs to.

• Host ID – uniquely identifies the host on that network.

IP provides two fundamental Network layer services:

• Logical addressing – provides a unique address that identifies both the host, and the network that host exists on.

• Routing – determines the best path to a particular destination network, and then routes data accordingly.

IP Version 4 (IPv4) was the first version to experience widespread deployment, and is defined in RFC 791. IPv4 will be the focus of this guide. IPv4 employs a 32-bit address, which limits the number of possible addresses to 4,294,967,296. IPv4 will eventually be replaced by IP Version 6 (IPv6), due to a shortage of available IPv4 addresses. IPv6 is covered in great detail in another guide.

IPv4 Addressing

A core function of IP is to provide logical addressing for hosts. An IP address provides a hierarchical structure to both uniquely identify a host, and what network that host exists on.

An IP address is comprised of four octets, separated by periods and most often represented in decimal, in the following format: **158.80.164.3**

Each octet is an 8-bit number, resulting in a 32-bit IP address. The smallest possible value of an octet is 0, or 00000000 in binary. The largest possible value of an octet is 255, or 11111111 in binary.

Sub-net mask

The Subnet Mask Part of an IP address identifies the network. The other part of the address identifies the host. A subnet mask is required to provide this distinction: 158.80.164.3 255.255.0.0 The above IP address has a subnet mask of 255.255.0.0. The subnet mask follows two rules:

• If a binary bit is set to a 1 (or on) in a subnet mask, the corresponding bit in the address identifies the network.

• If a binary bit is set to a 0 (or off) in a subnet mask, the corresponding bit in the address identifies the host.

The network portion of the subnet mask must be contiguous. For example, a subnet mask of 255.0.0.255 is **not** valid.

Hosts on the same logical network will have identical network addresses, and can communicate freely. For example, the following two hosts are on the same network:

Host A: 158.80.164.100 255.255.0.0

Host B: 158.80.164.101 255.255.0.0

Both share the same network address (158.80), which is determined by the 255.255.0.0 subnet mask. Hosts that are on different networks cannot communicate without an intermediating device. For example:

Host A: 158.80.164.100 255.255.0.0

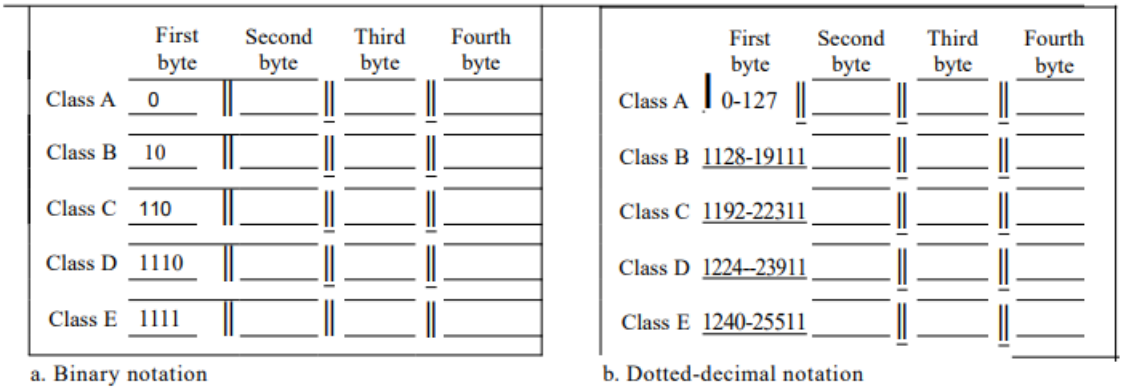
Host B: 158.85.164.101 255.255.0.0

The subnet mask has remained the same, but the network addresses are now different (158.80 and 158.85 respectively). Thus, the two hosts are not on the same network, and cannot communicate without a router between them. Routing is the process of forwarding packets from one network to another.

Classful Addressing

IPv4 addressing, at its inception, used the concept of classes. This architecture is called classful addressing. Although this scheme is becoming obsolete, we briefly discuss it here to show the rationale

behind classless addressing. In classful addressing, the address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space.



	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0-127			
Class B	1128-19111			
Class C	1192-22311			
Class D	1224--23911			
Class E	1240-25511			

b. Dotted-decimal notation

Classes and Blocks

One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size as shown in Table

In c1assfnl addressing, a large part of the available addresses were wasted.

Class	*Number ofBlocks*	*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

Subnetting is the process of creating new networks (or subnets) by stealing bits from the host portion of a subnet mask. There is one caveat: stealing bits from hosts creates more networks but fewer hosts per network.

Consider the following Class C network: 192.168.254.0

The default subnet mask for this network is 255.255.255.0. This single network can be segmented, or subnetted, into multiple networks. For example, assume a minimum of 10 new networks are required. Resolving this is possible using the following magical formula: $\mathbf{2^n}$

The exponent 'n' identifies the number of bits to steal from the host portion of the subnet mask. The default Class C mask (255.255.255.0) looks as follows in binary:

11111111.1111111.1111111.00000000

There are a total of 24 bits set to 1, which are used to identify the network. There are a total of 8 bits set to 0, which are used to identify the host, and these host bits can be stolen. Stealing bits essentially involves changing host bits (set to 0 or off) in the subnet mask to network bits (set to 1 or on). Remember, network bits in a subnet mask must always be contiguous - skipping bits is not allowed.

Consider the result if three bits are stolen. Using the above formula:

2^n = 2^3 = 8 = **8 new networks created**

However, a total of 8 new networks *does not* meet the original requirement of at least 10 networks. Consider the result if four bits are stolen:

2^n = 2^4 = 16 = **16 new networks created**

A total of 16 new networks *does* meet the original requirement. Stealing four host bits results in the following *new* subnet mask:

11111111.11111111.11111111.11110000 = 255.255.255.240

CIDR (Classless Inter-Domain Routing)

Classless Inter-Domain Routing (CIDR) is a simplified method of representing a subnet mask. CIDR identifies the number of binary bits set to a **1** (or *on*) in a subnet mask, preceded by a slash.

For example, a subnet mask of *255.255.255.240* would be represented as follows in binary:

11111111.11111111.11111111.11110000

The first 28 bits of the above subnet mask are set to *1*. The CIDR notation for this subnet mask would thus be ***/28***.

The CIDR mask is often appended to the IP address. For example, an IP address of *192.168.1.1* and a subnet mask of *255.255.255.0* would be represented as follows using CIDR notation:

192.168.1.1 /24

Class A Subnetting Example

Consider the following subnetted Class A network: 10.0.0.0 255.255.248.0

Now consider the following questions:

- How many new networks were created?
- How many usable hosts are there per network?

- What is the full range of the first three networks?

By default, the *10.0.0.0* network has a subnet mask of *255.0.0.0*. To determine the number of bits stolen:

255.0.0.0: 11111111.00000000.00000000.00000000
255.255.248.0: 11111111.11111111.11111000.00000000

Clearly, **13 bits** have been stolen to create the new subnet mask. To calculate the total number of new networks:

2^n = 2^{13} = **8192 new networks created**

There are clearly **11 bits** remaining in the host portion of the mask:

$2^n - 2$ = $2^{11} - 2$ = 2048 – 2 = **2046 usable hosts per network**

Calculating the ranges is a bit tricky. Using the shortcut method, subtract the third octet (*248)* of the subnet mask (*255.255.248.0*) from *256.*

256 – 248 = 8

The first network will begin at *0*, again. **However**, the ranges are spread across multiple octets. The ranges of the first three networks look as follows:

Subnet address	10.0.0.0	10.0.8.0	10.0.16.0
Usable Range	10.0.0.1 ↕	10.0.8.1 ↕	10.0.16.1 ↕
	10.0.7.254	10.0.15.254	10.0.23.254
Broadcast address	10.0.7.255	10.0.15.255	10.0.23.255

Private vs. Public IPv4 Addresses

The rapid growth of the Internet resulted in a shortage of available IPv4 addresses. In response, a specific subset of the IPv4 address space was designated as *private*, to temporarily alleviate this problem.

A **public address** can be routed on the Internet. Thus, hosts that must be Internet-accessible must be configured with (or *reachable* by) public addresses. Allocation of public addresses is governed by the Internet Assigned Numbers Authority (IANA).

A **private address** is intended for internal use within a home or organization, and can be freely used by anyone. However, private addresses can *never be routed* on the Internet. In fact, Internet routers are configured to immediately drop traffic with private addresses.

Three private address ranges were defined in RFC 1918, one for each IPv4 class:

- Class A - **10.x.x.x /8**
- Class B - **172.16.x.x /12**
- Class C - **192.168.x.x /24**

It is possible to *translate* between private and public addresses, using **Network Address Translation (NAT).** NAT allows a host configured with a private address to be *stamped* with a public address, thus allowing that host to communicate across the Internet. It is also possible to translate multiple privately-addressed hosts to a single public address, which conserves the public address space.

NAT provides an additional benefit – hiding the specific addresses and addressing structure of the internal (or *private*) network.

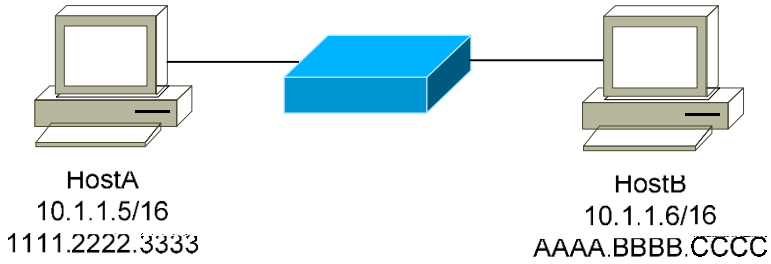
Note: NAT is *not* restricted to private-to-public address translation, though that is the most common application. NAT can also perform public-to-public address translation, as well as private-to-private address translation.

- Addresses that **cannot be assigned** to hosts for various reasons
- Special addresses that can be assigned to hosts but with **restrictions** on how those hosts can interact within the network.
- **Network and Broadcast Addresses**
    - within **each network** the **first** and **last** addresses cannot be assigned to hosts.
    - These are the **network address and the broadcast address**,
- **Default Route**
    - Is used as a "**catch all**" route when a more specific route is **not** available.
    - reserves all addresses in the **0.0.0.0 - 0.255.255.255.** address block.

Resolving Logical Addresses to Hardware Addresses

A host cannot directly send data to another host's logical address. A destination logical address must be mapped to a hardware address, so that the Data-Link layer can package a frame to transmit on the physical medium.

The Address Resolution Protocol (ARP) provides this mechanism for IPv4 on Ethernet networks. ARP allows a host to determine the MAC address for a particular destination IP address.



The ARP Table

A host can build an **ARP table** that contains a list of IP to MAC address translations. The ARP table is only locally significant to that host. There are two methods to populate an ARP table:

- **Statically**
- **Dynamically**

A **static ARP entry** is created manually on a host, and will remain permanently until purposely removed. More commonly, ARP tables are built **dynamically** by caching ARP replies. Cached entries will eventually be aged out of the ARP table. The aging time will vary depending on the operating system, and can range from several seconds to several hours.

What is VLSM

Variable Length Subnet Masks allow you a much tighter control over your addressing scheme. If you use a class C address with a default subnet mask you end up with one subnet containing 256 addresses. By using VLSM you can adjust the number of subnets and number of addresses depending on the specific needs of your network. The same rules apply to a class A or B addresses. VLSM is

supported by the following protocols: RIP version 2, OSPF,EIGRP, Dual IS-IS, and BGP,. You need to configure your router for Variable Length Subnet Masking by setting up one of these protocols. Then configure the subnet masks of the various interfaces in the IP address interface sub-command.

Benefits of VLSM

- Allows efficient use of address space
- Allows the use of multiple subnet mask lengths
- Breaks up an address block into smaller custom blocks
- Allows for route summarization
- Provides more flexibility in network design
- Supports hierarchical enterprise networks

Calculating VLSM Subnets

Objective

Use variable-length subnet mask (VLSM) to support more efficient use of the assigned IP addresses and to reduce the amount of routing information at the top level.

Background/Preparation

A class C address of 192.168.10.0/24 has been allocated.

Perth, Sydney, and Singapore have a WAN connection to Kuala Lumpur.

- Perth requires 60 hosts.
- Kuala Lumpur requires 28 hosts.
- Sydney and Singapore each require 12 hosts.

To calculate VLSM subnets and the respective hosts allocate the largest requirements first from the address range. Requirements levels should be listed from the largest to the smallest.

In this example Perth requires 60 hosts. Use 6 bits since $2^6 – 2 = 62$ usable host addresses. Thus 2 bits will be used from the 4^{th} Octet to represent the extended-network-prefix of /26 and the remaining 6 bits will be used for host addresses.

Step 1

The first step in the subnetting process is to divide the allocated address of 192.168.10.0/24 into four equal size address blocks. Since $4 = 2^2$, 2 bits are required to identify each of the 4 subnets.

Next, take subnet #0 (192.168.10.0/26) and identify each of its hosts.

Allocated Address	**Sub-networks**	**62 usable hosts/ sub-network (subnet #0)**
192.168.10.0/24	192.168.10.0/26	**192.168.10.0/26 (Network Address)**
	192.168.10.64/26	192.168.10.1/26
	192.168.10.128/26	192.168.10.2/26
	192.168.10.192/26	192.168.10.3/26
		thru
		192.168.10.61/26
		192.168.10.62/26
		192.168.10.63/26 (Broadcast Address)

Here is the range for the /26 mask.

Perth	**Range of addresses in the last octet**
192.168.10.0/26	From 0 to 63, 60 hosts required. Hosts 0 and 63 cannot be used because they are the network and broadcast addresses for their subnet

Step 2

Allocate the next level after all the requirements are met for the higher level or levels. Kuala Lumpur requires 28 hosts. The next available address after 192.168.10.63/26 is

192.168.10.64/26. Note from the above table that this is subnet number 1. Since 28 hosts are required, 5 bits will be needed for the host addresses, $2^5 - 2 = 30$ usable host addresses. Thus 5 bits will be required to represent the hosts and 3 bits will be used to represent the extended-network- prefix of /27. Applying VLSM on address 192.168.10.64/27 gives:

Sub-network #1	**Sub-sub-networks**	**30 usable hosts**
		192.168.10.64/27 (Network Address)
192.168.10.64/26	192.168.10.64/27	192.168.10.65/27
	192.168.10.96/27	192.168.10.66/27
	192.168.10.128/27	192.168.10.67/26
	192.168.10.192/27	thru
		192.168.10.93/27
		192.168.10.94/27
		192.168.10.95/27 (Broadcast Address)

Here is the range for the /27 mask.

Kuala Lumpur	**Range of addresses in the last octet**
192.168.10.64/27	From 64 to 95, 28 hosts required. Hosts 64 and 95 cannot be used because they are the network and broadcast addresses for their subnet. Thirty usable addresses are available in this range for the hosts.

Step 3

Now Sydney and Singapore require 12 hosts each. The next available address starts from 192.168.10.96/27. Note from Table 2 that this is the next subnet available. Since 12 hosts are required, 4 bits will be needed for the host addresses, $2^4 = 16$, $16 – 2 = 14$ usable addresses. Thus 4 bits are required to represent the hosts and 4 bits for the extended-network-prefix of /28. Applying VLSM on address 192.168.10.96/27 gives:

Sub-network	**Sub-sub-networks**	**14 usable hosts**
192.168.10.96/27	192.168.10.96/28	**192.168.10.96/28 (Network Address)**
	192.168.10.112/28	192.168.10.97/28
	192.168.10.128/28	192.168.10.98/28
	192.168.10.224/28	192.168.10.99/28
	192.168.10.240/28	thru
		192.168.10.109/28
		192.168.10.110/28
		192.168.10.111/28 (Broadcast Address)

Here is the range for the /28 mask.

Sydney	**Range of addresses in the last octet**
192.168.10.96/28	From 96 to 111,12 hosts required. Hosts 96 and 111 cannot be used because they are network and broadcast addresses for their subnet. Fourteen useable addresses are available in this range for the hosts.

Step 4

Since Singapore also requires 12 hosts, the next set of host addresses can be derived from the next available subnet (192.168.10.112/28).

Sub-sub-networks	**14 usable hosts**
192.168.10.96/28	**192.168.10.112/28 (Network Address)**
192.168.10.112/28	192.168.10.113/28
192.168.10.128/28	192.168.10.114/28
192.168.10.224/28	192.168.10.115/28
	Thru
192.168.10.240/28	192.168.10.125/28
	192.168.10.126/28
	192.168.10.127/28 (Broadcast Address)

Here is the range for the /28 mask.

Singapore	**Range of addresses in the last octet**
192.168.10.112/28	From 112 to 127, 12 hosts required. Hosts 112 and 127 cannot be used because they are network and broadcast addresses for their subnet. Fourteen usable addresses are available in this range for the hosts

Step 5

Now allocate addresses for the WAN links. Remember that each WAN link will require two IP addresses. The next available subnet is 192.168.10.128/28. Since 2 network addresses are required for each WAN link, 2 bits will be needed for host addresses, $2^2 - 2 = 2$ usable addresses. Thus 2 bits are required to represent the links and 6 bits for the extended-network-prefix of /30. Applying VLSM on 192.168.10.128/28 gives:

Sub-sub-networks	**14 usable hosts**
192.168.10.128/30	**192.168.10.128/30(Network Address)**
	192.168.10.129/30
	192.168.10.130/30
	192.168.10.131/30 (Broadcast Address)
192.168.10.132/30	**192.168.10.132/30(Network Address)**
	192.168.10.133/30
	192.168.10.134/30
	192.168.10.135/30 (Broadcast Address)
192.168.10.136/30	**192.168.10.136/30 (Network Address)**
	192.168.10.137/30
	192.168.10.138/30
	192.168.10.139/30 (Broadcast Address)

The available addresses for the WAN links can be taken from the available addresses in each of the /30 subnets.

Chapter 8: Data Security and Integrity

Network Security

Network security can provide one of the five services. Four of these services are related to the message exchanged using the network: message confidentiality, integrity, authentication, and nonrepudiation. The fifth service provides entity authentication or identification.

Message Confidentiality

Message confidentiality or privacy means that the sender and the receiver expect confidentiality. The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage. When a customer communicates with her bank, she expects that the communication is totally confidential.

Message Integrity

Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally nor maliciously. As more and more monetary exchanges occur over the Internet, integrity is crucial. For example, it would be disastrous if a request for transferring $100 changed to a request for $10,000 or $100,000. The integrity of the message must be preserved in a secure communication.

Message Authentication

Message authentication is a service beyond message integrity. In message authentication the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.

Message Nonrepudiation

Message nonrepudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send. The burden of proof falls on the receiver. For example, when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.

Entity Authentication

In entity authentication (or user identification) the entity or user is verified prior to access to the system resources (files, for example). For example, a student who needs to access her university resources needs to be authenticated during the logging process. This is to protect the interests of the university and the student.

Cryptography

Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. Figure 30.1 shows the components involved in cryptography.

Plaintext and Ciphertext

The original message, before being transformed, is called plaintext. After the message is transformed, it is called ciphertext. An encryption algorithm transforms the plaintext into ciphertext; a decryption algorithm transforms the ciphertext back into plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

Cipher

We refer to encryption and decryption algorithms as ciphers. The term cipher is also used to refer to different categories of algorithms in cryptography. This is not to say that every sender-receiver pair needs their very own unique cipher for a secure communication. On the contrary, one cipher can serve millions of communicating pairs.

Key

A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. To encrypt a message, we need an encryption algorithm, an encryption key, and the plaintext. These create the ciphertext. To decrypt a message, we need a decryption algorithm, a decryption key, and the ciphertext. These reveal the original plaintext

Authentication protocols

Authentication protocols are methods or procedures used to verify the identity of a user, device, or system. These protocols are designed to ensure that only authorized users or devices are able to access protected resources, and to prevent unauthorized access or tampering.

Types of Authentications

There are many different types of authentication protocols in use today, each with its own strengths and weaknesses. Here are some common types of authentications −

Password-based authentication − This is the most common form of authentication, in which a user provides a username and password to log in to a system or access a protected resource. Password-based authentication is relatively simple to implement, but can be vulnerable to attacks such as dictionary attacks or brute force attacks.

Two-factor authentication − This is a type of authentication that requires a user to provide two forms of identification, such as a password and a security token, to log in to a system or access a protected resource. Two-factor authentication can provide an additional layer of security, but may be inconvenient for users and may require additional infrastructure to support.

Biometric authentication − This is a type of authentication that uses physical or behavioral characteristics, such as a fingerprint or facial recognition, to verify the identity of a user. Biometric authentication can be highly secure, but may be expensive to implement and may not work well for all users (e.g., due to differences in physical characteristics).

It is important to choose an appropriate authentication protocol for your specific needs, taking into account factors such as the level of security required, the type of resources being protected, and the convenience and cost of implementing the protocol.

The Most Common Authentication Protocols are:

Kerberos

Kerberos is an authentication protocol that is used to securely identify users and devices on a network. It is designed to prevent attacks such as eavesdropping and replay attacks, and to allow users to securely access network resources without transmitting their passwords over the network.

The Kerberos protocol works by using a trusted third party, known as the Kerberos authentication server, to verify the identity of users and devices. When a user or device wants to access a network resource, they request access from the Kerberos authentication server. The authentication server verifies the user's identity and issues a ticket granting ticket (TGT) to the user, which can be used to request access to specific resources on the network.

The user or device can then use the TGT to request access to a specific network resource from the authentication server. The authentication server verifies the TGT and issues a service ticket (ST) to the user or device, which can be used to access the requested resource. The user or device presents the ST to the resource server, which grants access if the ST is valid.

Lightweight Directory Access Protocol (LDAP)

LDAP (Lightweight Directory Access Protocol) is a network protocol used to access and manage directory services, such as those provided by Active Directory or OpenLDAP. LDAP is designed to be a simple, fast, and secure protocol for accessing directory services over a network.

LDAP directory services are used to store and manage information about users, devices, and other objects in an organization. This information is organized in a hierarchical structure, with each object represented by an entry in the directory. LDAP enables users and applications to access and manipulate this information over a network using standard commands and protocols.

LDAP is typically used to authenticate users and devices, to look up information about users and devices, and to manage access to network resources. It is often used in conjunction with other protocols, such as Kerberos, to provide a complete solution for authentication and access control.

OAuth2

OAuth2 (Open Authorization 2.0) is an open standard for authorization that enables users to grant third-party applications access to their resources (such as data or services) without sharing their passwords. OAuth2 is used to enable secure authorization from web, mobile, and desktop applications.

The OAuth2 protocol works by allowing a user to grant a third-party application access to their resources without sharing their password. Instead, the user is redirected to a login page, where they can grant access to the third-party application by authenticating with their username and password. The third-party application can then use an access token to access the user's resources on their behalf.

SAML

SAML (Security Assertion Markup Language) is a standard protocol used to securely exchange authentication and authorization data between organizations. It is commonly used to enable single sign-on (SSO) and to provide secure access to web-based resources.

The SAML protocol works by allowing a user to authenticate with a SAML identity provider (IdP), which is a system that verifies the user's identity and issues an assertion (a statement) about the user's identity. The assertion is then provided to a SAML service provider (SP), which is a system that provides access to a web-based resource. The SP uses the assertion to grant the user access to the resource without requiring the user to authenticate again.

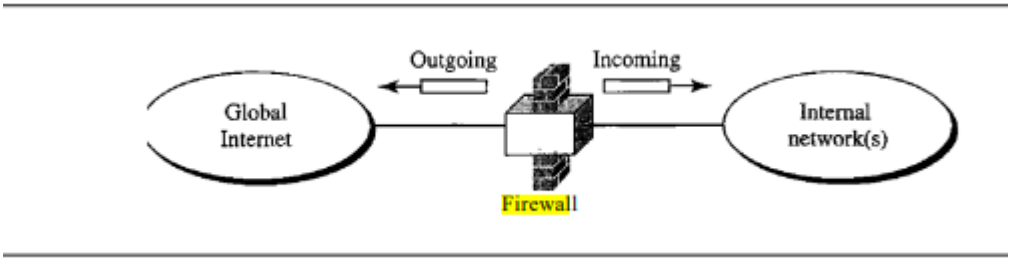
RADIUS

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol used to manage and authenticate users who connect to a network. It is commonly used to authenticate users who connect to a network using a dial-up connection, but it can also be used to authenticate users who connect to a network using other technologies, such as wireless or VPN.

The RADIUS protocol works by allowing a user to authenticate with a RADIUS server, which is a system that verifies the user's identity and authorizes their access to the network. When a user attempts to connect to the network, the RADIUS server receives a request for access and authenticates the user using the user's credentials (such as a username and password). If the user is authenticated, the RADIUS server grants access to the network and assigns the user a set of network parameters (such as an IP address and a subnet mask).

Firewalls

A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others.



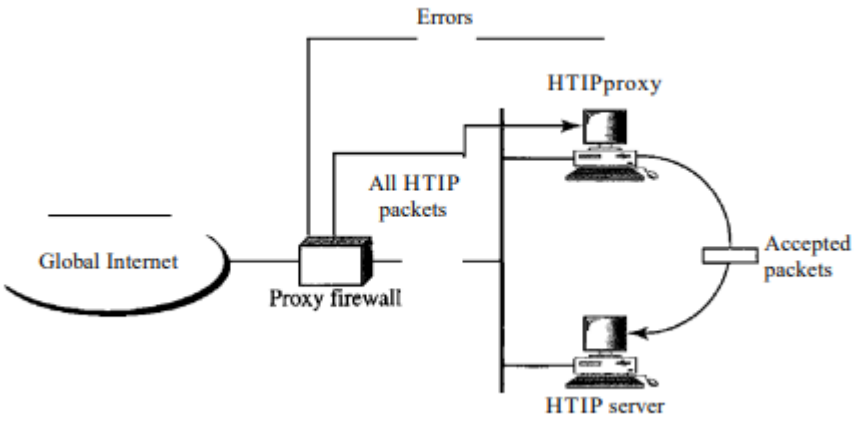
For example, a firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP. A firewall can be used to deny access to a specific host or a specific service in the organization. A firewall is usually classified as a packet-filter firewall or a proxy-based firewall.

Packet-Filter Firewall

A firewall can be used as a packet filter. It can forward or block packets based on the information in the network layer and transport layer headers: source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP). A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded).

Proxy Firewall

The packet-filter firewall is based on the information available in the network layer and transport layer headers (IP and TCPIUDP). However, sometimes we need to filter a message based on the information available in the message itself (at the application layer). As an example, assume that an organization wants to implement the following policies regarding its Web pages: Only those Internet users who have previously established business relations with the company can have access; access to other users must be blocked. In this case, a packet-filter firewall is not feasible because it cannot distinguish between different packets arriving at TCP port 80 (HTTP). Testing must be done at the application level (using URLs). One solution is to install a proxy computer (sometimes called an application gateway), which stands between the customer (user client) computer and the corporation computer.



When the user client process sends a message, the proxy firewall runs a server process to receive the request. The server opens the packet at the application level and finds out if the request is legitimate. If it is, the server acts as a client process and sends the message to the real server in the corporation. If it is not, the message is dropped and an error message is sent to the external user. In this way, the requests of the external users are filtered based on the contents at the application layer.

Virtual private Network

Virtual private network (VPN) is a technology that is gaining popularity among large organizations that use the global Internet for both intra- and interorganization communication, but require privacy in their internal communications. A private network is designed for use inside an organization. It allows access to shared resources and, at the same time, provides privacy.

Intranet

An intranet is a private network (LAN) that uses the Internet model. However, access to the network is limited to the users inside the organization. The network uses application programs defined for the global Internet, such as HTTP, and may have Web servers, print servers, file servers, and so on.

Extranet

An extranet is the same as an intranet with one major difference: Some resources may be accessed by specific groups of users outside the organization under the control of the network administrator. For example, an organization may allow authorized customers access to product specifications, availability, and online ordering. A university or a college can allow distance learning students access to the computer lab after passwords have been checked.

VPN creates a network that is private but virtual. It is private because it guarantees privacy inside the organization. It is virtual because it does not use real private WANs; the network is physically public but virtually private.

Transport layer security

A transport layer security provides end-to-end security services for applications that use a reliable transport layer protocol such as TCP. The idea is to provide security services for transactions on

the Internet. Two protocols are dominant today for providing security at the transport layer: the Secure Sockets Layer (SSL) Protocol and the Transport Layer Security (TLS) Protocol.

SSL

Services Secure Socket Layer (SSL) is designed to provide security and compression services to data generated from the application layer. Typically, SSL can receive data from any application layer protocol, but usually the protocol is HTTP. The data received from the application are compressed (optional), signed, and encrypted. The data are then passed to a reliable transport layer protocol such as TCP.SSL provides several services on data received from the application layer.

Fragmentation First, SSL divides the data into blocks of 214 bytes or less.

Compression Each fragment of data is compressed by using one of the lossless compression methods negotiated between the client and server. This service is optional.

Message Integrity To preserve the integrity of data, SSL uses a keyed-hash function to create a MAC.

Confidentiality To provide confidentiality, the original data and the MAC are encrypted using symmetric key cryptography.

Framing A header is added to the encrypted payload. The, payload is then passed to a reliable

transport layer protocol.

Transport Layer Security

Transport Layer Security (TLS) is the IETF standard version of SSL. The two are very similar, with slight differences. We highlight the differences below:

- Version. The SSLv3.0 discussed in this section is compatible with TLSv1.0.
- Cipher Suite. TLS cipher suite does not support Fortezza.
- Cryptography Secret. There are several differences in the generation of cryptographic secrets. TLS uses a pseudorandom function (PRF) to create the master key and the key materials.
- Alert Protocol. TLS deletes some alert messages and adds some new ones.
- Handshake Protocol. The details of some messages have been changed in TLS.

- Record Protocol. Instead of using MAC, TLS uses the HMAC