Chapter#1 Computer Network

Q1. What is computer network? Differentiate between computer network and distributed system. ***

- The old model in which a single computer used to serve all the computational needs of an organization has been replaced by a new one in which a large number of separate but interconnected computers do the job. Such systems are called as **computer networks**.

We can also say that computer network is an interconnection of various computers to share software, hardware and data through a communication medium between them. The computers connected in a network share files, folders, applications and resources like scanner, web-cams, printers etc. The best example of computer network is the Internet.

Differentiate between Computer Network and Distributed System:

A computer network is a group of interconnected computers and other devices that are able to communicate and share resources with each other. The main purpose of a computer network is to facilitate communication and data transfer between devices. Examples of computer networks include the internet, local area networks (LANs), and wide area networks (WANs).

A distributed system, on the other hand, is a collection of independent computers that work together as a single system to achieve a common goal. The main purpose of a distributed system is to provide a platform for distributed processing and collaboration. Examples of distributed systems include Hadoop, Spark, and Google File System.

The key differences between computer networks and distributed systems are:

Parameter	Computer Network	Distributed System
Control and administration	Computer networks typically have centralized control and administration,	while distributed systems have decentralized control and administration.
Focus	Computer networks focus on communication and data transfer,	while distributed systems focus on distributed processing and collaboration.
Scalability	Computer networks can be small or large-scale networks,	while distributed systems are typically used in large-scale environments such as cloud computing, parallel computing, or grid computing.
Fault Tolerance	Network redundancy and fault tolerance is possible but limited to certain layers	Distributed systems are designed for fault tolerance, with redundant tasks and data spread across multiple computers

Parameter	Computer Network	Distributed System
Resource Sharing	Computer networks are primarily used for resource sharing and data exchange,	while distributed systems are primarily used for parallel computing and task distribution.
Security	Computer networks require security measures to protect against unauthorized access,	while distributed systems require security measures to protect against data corruption and data loss.
Examples	Examples of computer networks include LAN, WAN, VPN, and the internet	Examples of distributed systems include Hadoop, Spark, Google File System and Bitcoin.

In summary, computer networks and distributed systems are both important for connecting devices and sharing resources, but they have different focuses and architectures. Computer networks are more focused on communication and resource sharing, while distributed systems are focused on coordination and task sharing. Both have their own advantages and disadvantages, and the choice between them depends on the specific needs of the organization or system.

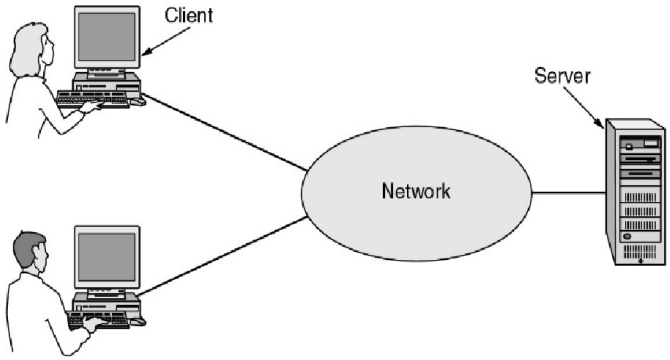
Q2. Write The uses of the Computer Network. ***

Before we start to examine the technical issues in detail, it is worth devoting some time to pointing out why people are interested in computer networks and what they can be used for. After all, if nobody were interested in computer networks, few of them would be built. We will start with traditional uses at companies, then move on to home networking and recent developments regarding mobile users, and finish with social issues.

The Uses of the Computer Network are -

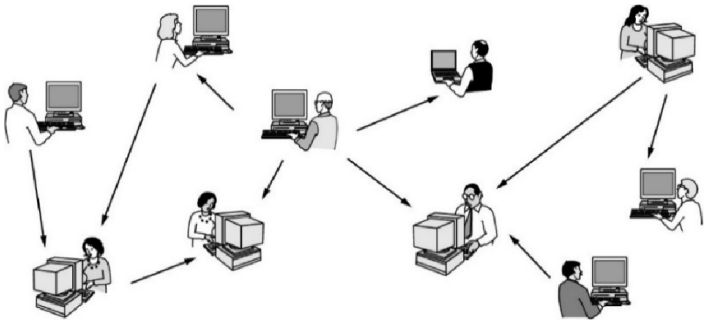
- Business Applications
- Home Applications
- Mobile Users
- Social Issues

Business Applications of Networks:



A network with two clients and one server.

Home Applications Networks:



In a peer-to-peer system there are no fixed clients and servers.

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on-line
P2P	Peer-to-peer	File sharing

Some forms of e-commerce.

Mobile Users Networks:

Wireless	Mobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

Combinations of wireless networks and mobile computing.

Social Issues Networks:

- Peer-to-Peer System
- Network Neutrality
- DMCA

Q3. Explain WAN using a Virtual Private Network (VPN). **

- A wide-area network (WAN) is a collection of local-area networks (LANs) or other networks that communicate with one another. A WAN is essentially a network of networks, with the Internet the world's largest WAN.

There are several types of WANs, built for a variety of use cases that touch virtually every aspect of modern life. VPN is a virtual private network is a mechanism for creating a secure connection between a computing device and a computer network, or between two networks, using an insecure communication medium such as the public Internet.

First, rather than lease dedicated transmission lines, a company might connect its offices to the Internet this allows connections to be made between the offices as virtual links that use the underlying capacity of the Internet. This arrangement, shown in Fig. 1-11, is called a VPN (Virtual Private Network). Compared to the dedicated arrangement, a VPN has the usual advantage of virtualization, which is that it provides flexible reuse of are source (Internet connectivity). Consider how easy it is to add a fourth office to see this. A VPN also has the usual disadvantage of virtualization, which is a lack of control over the underlying resources. With a dedicated line, the capacity is clear. With a VPN your mileage may vary with your Internet service.

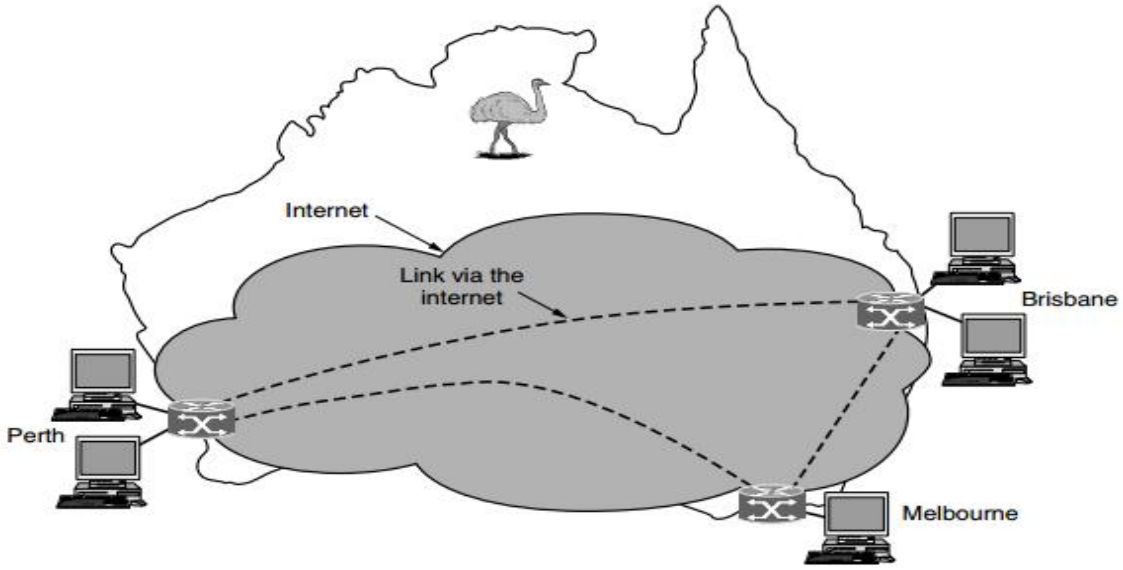


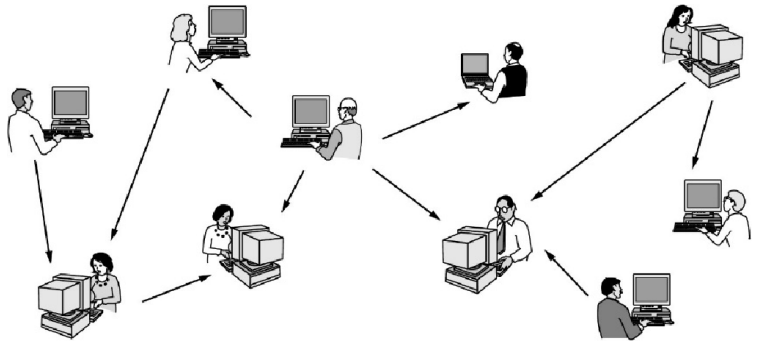
Figure 1-11.WAN using a virtual private network.

Q4. What is peer-to-peer system? Describe with example. *

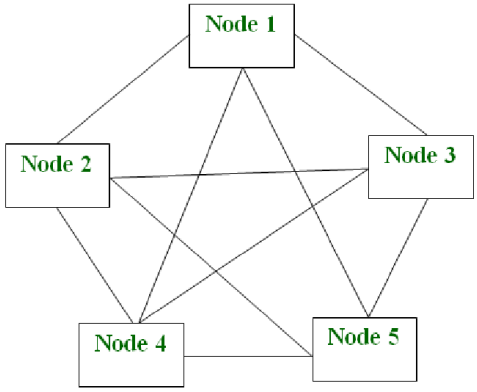
A peer-to-peer network is a simple network of computers. Here each computer acts as a node for file sharing within the formed network. Here each node acts as a server and thus there is no central server in the network. This allows the sharing of a huge amount of data. The tasks are equally divided amongst the nodes. Each node connected in the network shares an equal workload. For the network to stop working, all the nodes need to individually stop working. This is because each node works independently.

In the peer-to-peer network architecture, the computers connect with each other in a workgroup to share files, and access to internet and printers.

- Each computer in the network has the same set of responsibilities and capabilities.
- Each device in the network serves as both a client and server.
- The architecture is useful in residential areas, small offices, or small companies where each computer act as an independent workstation and stores the data on its hard drive.
- Each computer in the network has the ability to share data with other computers in the network.
- The architecture is usually composed of workgroups of 12 or more computers.



In a peer-to-peer system there are no fixed clients and servers.



P2P Architecture

Some of the popular P2P networks are Gnutella, BitTorrent, eDonkey, Kazaa, Napster, and Skype. do not have any central database of content. Instead, each user maintains his own database locally and provides a list of other nearby people who are members of the system.

Q5. Describe Client Server Model. (Fig: 1.1 & 1.2)

In the simplest of terms, one can imagine a company's information system as consisting of one or more databases with company information and some number of employees who need to access them remotely. In this model, the data are stored on powerful computers called servers. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simpler machines, called clients, on their desks, with which they access remote data, for example, to include in spreadsheets they are constructing. The client and server machines are connected by a network, This whole arrangement is called the client-server model. Show in Fig.1-1.

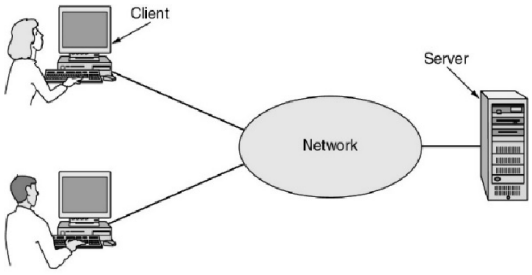


Figure 1-1. A network with two clients and one server.

For example, when a person at home accesses a page on the World Wide Web, the same model is employed, with the remote Web server being the server and the user's personal computer being the client.

Under most conditions, one server can handle a large number (hundreds or thousands) of clients simultaneously. If we look at the client-server model in detail, we see those two processes are involved, one on the client machine and one on the server machine. Communication takes the form of the client process sending a message over the network to the server process. The client process then waits for a reply message. When the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply. These messages are shown in Fig. 1-2.

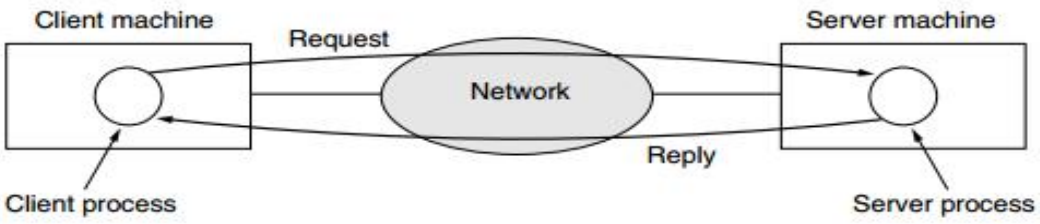


Figure 1-2. The client-server model involves requests and replies.

Q6. What is Network Neutrality?

Network neutrality, often referred to as net neutrality, is the principle that Internet service providers must treat all Internet communications equally, offering users and online content providers.

On the other hand, if you are a big company and pay well then you get good service, but if you are a small-time player, you get poor service. Opponents of this practice argue that peer-to-peer and other content should be treated in the same way because they are all just bits to the network. This argument for communications that are not differentiated by their content or source or who is providing the content is known as Network Neutrality.

NETWORKHARDWARE

There is no generally accepted taxonomy into which all computer networks fit, but two dimensions standout as important: **Transmission Technology & Scale**.

Q7. How many types of Transmission Technology? Explain it.

Broadly speaking, there are two types of transmission technology that are in widespread use: **Broadcast links and Point-to-point links.**

Q8. What is Broadcast Links & Point-to-point Links?

In contrast, on a **Broadcast Links** network, the communication channel is shared by all the machines on the network; packets sent by any machine are received by all the others. An address field within each packet specifies the intended recipient. Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored. A wireless network is a common example of a broadcast link, with communication shared over a coverage region that depends on the wireless channel and the transmitting machine.

Point-to-point links connect individual pairs of machines. To go from the source to the destination on a network made up of point-to-point links, short messages, called packets in certain contexts, may have to first visit one or more intermediate machines. Often multiple routes, of different lengths, are possible, so finding good ones is important in point-to-point networks. Common example is a Telephone call in which one telephone is connected with one other, and what is said by one caller can only be heard by the other.

Q9. What is Unicasting, Broadcasting & Multicasting?

Unicasting - Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called **unicasting**.

Broadcast systems usually also allow the possibility of addressing a packet to all destinations by using a special code in the address field. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called **broadcasting**.

Multicasting is a type of communication in which a message is sent from one device to a group of devices on the network.

Q10. Explain WAN using an ISP Network. ***

A WAN (Wide Area Network) is a network that spans over a large geographical area, such as a city, country or even worldwide. One common example of a WAN is the internet, which is a global network of interconnected networks.

An ISP (Internet Service Provider) is a company that provides internet access to customers. To provide internet access, an ISP creates a WAN network that connects their customers to the internet.

When a customer wants to access the internet, their device (such as a computer or smartphone) sends a request to the ISP's access network. The request is then routed through the access network to the ISP's aggregation network, where it is aggregated with traffic from other customers. The aggregated traffic is then routed through the core network to the PoP, where it is connected to the internet or to other networks.

In summary, an ISP network is a WAN that provides internet access to customers. The network consists of the access network, aggregation network, core network, and points of presence (PoPs). When a customer wants to access the internet, their request is routed through the network to the PoP, where it is connected to the internet or other networks.

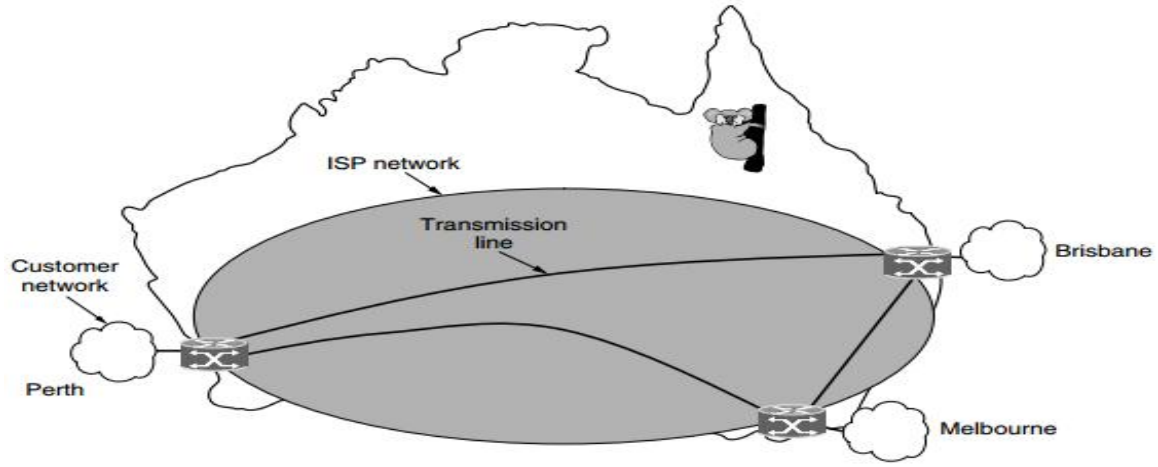


Figure 1-12. WAN using an ISP network.

Q11. Explain information flow supporting virtual communication in layer 5. ***

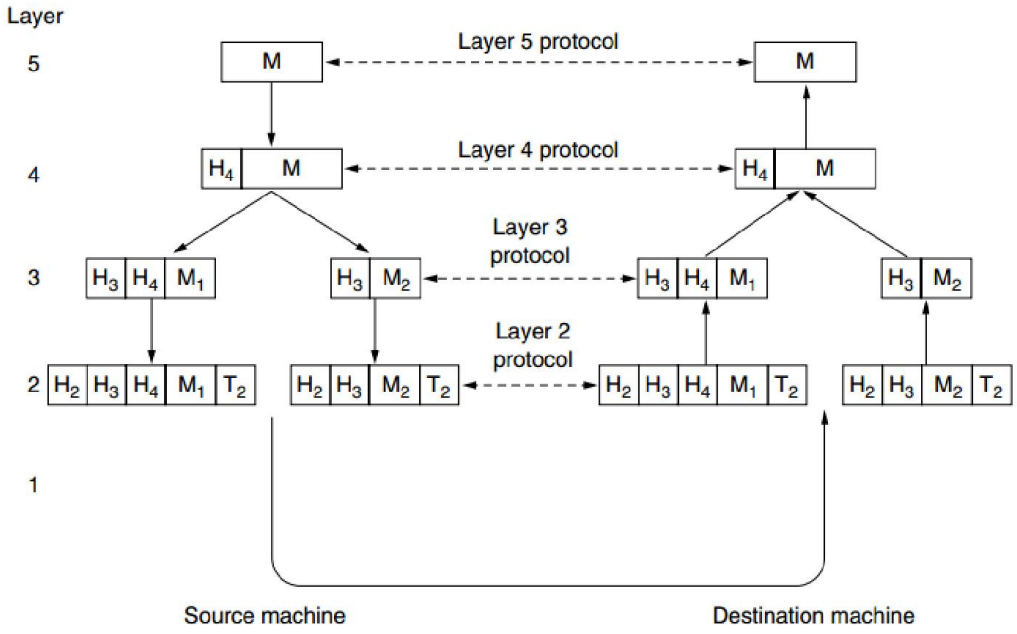


Figure 1-15. Example information flow supporting virtual communication in layer 5.

Now consider a more technical example: how to provide communication to the top layer of the five-layer network in Fig. 1-15. A message, M, is produced by an application process running in layer 5 and given to layer 4 for transmission. Layer 4 puts a header in front of the message to identify the message and passes the result to layer 3. The header includes control information, such as addresses, to allow layer 4 on the destination machine to deliver the message. Other examples of control information used in some layers are sequence numbers (in case the lower layer does not preserve message order), sizes, and times.

In many networks, no limit is placed on the size of messages transmitted in the layer 4 protocol but there is nearly always a limit imposed by the layer 3 protocol. Consequently, layer 3 must break up the incoming messages into smaller units, packets, prepending a layer 3 header to each packet. In this example, M is split into two parts, M1 and M2, that will be transmitted separately.

Q12. Define connection oriented and connectionless networks. Explain a simple client-server interaction using acknowledgment datagrams. ***

- There are two types of communication services in networking. Connection-oriented and connectionless services.

Connection-oriented service establishes a logical connection between two devices before transmitting data. This connection ensures the reliable delivery of data, and all packets are transmitted in the correct order. Examples of connection-oriented services include TCP (Transmission Control Protocol) and ATM (Asynchronous Transfer Mode).

Connectionless service, on the other hand, does not establish a logical connection between devices before transmitting data. Instead, each packet is treated as an independent unit and transmitted individually without guaranteeing reliability or order. Examples of connectionless services include UDP (User Datagram Protocol) and IP (Internet Protocol).

- The client process executes CONNECT to establish a connection with the server. The CONNECT call needs to specify who to connect to, so it might have a parameter giving the server's address. The operating system then typically sends a packet to the peer asking it to connect, as shown by (1) in Fig 1-18. The server process can then establish the connection with the ACCEPT call. This sends a response (2) back to the client process to accept the connection.

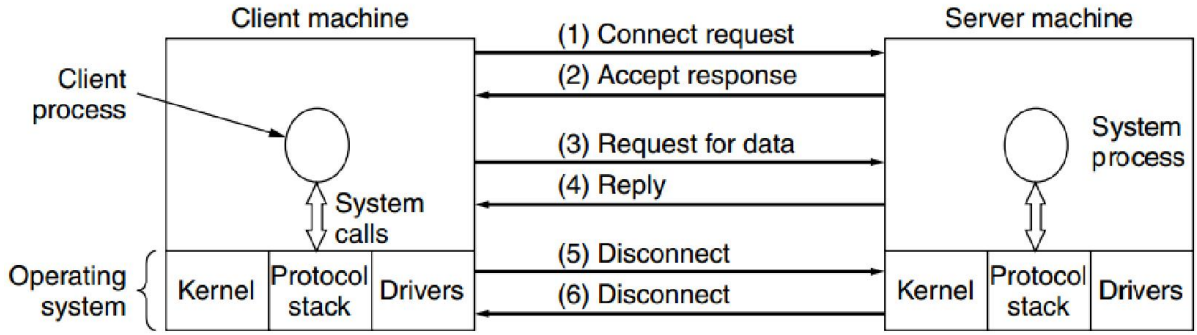


Figure 1-18. A simple client-server interaction using acknowledged datagrams.

Then the client executes SEND to transmit its request (3) followed by the execution of RECEIVE to get the reply. The arrival of the request packet at the server machine unblocks the server so it can handle the request. After it has done the work, the server uses SEND to return the answer to the client (4). Usually, an initial DISCONNECT is a blocking call, suspending the client and sending a packet to the server saying that the connection is no longer needed. When the client is done, it executes DISCONNECT to terminate the connection (5). When the server gets the packet, it also issues a DISCONNECT of its own, acknowledging the client and releasing the connection (6). In a nutshell, this is how connection-oriented communication works.

Q13. What is connection oriented & connectionless services? Differentiate between connection oriented and connectionless services. ***

- There are two types of communication services in networking. Connection-oriented and connectionless services.

Connection-oriented service establishes a logical connection between two devices before transmitting data. This connection ensures the reliable delivery of data, and all packets are transmitted in the correct order. Examples of connection-oriented services include TCP (Transmission Control Protocol) and ATM (Asynchronous Transfer Mode).

Connectionless service, on the other hand, does not establish a logical connection between devices before transmitting data. Instead, each packet is treated as an independent unit and transmitted individually without guaranteeing reliability or order. Examples of connectionless services include UDP (User Datagram Protocol) and IP (Internet Protocol).

Here's a sample table comparing the characteristics of connection-oriented and connectionless services:

Parameter	Connection-Oriented Services	Connectionless Services
Definition	Communication between devices established by setting up a logical connection before data is transmitted	Communication between devices without establishing a logical connection beforehand
Reliability	Provides reliable data delivery with error checking and correction	Does not provide reliability, with no guarantee that data will be received or in the correct order
Overhead	Higher overhead due to connection setup and maintenance	Lower overhead, as there is no connection setup and teardown
Delivery confirmation	Provides delivery confirmation to ensure data has been received	No delivery confirmation, data is sent and not tracked
Bandwidth allocation	Requires a fixed amount of bandwidth for the duration of the connection	Bandwidth is not allocated, which allows for efficient use of network resources
Usage	Best for applications that require guaranteed delivery of data, such as file transfer, email, and streaming media	Best for applications that require efficient use of network resources, such as voice and video communication
Examples	Examples of connection-oriented services include TCP and ATM	Examples of connectionless services include UDP and IP

Q14. Different types of service with examples.

- The different types of services summarize in the figures given below:

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Movie download
	Unreliable connection	Voice over IP
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Text messaging
	Request-reply	Database query

Figure 1-16. Six different types of service.

Q15. Show the Interaction between layers in the OSI reference model. ***

- The **OSI (Open Systems Interconnection)** reference model is a theoretical framework used to describe the communication process between different devices in a network. The model is divided into seven layers, each with a specific function. The layers interact with each other to ensure reliable and efficient communication between devices. Here is the interaction between layers in the OSI reference model:

Physical Layer: This is the first layer in the OSI model and deals with the physical aspects of communication, such as the transmission and reception of data over the physical medium. The physical layer interacts directly with the hardware and transmits the raw bit stream across the physical medium.

Data Link Layer: The Data Link Layer is responsible for the error-free transfer of data between two adjacent nodes on a network. It provides flow control and error detection and correction. The Data Link Layer interacts with the Physical Layer to transmit and receive frames over the physical medium.

Network Layer: The Network Layer provides the addressing and routing services that enable packets to be routed between different networks. It interacts with the Data Link Layer to encapsulate the data into packets and to determine the best path for the packets to take through the network.

Transport Layer: The Transport Layer provides end-to-end data transfer between applications running on different devices. It interacts with the Network Layer to ensure that packets are delivered reliably and in the correct order.

Session Layer: The Session Layer establishes, manages, and terminates connections between applications. It interacts with the Transport Layer to establish and maintain a connection between applications.

Presentation Layer: The Presentation Layer translates the data from the Application Layer into a format that can be understood by the network. It interacts with the Session Layer to establish the context for the data transfer.

Application Layer: The Application Layer provides services to end-users, such as email, file transfer, and web browsing. It interacts with the Presentation Layer to provide an interface between the user and the network.

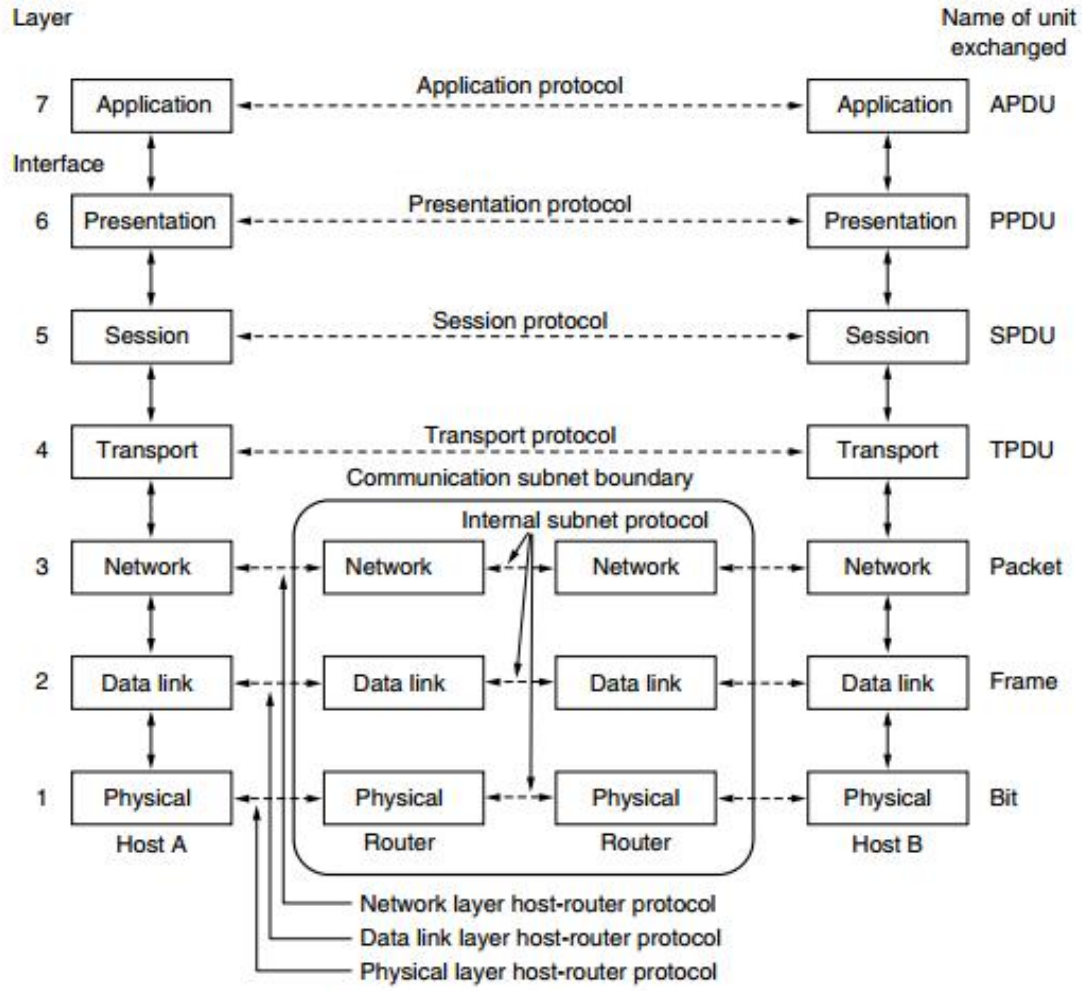


Figure 1-20. The OSI reference model.

In summary, the OSI reference model has seven layers that interact with each other to provide a seamless communication process between devices in a network. Each layer has a specific function and interacts with the layer above and below it to ensure that data is transmitted reliably and efficiently.

Q16. Describe the ARPANET. ***

- ARPANET (Advanced Research Projects Agency Network) was the first operational packet-switching network and the precursor to the modern Internet. It was funded by the U.S. Department of Defense's Advanced Research Projects Agency (ARPA) and was developed in the late 1960s and early 1970s.

ARPANET was designed to allow researchers to share computing resources and exchange information through a decentralized network. It used packet-switching technology to transmit data in small packets between interconnected computers, allowing data to be transmitted efficiently and reliably even if parts of the network were damaged or offline.

The first ARPANET message was sent in October 1969 between two computers located at University in Los Angeles, California (UCLA) and the Stanford Research Institute (SRI). Over the next few years, more universities and research institutions were connected to the network, and email, file transfer, and remote login capabilities were developed.

ARPANET paved the way for the development of the modern Internet, which emerged in the 1980s and 1990s with the creation of the World Wide Web and the introduction of the TCP/IP protocol. The original ARPANET design is shown in Fig. 1-26.

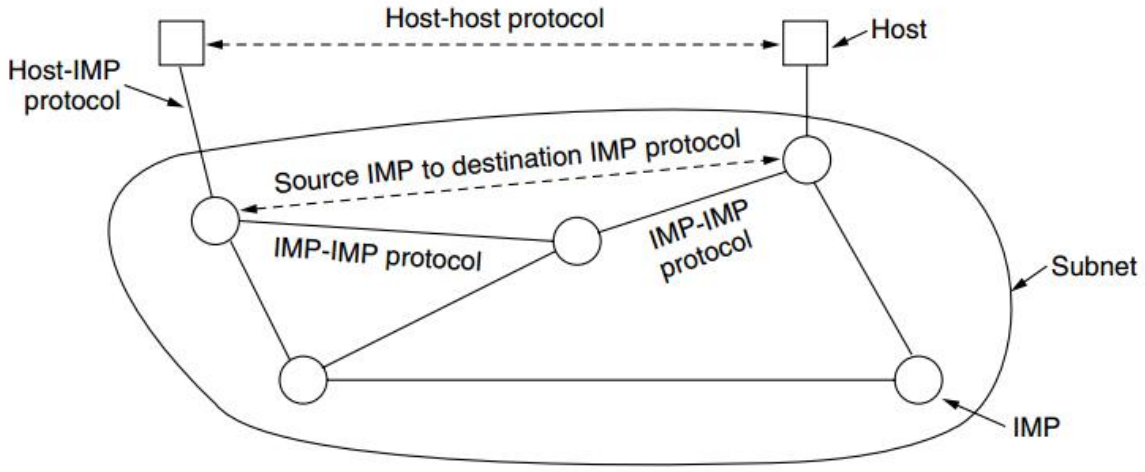


Figure 1-26. The original ARPANET design.

Q17. Explain the Architecture of the Internet. *

- The architecture of the Internet can be described as a layered architecture, with each layer responsible for a specific function or set of functions. This architecture is based on the Internet Protocol (IP) and the Transmission Control Protocol (TCP), which provide a standardized set of rules and procedures for communication between network devices.

The Internet architecture is typically divided into five layers, which are:

1. **Physical layer:** This layer deals with the physical transmission of data over the network, including the transmission medium (such as copper wire or fiber optic cable) and the protocols used for transmitting data over the medium (such as Ethernet or Wi-Fi).
2. **Data link layer:** This layer provides a way for devices on the same physical network to communicate with each other, by defining how data is framed, transmitted, and received. The most common data link layer protocols used on the Internet are Ethernet and Wi-Fi.
3. **Network layer:** This layer is responsible for routing packets of data between networks, using the Internet Protocol (IP). The IP protocol provides a way to uniquely identify each device on the network and route packets of data between them.
4. **Transport layer:** This layer provides reliable end-to-end delivery of data between devices, using the Transmission Control Protocol (TCP). TCP provides a way to establish a connection between two devices and to reliably transmit data between them, with error detection and correction mechanisms.
5. **Application layer:** This layer provides the interface between the network and the applications that use it, such as web browsers, email clients, and file transfer utilities. Applications use protocols such as HTTP, FTP, and SMTP to communicate with other devices over the network.

Each layer of the Internet architecture provides a set of services to the layer above it, and relies on the services provided by the layer below it. This layered architecture allows for flexibility, scalability, and interoperability, as new technologies and protocols can be added or replaced at each layer without affecting the functionality of the layers above or below.

The big picture is shown in Fig. 1-29. Let us examine this figure piece by piece, starting with a computer at home (at the edges of the figure). To join the Internet, the computer is connected to an Internet Service Provider, or simply ISP, from whom the user purchases Internet accessor connectivity. This lets the computer exchange packets with all of the other accessible hosts on the Internet. The user might send packets to surf the Web or for any of a thousand other uses, it does not matter. There are many kinds of Internet access, and they are usually distinguished by how much bandwidth they provide and how much they cost, but the most important attribute connectivity.

A

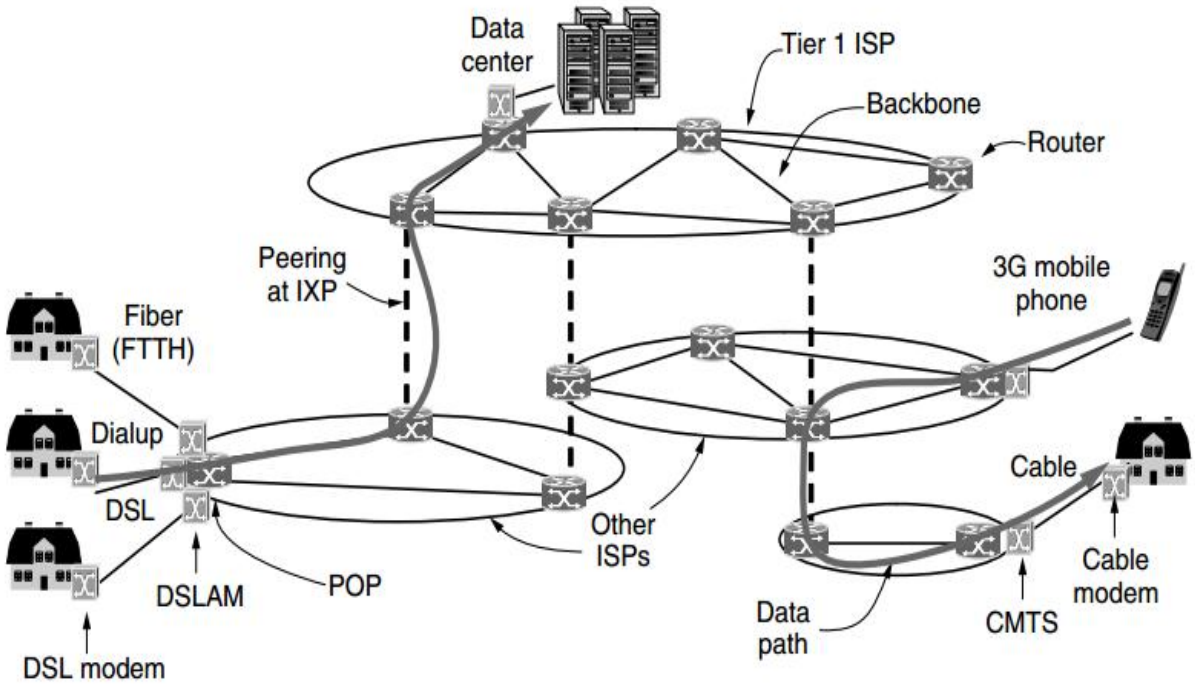


Figure 1-29. Overview of the Internet architecture.

common way to connect to an ISP is to use the phone line to your house, in which case your phone company is your ISP.DSL, short for Digital Subscriber Line, reuses the telephone line that connects to your house for digital data transmission. The computer is connected to a device called a DSL modem that converts between digital packets and analog signals that can pass unhindered over the telephone line. At the other end, a device called a DSLAM (Digital Subscriber Line Access Multiplexer) converts between signals and packets.

Q18. Name and define the basic components of a RFID network with necessary diagram. ***

- RFID (Radio Frequency Identification) is a technology that uses radio waves to identify and track objects or people. The basic components of an RFID network include:

1. **RFID Tags:** An RFID tag is a small device that contains an antenna and a microchip. The microchip stores information about the object or person being tracked, such as its unique identifier or product details. The antenna allows the tag to communicate with an RFID reader using radio waves. RFID tags come in a variety of shapes and sizes, from small adhesive labels to ruggedized tags used in harsh environments.

2. **RFID Readers:** An RFID reader is a device that sends out radio waves to communicate with RFID tags. The reader captures the information stored on the tag and sends it to a backend system for processing. RFID readers can be fixed or handheld and can be configured to read tags at different distances and frequencies.

3. **Antennas:** Antennas are used to transmit and receive radio waves between RFID tags and readers. They can be integrated into readers or mounted separately to provide greater flexibility in reading tags. Antennas come in a variety of sizes and shapes and can be designed to read tags at specific frequencies and ranges.

4. **Backend System:** The backend system is responsible for processing the data collected by RFID readers. This system can include a database for storing tag information, software for managing and analyzing the data, and applications for integrating the data into other systems.

Here's a diagram that shows the basic components of an RFID network:

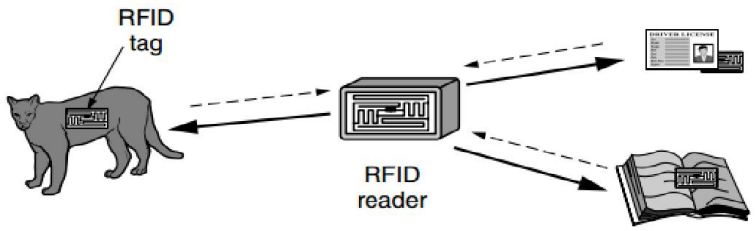


Figure 1-36. RFID used to network everyday objects.

In this diagram, the RFID tag communicates with the RFID reader using radio waves. The reader captures the data from the tag and sends it to the backend system for processing. The backend system can then store the data in a database, analyze it, or integrate it into other systems.

Q19. Differentiate between OSI and TCP/IP reference model. ***

- The **OSI** (Open Systems Interconnection) model and the **TCP/IP** (Transmission Control Protocol/Internet Protocol) model are both conceptual models that describe how data is transmitted over a network, but there are some key differences between them.

1. **Number of Layers:**
   The OSI model has seven layers, while the TCP/IP model has only four layers. The seven layers in the OSI model are: Physical, Data Link, Network, Transport, Session, Presentation, and Application. The four layers in the TCP/IP model are: Network Access, Internet, Transport, and Application.

2. Functionality of Layers:
The layers in the two models have similar functions, but the way they are organized and named differs. For example, the OSI model has a session layer, which is responsible for establishing and managing connections between devices, while the TCP/IP model does not have a dedicated session layer. The TCP/IP model combines the session, presentation, and application layers of the OSI model into a single application layer.

3. Protocol Standards:
The OSI model is a theoretical model that was developed by the International Organization for Standardization (ISO) in the 1980s. It was intended to be a standardized framework for network communication, but it has yet to be widely adopted in practice. The TCP/IP model, on the other hand, is the model that is actually used in the design and implementation of the Internet and many other networks.

4. Layer Functions:
The OSI model is designed to be independent of any specific technology or protocol, while the TCP/IP model is closely tied to the specific protocols used in the Internet. The OSI model provides a framework for communication, while the TCP/IP model provides a set of protocols for implementing that framework.

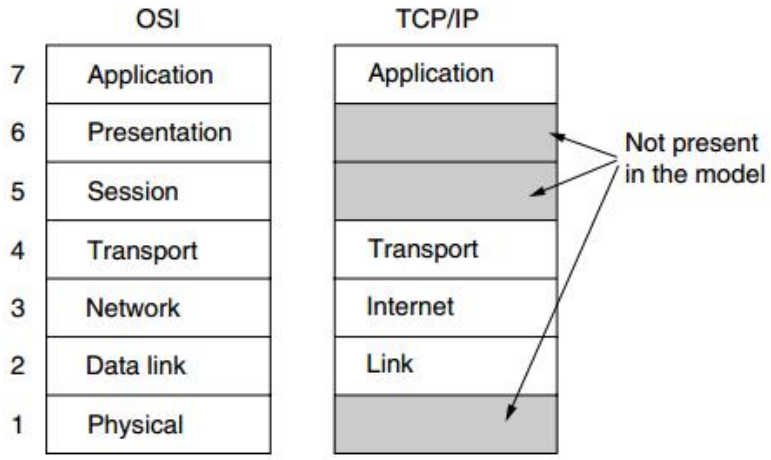


Figure 1-21. The TCP/IP reference model.

Overall, the OSI model is more complex and theoretical than the TCP/IP model, which is simpler and more practical. However, both models provide a useful way of thinking about network communication and understanding how data is transmitted over a network.

Q20. Explain the major components of an optical system and also explain the working principle of fiber optic. ***

An optical system is a system that uses light to transmit information or perform other functions. The major components of an optical system include:

1. **Light Source:** The light source is a device that produces light. Examples of light sources include LEDs (light emitting diodes), laser diodes, and lamps.

2. **Optical Fibers:** Optical fibers are thin, flexible strands of glass or plastic that are used to transmit light over long distances. The core of an optical fiber is the region through which light travels, and it is surrounded by a cladding layer that reflects the light back into the core. The core and cladding are covered by a protective coating.

3. **Connectors:** Connectors are used to join optical fibers together or to connect fibers to other components in the optical system, such as light sources and detectors.

4. **Detectors:** Detectors are devices that convert light signals into electrical signals. Examples of detectors include photodiodes, photomultiplier tubes, and CCD (charge-coupled device) arrays.

Working Principle of Fiber Optic:

Fiber optic technology uses the principle of total internal reflection to transmit light through an optical fiber. When light enters the core of an optical fiber at an angle that is greater than the critical angle, it is reflected back into the core and continues to travel along the fiber. This allows light to be transmitted over long distances with minimal loss.

Here's a step-by-step explanation of how fiber optic works:

1. A light source, such as a laser or LED, produces a beam of light.
2. The light is coupled into the core of an optical fiber using a connector.
3. The light travels down the core of the fiber, reflecting off the cladding layer and staying within the core due to total internal reflection.
4. The light continues to travel along the fiber until it reaches the end, where it is detected by a photodetector.
5. The photodetector converts the light signal back into an electrical signal that can be processed by electronic equipment.

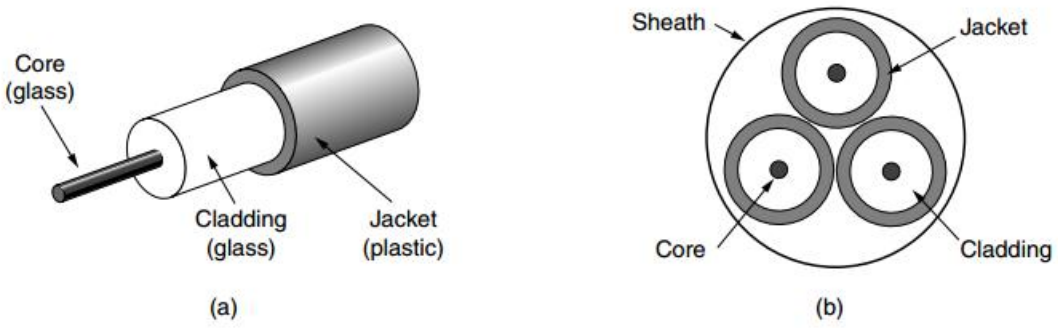


Figure 2-8. (a) Side view of a single fiber. (b) End view of a sheath with three fibers.

Fiber optic technology has many advantages over other forms of communication, including high bandwidth, low loss, and immunity to electromagnetic interference. These properties make fiber optic ideal for use in telecommunications, data centers, and other applications where high-speed and reliable communication is required.

Q21. What is geostationary satellites? Illustrate VSAT system using a hub. ***

- Geostationary satellites are satellites that are positioned in orbit around the Earth's equator at an altitude of approximately 36,000 km. These satellites orbit the Earth at the same speed as the Earth rotates, which allows them to appear stationary from the ground. This property makes geostationary satellites ideal for communications applications, such as television broadcasting and satellite internet.

VSAT (Very Small Aperture Terminal) is a satellite communication system that uses small dish antennas to transmit and receive data over satellite links. The system consists of a hub station and multiple remote terminals, each of which has a small dish antenna.

Here's a diagram that illustrates a VSAT system using a hub:

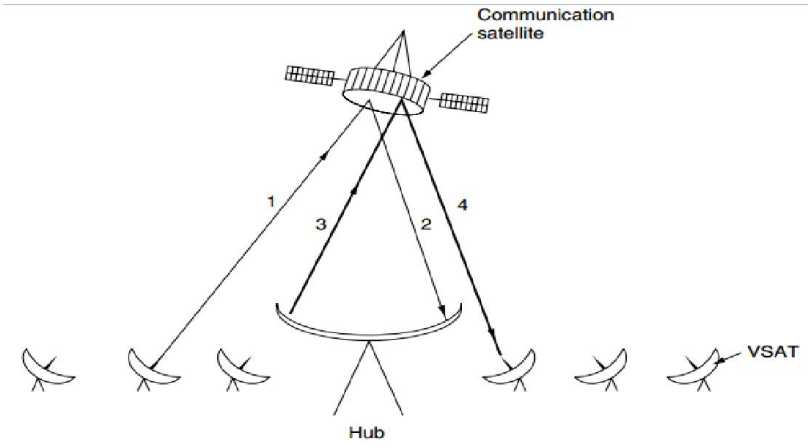


Figure 2-17. VSATs using a hub.

In this diagram, the hub station communicates with the remote terminals over a satellite link. The hub station is connected to a terrestrial network, such as the internet or a private network, which allows it to provide connectivity to the remote terminals.

Here's how the VSAT system works:

1. The hub station sends data to the satellite, which relays the data to the remote terminals.
2. The remote terminals receive the data from the satellite using their dish antennas.
3. The remote terminals send data to the hub station by transmitting the data through their dish antennas to the satellite, which relays the data to the hub station.
4. The hub station receives the data from the remote terminals and forwards it to the terrestrial network.

VSAT systems are used in a wide range of applications, including remote site connectivity, mobile satellite communications, and disaster recovery.

Q22. Define the Nyquist theorem formula with maximum data rate definition. *

- The Nyquist theorem, also known as the sampling theorem, states that in order to accurately reconstruct a continuous signal from its samples, the sampling frequency must be at least twice the highest frequency component present in the signal. Mathematically, the Nyquist theorem can be expressed as:

$f_s \geq 2f_m$

where f_s is the sampling frequency and f_m is the highest frequency component in the signal.

The maximum data rate, also known as the Nyquist rate, is the maximum rate at which data can be transmitted without loss of information, and it is given by:

$D_{max} = 2B \log_2 M$

where B is the bandwidth of the channel in hertz, M is the number of discrete levels that can be used to represent the signal, and log2 is the binary logarithm.

Thus, the Nyquist theorem and the maximum data rate formula are closely related, as the maximum data rate is determined by the bandwidth of the channel and the number of discrete levels that can be used to represent the signal, both of which are constrained by the Nyquist theorem.

Q23. Define the maximum data rate of a channel or SNR-to-noise ratio.

- The maximum data rate of a channel, also known as the channel capacity, is the maximum rate at which data can be reliably transmitted over the channel without any errors. The channel capacity depends on several factors such as the bandwidth of the channel, the signal-to-noise ratio (SNR) of the channel, and the modulation scheme used for transmitting the data.

The Shannon-Hartley theorem is a mathematical formula that provides an upper bound on the maximum data rate of a channel, and it is given by:

$C = B \log_2(1 + SNR)$

where C is the channel capacity in bits per second, B is the bandwidth of the channel in hertz, and SNR is the signal-to-noise ratio of the channel. The Shannon-Hartley theorem states that the channel capacity is directly proportional to the bandwidth of the channel and the logarithm of the SNR.

The maximum data rate of a channel can also be affected by factors such as interference, attenuation, and multipath fading, which can reduce the SNR and limit the channel capacity. To overcome these limitations, various techniques such as error-correcting codes, adaptive modulation, and diversity techniques can be used to improve the reliability and efficiency of data transmission over the channel.

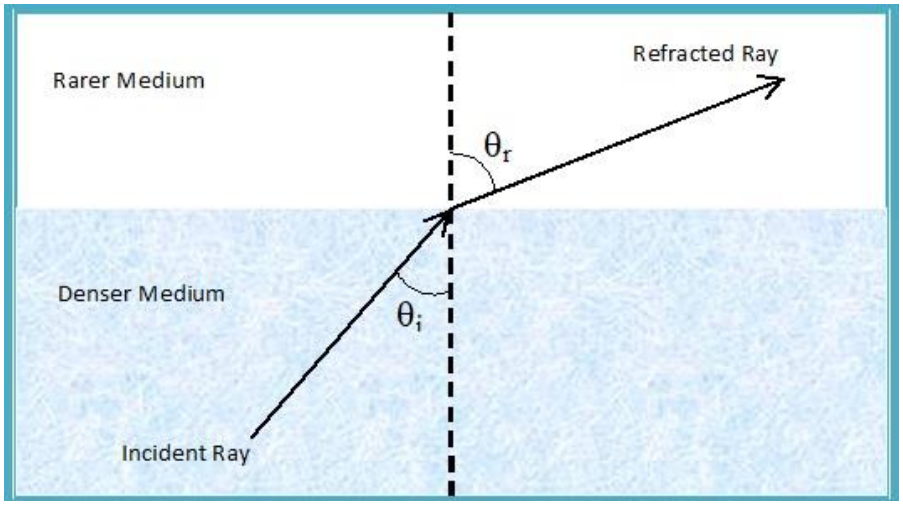
Q24. Describe Transmission of Light Through Fiber. ***

- In fiber optic communication, signals are transmitted through an optical fiber. This is based upon certain characteristics of light, namely refraction and total internal reflection.

When a light ray goes from a denser transmission medium to a rarer one or vice versa, then its direction changes at the interface of the two mediums. This phenomenon is called refraction of light.

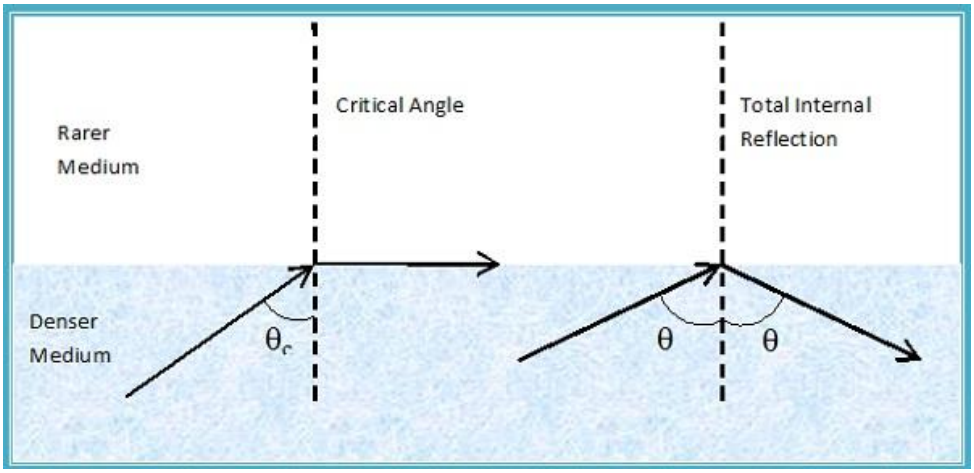
The density of an optical medium is measured in refractive index. Higher the refractive index, denser it is.

The angle between the incident ray and the normal is called angle of incidence Θi, while the angle between the refracted ray and the normal is called the angle of refraction Θr. When light travels from denser to rarer medium, the angle of refraction is greater than the angle of incidence.



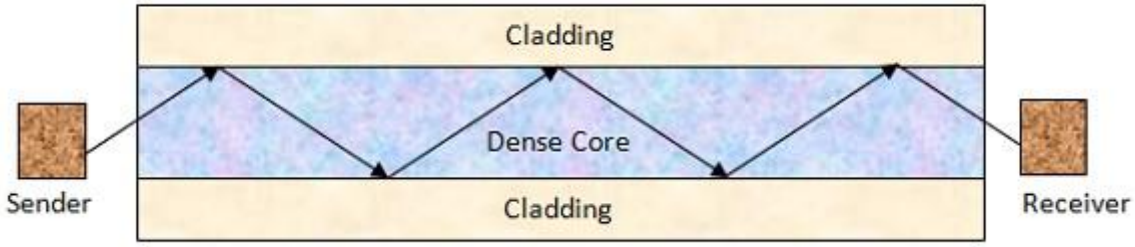
For light propagating from denser medium to rarer medium, if the angle of refraction is 〖90〗^0, the corresponding angle of incidence is called critical angleΘc.

If a light ray is an incident at the interface of two media with an angle greater than the critical angle, it is completely reflected back to the denser medium. This phenomenon is called total internal reflection.



Transmission of Light in Fiber Optic Cable

Optical fibers use total internal reflection to transmit light. It has a solid core of dense glass surrounded by a less dense cladding. The light ray passing through the inner core is reflected back instead of being refracted to the rarer cladding.



Theoretically, there should not be any loss of light waves due to total internal reflection. However, attenuation of light occurs depending upon the wavelength of light waves and the properties of the glasses. The three commonly used wavelength bands for propagation are 0.85 microns, 1.30 microns, and 1.55 microns.

Q25. Describe PSTN

PSTN stands for Public Switched Telephone Network, which is the traditional network used for landline telephone communication. PSTN is a circuit-switched system that relies on copper wires and analog signals to transmit voice and data over the network. PSTN is made up of various components, such as local loops, central offices, and long-distance trunks.

When a person makes a call, the voice signal is converted into an analog signal and transmitted over the copper wire through the local loop to the central office. The central office then connects the call to the recipient's local loop or sends it over the long-distance trunk to the recipient's central office, which then routes the call to the recipient's local loop.

PSTN was the dominant telephone network for many years but is now being replaced by digital communication technologies like VoIP (Voice over Internet Protocol). However, PSTN still plays an important role in providing reliable communication services in areas where broadband internet is not available.

Q26. Define, End Office, Local Central Office, Local Loop, Toll Office, Intertoll Trunks. ***

- **End Office:** An End Office is a type of central office in a telephone network that is responsible for providing telephone service to subscribers in a particular geographic area. End Offices are typically located at the edge of a local calling area and are connected to other End Offices through trunk lines.
- **Local Central Office:** A Local Central Office is a type of central office that serves as the hub for telephone lines within a particular local calling area. Local Central Offices are

responsible for connecting subscribers to the telephone network and routing calls to other Local Central Offices or Toll Offices as needed.

- **Local Loop:** The Local Loop is the physical connection between a customer's premises and the Local Central Office or End Office. The Local Loop typically consists of a pair of copper wires that transmit voice and data signals between the customer's premises and the central office.
- **Toll Office:** A Toll Office is a type of central office in a telephone network that is responsible for routing long-distance calls to other Toll Offices or Local Central Offices. Toll Offices are also responsible for handling the billing and accounting for long-distance calls.
- **Intertoll Trunks:** Intertoll Trunks are the trunk lines that connect Toll Offices to other Toll Offices or Local Central Offices in a telephone network. Intertoll Trunks are used to carry long-distance calls between different regions or areas and can span hundreds or thousands of miles. Intertoll Trunks are typically high-capacity lines that can handle large volumes of voice and data traffic.

Q27. Draw A typical circuit route for a long-distance call and explain the function of its components. ***

Here is a diagram of a typical circuit route for a long-distance call:

In

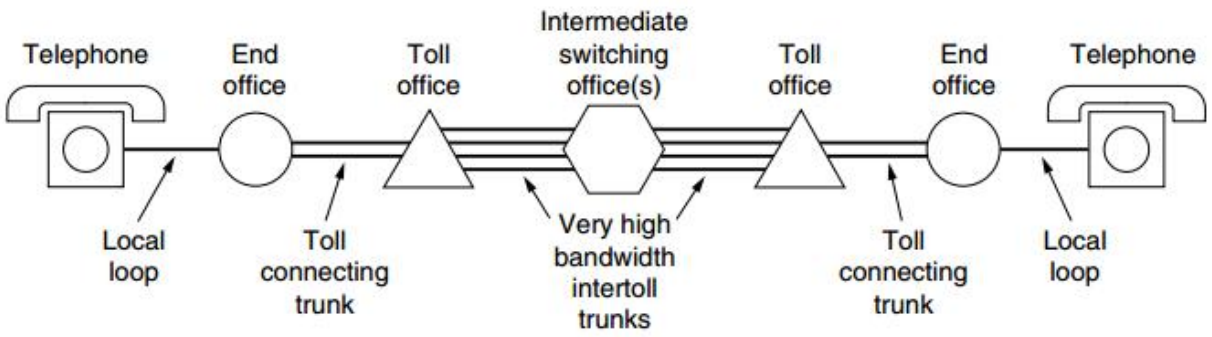


Figure 2-30. A typical circuit route for a long-distance call.

summary, the telephone system consists of three major components:

1. Local loops (analog twisted pairs going to houses and businesses).
2. Trunks (digital fiber optic links connecting the switching offices).
3. Switching offices (where calls are moved from one trunk to another).

The function of each component in the circuit route for a long-distance call is as follows:

- **Caller's phone:** The caller's phone is used to initiate the call and transmit the voice signals over the local loop to the local central office.

- **Local Central Office:** The local central office connects the caller's phone to the wider telephone network and routes the call to the toll office.
- **Toll Office:** The toll office is responsible for routing the call between different local calling areas and connecting it to the interexchange carrier's network.
- **Interexchange Carrier:** The interexchange carrier provides long-distance telephone service between different regions or areas. It connects the call to the distant toll office using interexchange trunks.
- **Distant Toll Office:** The distant toll office receives the call from the interexchange carrier and routes it to the distant central office.
- **Distant Central Office:** The distant central office connects the call to the receiver's phone and transmits the voice signals over the local loop.
- **Receiver's phone:** The receiver's phone receives the call and transmits the voice signals over the local loop to the distant central office.

Q28. Define the Local Loop: Modems, ADSL, and Fiber

The Local Loop is the physical connection between a customer's premises and the local telephone exchange or central office of a telecommunications provider. The Local Loop is the last mile of the telecommunications network and is responsible for connecting a customer's telephone, internet, and other communication services to the provider's network.

Modems are devices that modulate and demodulate signals over the Local Loop. Modems convert digital data from a computer or other device into analog signals that can be transmitted over the Local Loop and vice versa. Modems are used for both dial-up and broadband connections and are typically connected to the Local Loop through a telephone jack.

ADSL, or Asymmetric Digital Subscriber Line, is a technology used to provide high-speed internet access over the Local Loop. ADSL works by dividing the Local Loop into two frequency bands, one for voice communication and the other for data transmission. ADSL provides faster download speeds than upload speeds, hence the term "asymmetric." ADSL requires an ADSL modem to convert the digital data into an ADSL signal that can be transmitted over the Local Loop.

Fiber is a newer technology for providing high-speed internet access over the Local Loop. Fiber optic cables use light to transmit data over the Local Loop, providing much faster data transfer rates than copper cables used in traditional telephone networks. Fiber requires a different type of modem, known as an Optical Network Terminal (ONT), to convert the light signals into digital data that can be used by a computer or other device. Fiber is becoming more widely available but is still not as widely deployed as ADSL or traditional copper-based telephone networks.

Q29. Define ADSL, DSL, xDSL

ADSL, DSL, and xDSL are all digital subscriber line technologies that provide high-speed internet access over traditional copper telephone lines. Here's a brief explanation of each technology:

- DSL (Digital Subscriber Line): DSL is a technology that provides high-speed internet access over traditional copper telephone lines. It works by dividing the existing telephone line into two separate channels, one for voice and one for data. The data channel uses a higher frequency than the voice channel, allowing for faster data transfer rates. DSL is a generic term that refers to all types of digital subscriber line technologies.
- ADSL (Asymmetric Digital Subscriber Line): ADSL is a type of DSL technology that provides faster download speeds than upload speeds. It is called "asymmetric" because the download speed is typically much faster than the upload speed. ADSL works by using different frequencies for upstream and downstream data transmission.
- xDSL (Digital Subscriber Line): xDSL is a term that refers to all types of DSL technologies, including ADSL, SDSL (Symmetric Digital Subscriber Line), VDSL (Very High Bitrate Digital Subscriber Line), and others. The "x" in xDSL stands for "any," as there are several different variations of DSL technology.

Overall, DSL and its various types, like ADSL and xDS,L provide a cost-effective way to deliver high-speed internet access to customers over existing copper telephone lins, without requiring significant infrastructure upgrades.

Q30. Draw a typical ADSL equipment configuration. Also, explain the function of its components. ***

Here is a diagram of a typical ADSL equipment configuration:

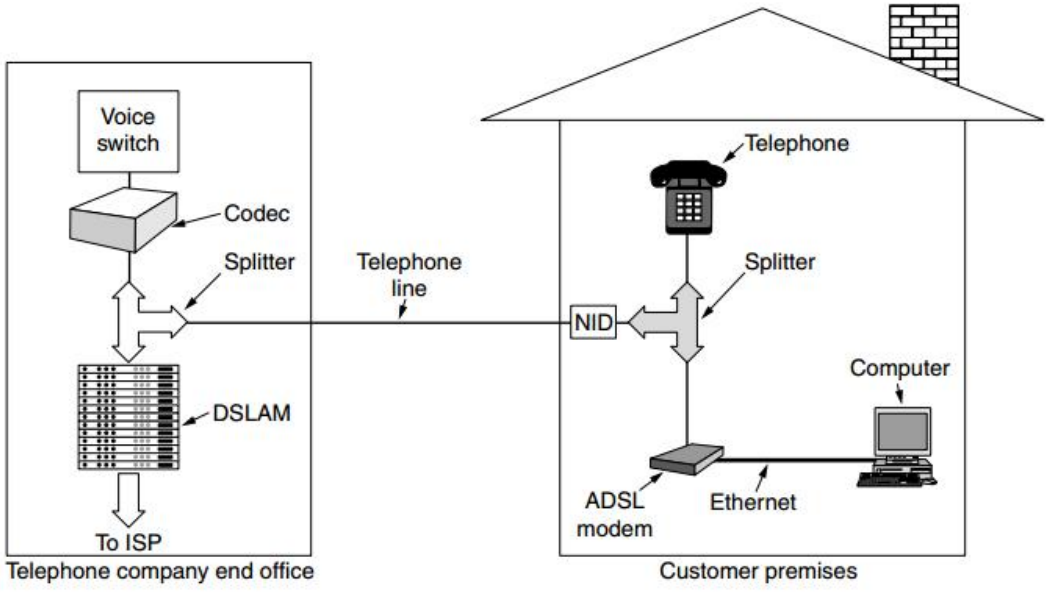


Figure 2-35. A typical ADSL equipment configuration.

The function of each component in the ADSL equipment configuration is as follows:

- **Telephone Line:** The telephone line provides the physical connection between the ADSL modem and the telephone exchange. It carries the ADSL signal between the two devices.
- **ADSL Modem:** The ADSL (Asymmetric Digital Subscriber Line) modem receives the ADSL signal from the telephone line and converts it into digital data that can be used by the computer or router to connect to the internet. It also modulates the data from the computer or router into an ADSL signal that can be transmitted over the telephone line.
- **Computer or Router:** The computer or router connects to the ADSL modem and uses the internet connection to access online resources. It sends data to the ADSL modem for modulation and transmission over the telephone line and receives data from the ADSL modem that has been demodulated from the ADSL signal. It then processes this data and presents it to the user in the form of web pages, emails or other online resources.
- **NID:** A telephone company technician must install a NID (Network Interface Device) on the customer's premises. This small plastic box marks the end of the telephone company's property and the start of the customer's property. Close to the NID (or sometimes combined with it) is a splitter, an analog filter that separates the by POTS from the data.

At the other end of the wire, on the end office side, a corresponding splitter is installed. Here, the voice portion of the signal is filtered out and sent to the normal voice switch. The signal above 26 kHz is routed to a new kind of device called a DSLAM (Digital Subscriber Line Access Multiplexer), which contains the same kind of digital signal processor as the ADSL modem. Once the bits have been recovered from the signal, packets are formed and sent off to the ISP.

Q31. Define SONET/SDH

SONET (Synchronous Optical Network) and SDH (Synchronous Digital Hierarchy) are two related standards for synchronous data transmission over fiber-optic networks.

SONET was developed in the United States, while SDH was developed in Europe, but both standards perform the same basic function of providing a standard for multiplexing multiple digital signals onto a single optical fiber for high-speed communication. They also provide a standardized framework for network management, performance monitoring, and fault detection.

SONET/SDH allow for transmission rates ranging from 51.84 Mbps up to 10 Gbps, and even higher in some cases. The main benefit of SONET/SDH is its ability to carry both voice and data traffic over long distances, making it a critical technology for telecommunications networks.

Q32. What is Switching? Define Circuit Switching, Packet Switching? Differentiate between Packet Switching and Circuit Switching? ***

- **Switching** is the process of directing data between devices on a network. It involves the use of specialized hardware or software that manages the flow of data between devices, ensuring that packets of data are sent to their intended destination.

There are two primary types of switching: circuit switching and packet switching.

Circuit switching is a method of establishing a dedicated communication path between two devices before any data is transmitted. In circuit switching, a physical path is created between two devices for the duration of the communication session. This ensures that the bandwidth is reserved for the duration of the session and guarantees that no other traffic can use that path during that time. Circuit switching is commonly used in traditional telephone networks.

Packet switching, on the other hand, is a method of transmitting data across a network by breaking it up into small packets and sending each packet individually. Each packet contains information about its destination, and the network devices use this information to route the packet to its destination. Unlike circuit switching, packet switching allows multiple packets to share the same network resources simultaneously, and the available bandwidth is dynamically allocated to each packet as needed. Packet switching is the dominant method of data transmission on the Internet and most modern computer networks.

Here is a summary of the key differences between packet switching and circuit switching:

Feature	Packet Switching	Circuit Switching
Type of Connection	Connectionless	Connection-oriented
Resource Allocation	Dynamic allocation	Dedicated allocation
Bandwidth Utilization	Shared by multiple packets	Dedicated to a single connection
Delay	Variable delay	Fixed delay
Network Congestion	Can lead to network congestion	Less likely to lead to network congestion
Quality of Service	QoS can be difficult to guarantee	QoS can be guaranteed
Examples	Internet	Traditional telephone networks

In summary, packet switching is more flexible and adaptable, while circuit switching provides a dedicated connection and higher quality of service.

Q33. Explain Circuit switching and Packet switching with timing events also distinguish between them. ***

Circuit switching and packet switching are two different methods used in telecommunications networks for transmitting data between two devices. Here's an explanation of both methods with timing events and a comparison between them:

Circuit Switching: In circuit switching, a dedicated communication path is established between the two communicating devices before any data is transmitted. This path remains open for the duration of the communication, and the resources used by this path are exclusively dedicated to this communication. The communication path is divided into time slots, and the resources are allocated to these time slots in a fixed manner.

Here's an example of how circuit switching works with timing events:

- Caller picks up the phone and initiates a call
- The network establishes a dedicated connection between the caller and the receiver
- The connection remains open for the duration of the call
- When the call is finished, the connection is terminated and the resources are released.

Packet Switching: In packet switching, data is broken up into small packets, and each packet is sent individually over the network. Each packet is sent independently and can take a different route through the network. Each packet contains a header that specifies its destination and other relevant information. The packets are reassembled at the receiver's end to form the original data.

Here's an example of how packet switching works with timing events:

- Sender breaks up data into packets and sends them over the network
- Each packet takes a different route through the network
- The receiver's device receives the packets and reassembles them into the original data
- The communication is completed.

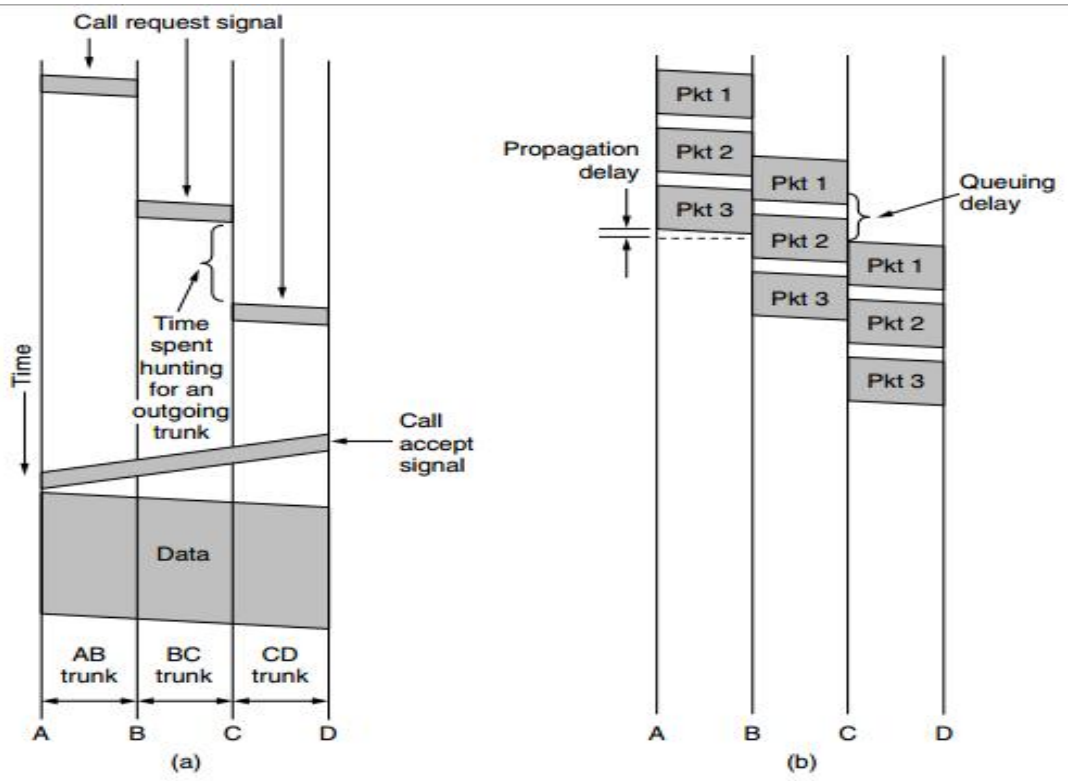


Figure 2-43. Timing of events in (a) circuit switching, (b) packet switching.

Comparison or Distinguish:

- Circuit switching is dedicated to a single communication path, while packet switching allows multiple communications to be transmitted simultaneously over the same network.
- Circuit switching is more reliable than packet switching because it establishes a dedicated path between the two devices, while packet switching is susceptible to network congestion and packet loss.
- Circuit switching requires all resources to be reserved for the entire duration of the communication, while packet switching dynamically allocates network resources as needed for each packet.
- Circuit switching is used for real-time applications such as voice and video calls, while packet switching is used for applications that can tolerate some delay, such as file transfers and email.

In summary, circuit switching and packet switching are two different methods used in telecommunications networks for transmitting data. Circuit switching establishes a dedicated path between two devices and is more reliable, while packet switching breaks up data into small packets and allows multiple communications to be transmitted simultaneously over the same network. Circuit switching is used for real-time applications, while packet switching is used for applications that can tolerate some delay.

Q34. What are the Functions performed by the data link layer? **

The data link layer is the second layer of the OSI (Open Systems Interconnection) model and is responsible for providing reliable data transfer across a physical link between network nodes. The main functions performed by the data link layer include:

- **Framing**: The data link layer divides the stream of bits it receives from the network layer into manageable data units called frames. Each frame includes a header, data payload, and a trailer that provides error detection and correction capabilities.
- **Physical addressing:** The data link layer adds a physical address, such as a Media Access Control (MAC) address, to the header of each frame to identify the source and destination of the data on the physical network.
- **Flow control:** The data link layer manages the flow of data between two network nodes to prevent data loss or corruption due to overflow or congestion.
- **Error detection and correction:** The data link layer includes error detection and correction mechanisms to ensure that data is transferred accurately and without corruption.
- **Access control:** The data link layer also manages access to the network medium by implementing protocols such as Carrier Sense Multiple Access with Collision Detection (CSMA/CD) in Ethernet networks.
- **Logical link control:** The data link layer provides a logical link control sub-layer that manages the establishment, maintenance, and termination of logical connections between nodes in a network.

In summary, the data link layer performs a variety of critical functions that ensure reliable data transfer and network communication. It provides framing, addressing, flow control, error detection and correction, access control, and logical link control to facilitate communication between network nodes.

Q35. Describe framing and its method.

Framing is the process of breaking down a stream of data into smaller, more manageable units called frames. Each frame contains a header, data payload, and trailer, which provide information necessary for the reliable transmission of data across a network.

The header of a frame includes information about the frame itself, such as the frame's start and end, the type of data contained in the frame, and the addressing information necessary for the frame to be routed to its destination. The data payload contains the actual data being transmitted, while the trailer provides error detection and correction information to ensure that the data is transferred accurately and without corruption.

The two most common methods used for framing are character stuffing and bit stuffing:

- Character stuffing: Character stuffing is used when data contains special characters that can be confused with framing characters. To avoid this confusion, an additional character, called a "flag," is added to the beginning and end of each frame to indicate the start and end of the frame. If the data contains the flag character, an additional escape character is added before it to indicate that the character is not the flag but part of the data.
- Bit stuffing: Bit stuffing is used when data contains long runs of 1s or 0s, which can cause synchronization problems. In bit stuffing, an additional bit, called a "flag," is added to the beginning and end of each frame to indicate the start and end of the frame. If the data contains a run of 5 or more consecutive 1s, an extra 0 is inserted after the fifth 1 to avoid synchronization issues.

In summary, framing is the process of breaking down a stream of data into smaller units called frames, which include a header, data payload, and trailer. The two most common methods used for framing are character stuffing and bit stuffing, which ensure the reliable transmission of data across a network.

Q36. Suppose a message M=10101. Find the transmitted code and correct the received code when there is error using Hamming method with even parity. ***

To generate the Hamming code with even parity, we need to follow the steps below:

1. Determine the number of parity bits required

We can calculate the number of parity bits required using the following formula:

2^r >= m + r + 1

Where:

r = number of parity bits
m = number of message bits

In this case, we have m = 5, so we need to find the smallest value of r that satisfies the above inequality:

2^r >= 5 + r + 1
2^r >= r + 6
From trial and error, we can see that r = 3 satisfies this inequality, so we need 3 parity bits.

2. Insert the parity bits

We insert the parity bits into the Hamming code at positions that are powers of 2 (i.e., 1, 2, 4, 8, etc.). The parity bit at position i checks all the bits whose binary representation includes the i-th bit (e.g., the parity bit at position 1 checks bits 1, 3, 5, 7, etc.).

3. Calculate the parity bits

For each parity bit, we calculate its value by XOR-ing the message and check bits that correspond to its position. For example, the parity bit at position 1 checks bits 1, 3, 5, 7, so we XOR them as follows:

P1 = M3 XOR M5 XOR M7 = 1 XOR 0 XOR 1 = 0

Similarly, we calculate the values of P2 and P3:

P2 = M3 XOR M6 XOR M7 = 1 XOR 1 XOR 1 = 1

P3 = M5 XOR M6 XOR M7 = 0 XOR 1 XOR 1 = 0

4. Construct the Hamming code

We insert the parity bits into the Hamming code at their respective positions to get the transmitted code:
T = P1 P2 M3 P3 M5 M6 M7
T = 0101011

Suppose that during transmission, the third bit (M3) is flipped, resulting in the received code:
R = 1111011

5. Detect the error

We can detect the error by calculating the parity bits for the received code and comparing them to the transmitted parity bits. If there is a mismatch, then we know there was an error.

P1' = R3 XOR R5 XOR R7 = 1 XOR 1 XOR 1 = 1

P2' = R3 XOR R6 XOR R7 = 1 XOR 1 XOR 1 = 1

P3' = R5 XOR R6 XOR R7 = 0 XOR 1 XOR 1 = 0

Comparing P1' with P1, P2' with P2, and P3' with P3, we see that P1' and P2' do not match their corresponding transmitted parity bits, indicating that there was an error in the third bit.

6. Correct the error

To correct the error, we can use the Hamming distance to determine which bit to flip. The Hamming distance is the number of bits that are different between two codes. In this case, the Hamming distance between R and T is 2, so we know that there is one error that can be corrected.

To correct the error, we flip the bit at the position corresponding to the XOR of the positions of the incorrect parity bits:

E = 2^0 + 2^1 = 3

R[E] = 1 -> flip to 0

Q37. Suppose a message M=11100. Find the transmitted code and correct the received code when there is error using Hamming method with even parity. ***

- To use Hamming method with even parity, we need to add parity bits to the message to detect and correct errors.

Step 1: Determine the number of parity bits required.

To determine the number of parity bits required, we use the formula:
2^r >= m + r + 1

where:
r = number of parity bits
m = length of message

For m = 5 (11100), we have:

2^r >= 5 + r + 1
2^r >= 6 + r
Trying different values of r, we find that the smallest value of r that satisfies the inequality is 3. So we need 3 parity bits.

Step 2: Insert the message bits into the code word.

We insert the message bits into the code word at positions that are powers of 2 (1, 2, 4, 8, ...). The remaining positions are reserved for the parity bits. For even parity, we set the parity bits to 0 or 1 so that the total number of 1's in the positions they cover (including themselves) is even.

The code word with the message M=11100 is:
P1 P2 M1 P3 M2 M3 M4
0 1 1 0 1 1 0
where P1, P2, and P3 are the parity bits.

Step 3: Check for errors.

To check for errors, we calculate the values of the parity bits using the same scheme as in Step 2. We then compare the calculated parity bits with the received parity bits. If there is a mismatch, we can determine the position of the error by looking at the parity bit positions.

Suppose the received code word is:

P1 P2 R1 P3 R2 M4 M5
0 1 0 0 1 0 0

We calculate the parity bits:

P1 = R1 XOR R2 XOR M4 = 0 XOR 1 XOR 0 = 1
P2 = R1 XOR M4 XOR M5 = 0 XOR 0 XOR 0 = 0
P3 = R2 XOR M4 XOR M5 = 1 XOR 0 XOR 0 = 1
Comparing the calculated parity bits with the received parity bits, we see that there is an error in position 5 (M2), since P2 is incorrect. We can correct the error by flipping the bit at position 5:

P1 P2 R1 P3 R2 M4 M5
0 1 0 0 1 0 0
^
|
flip this bit

The corrected code word is:

P1 P2 R1 P3 R2 M4 M5
0 1 0 0 1 0 1
The message is then obtained by extracting the message bits (ignoring the parity bits):

M = M1 M2 M3 = 1 0 0

Therefore, the transmitted code is 0110100 and the corrected received code is 0101101.

Q38. Define framing. Explain the framing method bit stuffing with an example. **

Framing is a process used in data communications to divide a stream of data into smaller, more manageable units called frames. Each frame consists of a header, a payload, and a trailer. The header provides information about the frame itself, such as the starting and ending points, and the trailer provides error detection and correction capabilities.

Bit stuffing is a specific method of framing that is used to avoid synchronization problems when data contains long runs of 1s or 0s. In bit stuffing, an extra 0 bit is inserted into the data stream after a predetermined number of consecutive 1 bits, or vice versa, to prevent the receiver from mistaking the data for the synchronization pattern.

Here is an example of how bit stuffing works:

Suppose we want to transmit the binary data stream "111110111101111" across a communication channel that uses bit stuffing with a maximum of five consecutive 1s allowed. The data would be framed as follows:

- The first frame would consist of the start flag (01111110) and the first five data bits (11111), resulting in the frame "01111110 111110."
- The second frame would consist of the next five data bits (01111), the inserted 0 bit, and the last five data bits (11011), resulting in the frame "01111110 011110 0111110."
- The third and final frame would consist of the remaining four data bits (1111) and the end flag (01111110), resulting in the frame "01111110 11110 01111110."

At the receiving end, the frames are reconstructed by stripping off the start and end flags and removing any stuffed bits. This process ensures that the original data is transmitted accurately and without any synchronization problems.

In summary, bit stuffing is a framing method used to ensure that data is transmitted accurately across a communication channel. It involves the insertion of an extra bit into the data stream after a predetermined number of consecutive bits to avoid synchronization problems at the receiving end.

Q39. What does the data link layer perform for the Design issues/Functions? **

-The data link layer is responsible for providing reliable communication between two nodes that are directly connected by a physical communication link. Some of the key design issues/functions of the data link layer include:

1. **Framing:** The data link layer divides the incoming data into frames and adds a header and trailer to each frame to facilitate identification, error detection, and error correction.
2. **Addressing:** The data link layer adds source and destination addresses to each frame to ensure that the frame is delivered to the intended recipient.
3. **Error control:** The data link layer uses various error detection and correction techniques, such as checksums and retransmission, to ensure that the data is transmitted without errors.
4. **Flow control:** The data link layer uses techniques such as windowing and buffering to control the flow of data between the sender and receiver and to prevent data loss or congestion.
5. **Access control:** The data link layer is responsible for controlling access to the communication channel to ensure that multiple devices can share the channel without interfering with each other. This can be achieved through techniques such as time-division multiplexing, frequency-division multiplexing, or carrier sense multiple access.

Overall, the data link layer plays a critical role in ensuring reliable and efficient communication between two directly connected nodes in a network.

Q40. Describe framing with byte stuffing. **

- Framing is the process of dividing a stream of data into smaller, more manageable units called frames. In the data link layer of a network, framing is used to transmit data between two nodes that are directly connected by a communication link.

One common technique used for framing is byte stuffing. In byte stuffing, a special flag byte is used to mark the beginning and end of each frame. However, if the flag byte appears within the data of the frame, it could be mistaken for the end of the frame and cause errors in the transmission.

To prevent this problem, a technique called byte stuffing is used. In byte stuffing, an additional byte is added to the data whenever the flag byte appears within the data of the frame. This additional byte is called an escape character or escape sequence.

When a flag byte is encountered within the data, the sender replaces it with the escape sequence, consisting of two bytes. The first byte is the escape character, and the second byte is a code indicating the original byte that was replaced. The receiver then knows to replace the escape sequence with the original byte.

This process ensures that the flag byte is not mistaken for the end of the frame and that the data is transmitted without errors. The receiver can detect the end of the frame by detecting the flag byte at the end of the frame. Byte stuffing is a commonly used technique for framing in data link layer protocols such as HDLC and PPP.

Chapter#4 The MAC Sublayer

Q41. What is MAC? **

- The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

The data link layer is the second lowest layer. It is divided into two sublayers –

a) The logical link control (LLC) sublayer

b) The medium access control (MAC) sublayer

Q42.What are the assumptions of Dynamic channel allocation? **

- Dynamic channel allocation (DCA) is a method of allocating channels dynamically in a wireless network. The assumptions of DCA include:

1. Independent Traffic: The model consists of N independent stations (e.g., computers, telephones), each with a program or user that generates frames for transmission. The expected number of frames generated in an interval of length Δt is $\lambda \Delta t$, where λ is a constant (the arrival rate of new frames). Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.

2. Single Channel: A single channel is available for all communication. All stations can transmit on it and all can receive from it. The stations are assumed to be equally capable, though protocols may assign them different roles (e.g., priorities).

3. Observable Collisions: If two frames are transmitted simultaneously, they overlap in time and the resulting signal is garbled. This event is called a collision. All stations can detect that a collision has occurred. A collided frame must be transmitted again later. No errors other than those generated by collisions occur.

4. Continuous or Slotted Time: Time may be assumed continuous, in which case frame transmission can begin at any instant. Alternatively, time may be slotted or divided into discrete intervals (called slots). Frame transmissions must then begin at the start of a slot. A slot may

contain 0, 1, or more frames, corresponding to an idle slot, a successful transmission, or a collision, respectively.

5. Carrier Sense or No Carrier Sense: With the carrier sense assumption, stations can tell if the channel is in use before trying to use it. No station will attempt to use the channel while it is sensed as busy. If there is no carrier sense, stations cannot sense the channel before trying to use it. They just go ahead and transmit. Only later can they determine whether the transmission was successful.

Q43. Explain the frame generation in an ALOHA system. Or Illustrate the frame generation technique in an ALOHA system. ***

- In an ALOHA system, frame generation involves creating packets of data that are to be transmitted over the network. The following steps describe the frame generation process in an ALOHA system:

1. **Data encapsulation:** The data to be transmitted is first encapsulated into a packet that includes a header and a payload. The header contains information such as the source and destination addresses, packet length, and other control information.
2. **Adding a frame check sequence:** A frame check sequence (FCS) is added to the packet. The FCS is a checksum that is used to detect errors in the data during transmission.
3. **Setting the transmission time:** The packet is assigned a random transmission time based on the ALOHA protocol. In pure ALOHA, the transmission time is completely random. In slotted ALOHA, the transmission time is aligned with the time slots used by the system.
4. **Transmitting the packet:** When the assigned transmission time arrives, the packet is transmitted over the network. If the transmission is successful, the receiving device sends an acknowledgment back to the transmitting device. If the transmission fails, the transmitting device waits for a random amount of time and then retries the transmission.
5. **Repeat steps 1-4:** The process of generating and transmitting packets is repeated for each packet of data that needs to be transmitted over the network.

The frame generation process in an ALOHA system is designed to be simple and efficient, allowing devices to transmit data without the need for complex coordination or scheduling mechanisms. However, the random nature of the transmission times can lead to collisions and inefficiencies in the system, particularly when the network is heavily loaded.

Q44. Distinguish between Pure ALOHA and Slotted ALOHA. ***

- The differences between Pure ALOHA and Slotted ALOHA:

Feature	Pure ALOHA	Slotted ALOHA
Time Division	Continuous	Divided into equal time slots
Transmission Timing	Completely random	Aligned with time slots
Transmission Window	Unlimited	Limited to one time slot
Efficiency	Low (18% maximum)	Higher (36% maximum)
Collision Probability	High	Lower than pure ALOHA
System Complexity	Simple	Slightly more complex

In Pure ALOHA, transmissions can occur at any time and can potentially collide with other transmissions, which reduces the efficiency of the system. In Slotted ALOHA, the transmission time is divided into equal time slots, and transmissions are aligned with these slots, reducing the probability of collisions and improving the efficiency of the system.

In Pure ALOHA, there is no limit on the transmission window, which means that a device can keep attempting transmission until it is successful. In Slotted ALOHA, the transmission window is limited to one time slot, which helps to reduce collisions and improve efficiency.

Overall, Slotted ALOHA is more efficient than Pure ALOHA, as it reduces the probability of collisions and makes better use of the available transmission time. However, it is slightly more complex than Pure ALOHA due to the need to synchronize transmissions with time slots.

Q45. Explain CSMA with Collision Detection also draw the figure? *

- CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is a media access control method used in Ethernet networks. It allows multiple devices to share a common communication medium by transmitting data in a controlled manner, minimizing the chances of data collisions.

The basic principle of CSMA/CD is that a device listens to the communication medium (e.g. Ethernet cable) before transmitting data. If the medium is idle (no other device is transmitting), the device can begin transmitting its data. However, if the medium is busy (another device is transmitting), the device must wait until the medium is free before transmitting its own data.

The algorithm/process of CSMA/CD is:

1. When a frame is ready, the transmitting station checks whether the channel is idle or busy.

2. If the channel is busy, the station waits until the channel becomes idle.
3. If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.
4. If a collision is detected, the station starts the collision resolution algorithm.
5. The station resets the retransmission counters and completes frame transmission.

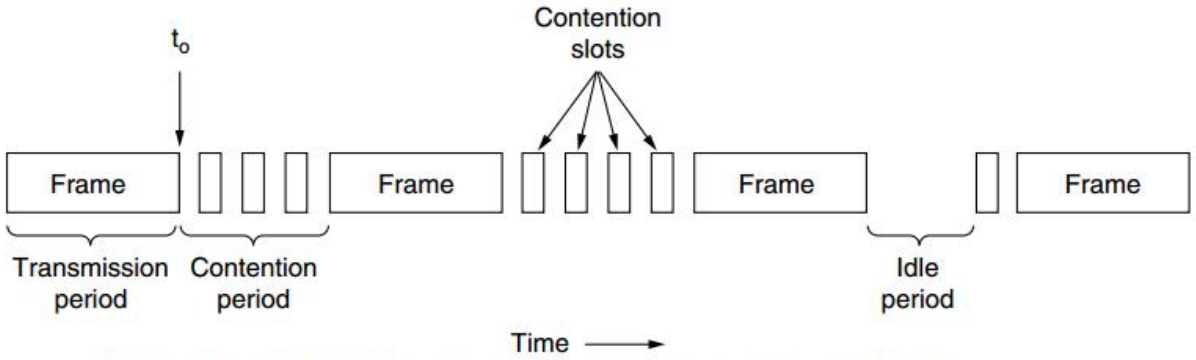


Figure 4-5. CSMA/CD can be in contention, transmission, or idle state.

Therefore, our model for CSMA/CD will consist of alternating contention and transmission periods, with idle periods occurring when all stations are quiet (e.g., for lack of work).

Q46. What is WiMAX?

- WiMAX (Worldwide Interoperability for Microwave Access) is a wireless broadband communication technology based on the IEEE 802.16 standard. It is designed to provide high-speed wireless access over a wide area, similar to Wi-Fi but with a larger coverage range and higher data transfer rates.

WiMAX can operate in both licensed and unlicensed frequency bands, providing a flexible solution for wireless broadband access. It uses a point-to-multipoint architecture, allowing multiple devices to connect to a single base station over a large area, such as a city or rural region. WiMAX also supports Quality of Service (QoS) features, allowing for prioritization of data traffic based on user requirements.

WiMAX has several advantages over traditional wired broadband technologies, such as cable or DSL. It can provide high-speed internet access to areas that are difficult to reach with wired connections, such as rural or remote areas. It also has a lower infrastructure cost compared to wired broadband, as it requires fewer physical cables and equipment.

WiMAX has several applications, including providing broadband access to homes and businesses, connecting mobile devices to the internet, and providing backhaul for cellular networks. However, the adoption of WiMAX has been slower than expected, and it has faced competition from other wireless broadband technologies, such as LTE (Long-Term Evolution) and 5G.

Overall, WiMAX is a wireless broadband technology that provides high-speed internet access over a wide area. It has several advantages over traditional wired broadband technologies, but it has faced competition from other wireless broadband technologies and has not achieved widespread adoption.

Q47. Comparison of 802.16 with 802.11 and 3G. *

- Here is a comparison table between 802.16, 802.11, and 3G technologies:

Features	802.16 (WiMAX)	802.11 (Wi-Fi)	3G
Frequency Band	2-66 GHz	2.4 GHz and 5 GHz	1.9 GHz
Coverage Range	Up to 50 km	Up to 100 m	Up to 10 km
Data Transfer Rate	Up to 75 Mbps	Up to 600 Mbps	Up to 2 Mbps
Quality of Service (QoS)	Yes	Limited	Yes
Point-to-Multipoint Architecture	Yes	No	No
Mobility	Limited	High	High
Backward Compatibility	No	Yes	Yes
Application	Broadband Access	Local Area Networking	Cellular Telephony

As seen in the table, each technology has its own set of advantages and disadvantages. 802.16 has a larger coverage range and supports QoS, making it suitable for broadband access applications. Wi-Fi (802.11) has higher data transfer rates and high mobility, making it suitable for local area networking applications. 3G provides cellular telephony and is widely used for mobile data applications.

However, it is important to note that these technologies are not mutually exclusive and can complement each other. For example, WiMAX can be used to provide broadband access to areas where wired connections are difficult to reach, and Wi-Fi can be used to provide local wireless connectivity within buildings. 3G can be used to provide mobile data access in areas where WiMAX or Wi-Fi are not available.

Q48. What is RFID? How does RFID work? ***

- RFID (Radio Frequency Identification) is a technology that uses radio waves to identify and track objects or people.

RFID (Radio-Frequency Identification) is a technology that uses radio waves to automatically identify and track objects. It is a wireless communication technology that enables contactless communication

between a reader and an RFID tag attached to an object. The RFID system consists of three basic components: the RFID tag, the reader, and the backend software.

The basic components of an RFID network include:

1. **RFID Tags:** An RFID tag is a small device that contains an antenna and a microchip. The microchip stores information about the object or person being tracked, such as its unique identifier or product details. The antenna allows the tag to communicate with an RFID reader using radio waves. RFID tags come in a variety of shapes and sizes, from small adhesive labels to ruggedized tags used in harsh environments.

2. **RFID Readers:** An RFID reader is a device that sends out radio waves to communicate with RFID tags. The reader captures the information stored on the tag and sends it to a backend system for processing. RFID readers can be fixed or handheld and can be configured to read tags at different distances and frequencies.

3. **Antennas:** Antennas are used to transmit and receive radio waves between RFID tags and readers. They can be integrated into readers or mounted separately to provide greater flexibility in reading tags. Antennas come in a variety of sizes and shapes and can be designed to read tags at specific frequencies and ranges.

4. **Backend System:** The backend system is responsible for processing the data collected by RFID readers. This system can include a database for storing tag information, software for managing and analyzing the data, and applications for integrating the data into other systems.

Here's a diagram that shows the basic components of an RFID network:

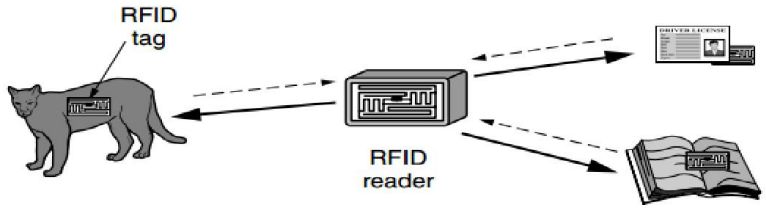


Figure 1-36. RFID used to network everyday objects.

In this diagram, the RFID tag communicates with the RFID reader using radio waves. The reader captures the data from the tag and sends it to the backend system for processing. The backend system can then store the data in a database, analyze it, or integrate it into other systems.

Q49. Describe The 802.16 Architecture and Protocol Stack. *

- The 802.16 standard, also known as WiMAX (Worldwide Interoperability for Microwave Access), defines the architecture and protocol stack for a wireless broadband access network. The 802.16 architecture consists of two main components: the Access Service Network (ASN) and the Connectivity Service Network (CSN).

The Access Service Network (ASN) is responsible for providing wireless access to subscriber stations (SS) in a specific coverage area. It consists of two main elements: the Base Station (BS) and the Subscriber Station (SS). The Base Station acts as a gateway between the wireless network and the wired infrastructure, and it communicates with multiple subscriber stations. The Subscriber Station communicates with the Base Station to access the network and provides a wireless connection to end-users.

The Connectivity Service Network (CSN) is responsible for managing the overall network operations and services. It consists of several network elements, including the Authentication, Authorization, and Accounting (AAA) server, the Home Agent (HA), and the Gateways. The AAA server authenticates and authorizes subscribers to access the network, and it keeps track of usage for billing purposes. The Home Agent manages the mobility of subscribers across different base stations, and the Gateways provide interconnection between the WiMAX network and other networks such as the Internet.

The 802.16 protocol stack consists of three main layers: the Physical Layer (PHY), the Medium Access Control (MAC) Layer, and the Convergence Sublayer (CS). The Physical Layer is responsible for transmitting and receiving data over the wireless medium. It uses different modulation techniques and coding schemes to provide high throughput and low latency. The Medium Access Control Layer is responsible for managing the access to the wireless medium and providing quality of service (QoS) guarantees. It uses different access methods such as Time Division Multiple Access (TDMA) and Orthogonal Frequency Division Multiple Access (OFDMA) to allocate the wireless resources to different users. The Convergence Sublayer is responsible for converting the data from higher layer protocols to the 802.16 format and vice versa.

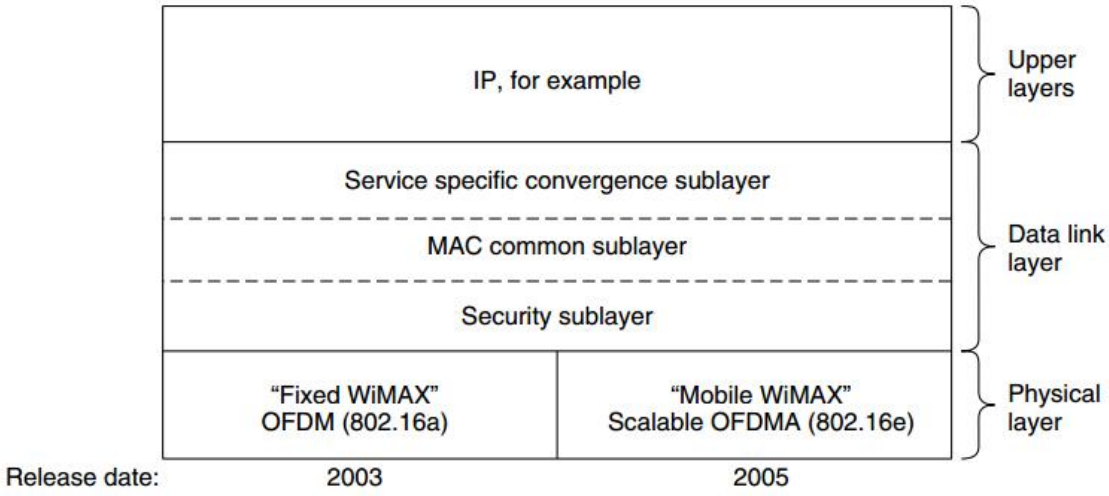


Figure 4-31. The 802.16 protocol stack.

Overall, the 802.16 architecture and protocol stack provide a flexible and scalable framework for deploying wireless broadband access networks. It enables high-speed data transfer, supports mobility, and provides quality of service guarantees for different types of applications.

Q50. Write Short note on Ethernet, Bluetooth.

- Ethernet:

1. Ethernet is a wired networking technology that uses a physical cable to transmit data between devices and is widely used in local area networks (LANs).
2. Ethernet uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol to manage access to the network and avoid collisions between data packets.
3. Ethernet has evolved over time with faster speeds and improved capabilities like Power over Ethernet (PoE) and Ethernet over Fiber.

Bluetooth:

1. Bluetooth is a wireless communication technology that enables short-range communication between devices and supports a variety of applications like audio streaming, file transfer, and Internet of Things (IoT) devices.
2. Bluetooth uses radio waves to establish a wireless connection between devices and supports multiple devices to connect to the same network simultaneously.
3. Bluetooth has evolved over time with improved speed, range, and security features like Bluetooth Low Energy (BLE) and Bluetooth 5.0.

Q51. Difference between Fast Ethernet Vs Gigabit Ethernet?

- Fast Ethernet and Gigabit Ethernet are both types of Ethernet technologies, but they differ in terms of their speed and other characteristics. Here is a table that compares the two:

Feature	Fast Ethernet	Gigabit Ethernet
Maximum speed	100 Mbps	1000 Mbps (1 Gbps)
Standard	IEEE 802.3u	IEEE 802.3z
Cable type	Category 5 (or higher)	Category 5e (or higher)
Maximum cable length	100 meters	100 meters
Auto-negotiation	Yes	Yes
Duplex	Half or full	Full
Backward compatibility	Yes	Yes
Power consumption	Lower than Gigabit Ethernet	Higher than Fast Ethernet
Cost	Less expensive than Gigabit Ethernet	More expensive than Fast Ethernet

As shown in the table, the main difference between Fast Ethernet and Gigabit Ethernet is their maximum speed, with Gigabit Ethernet offering ten times faster speed than Fast Ethernet. Gigabit Ethernet also has a higher standard, supports higher category cables, and requires more power consumption. However, both technologies support auto-negotiation, duplex mode, and backward compatibility. Gigabit Ethernet is also more expensive than Fast Ethernet due to its higher speed and capabilities.

Q52. What is VLAN?

- A VLAN, or Virtual Local Area Network, is a logical network that allows a group of devices to communicate with each other as if they were on the same physical network, even if they are located in different geographical locations. VLANs are created by dividing a physical network into multiple logical segments, and can be used to improve network security, reduce network congestion, and simplify network management. VLANs are often used in enterprise networks to group devices based on department, location, or function, and can be configured and managed using VLAN tagging and VLAN trunking protocols.

Q53. Distinguish between Hub and Switch.

- Hubs and switches are two types of network devices that are used to connect multiple devices in a local area network (LAN). Although they both perform similar functions, there are significant differences between them. Here is a table that compares hubs and switches:

Feature	Hub	Switch
Function	Shares network bandwidth among all devices	Directs network traffic to specific devices
Ports	Multiple ports for connecting devices	Multiple ports for connecting devices
Transmission Mode	Half duplex	Full duplex
Collision Domain	All devices share the same collision domain, leading to collisions and network congestion	Each port has its own collision domain, reducing collisions and network congestion
Performance	Shared bandwidth leads to slow performance when multiple devices are transmitting data	Directs data only to the devices that need it, leading to better performance
Security	No built-in security features	Supports VLANs, ACLs, and other security features
Cost	Less expensive than switches	More expensive than hubs
Reliability	Single point of failure	Redundant power supplies and network paths for improved reliability

As shown in the table, the main difference between hubs and switches is the way they handle network traffic. Hubs simply forward all data to all connected devices, leading to collisions and network congestion, whereas switches direct data only to the devices that need it, leading to better performance. Switches also support security features like VLANs and ACLs, making them more secure than hubs. Hubs are less expensive than switches but are also less reliable, as they represent a single point of failure in the network.

Q54. Comparison and usage of Repeater, Hub, bridge, switch, router, gateway. ***

- Repeaters, hubs, bridges, switches, routers, and gateways are all network devices used to connect devices together in a local area network (LAN) or a wide area network (WAN). Here is a comparison of the devices and their common usage:

1. Repeater: A repeater is a network device that amplifies or regenerates signals to extend the range of a network. It operates at the physical layer of the OSI model and can be used to extend the distance of a network segment. Repeaters are commonly used in long-distance fiber optic networks and in wireless networks.
2. Hub: A hub is a network device that connects multiple devices together in a LAN. It operates at the physical layer of the OSI model and broadcasts all data to all connected devices, creating a single collision domain. Hubs are inexpensive and easy to use, but can lead to network congestion and collisions.
3. Bridge: A bridge is a network device that connects two LAN segments together and forwards data between them based on their MAC addresses. It operates at the data link layer of the OSI model and creates separate collision domains for each LAN segment. Bridges can be used to extend the range of a LAN or to segment a LAN into smaller parts.
4. Switch: A switch is a network device that connects multiple devices together in a LAN and forwards data between them based on their MAC addresses. It operates at the data link layer of the OSI model and provides dedicated bandwidth for each connected device, creating separate collision domains. Switches are more efficient than hubs and can be used to improve network performance.
5. Router: A router is a network device that connects multiple LANs together or connects a LAN to a WAN. It operates at the network layer of the OSI model and forwards data between networks based on their IP addresses. Routers can be used to segment a LAN into smaller parts or to connect multiple LANs together.
6. Gateway: A gateway is a network device that connects two different types of networks together. It translates data between different protocols and formats and can be used to connect a LAN to a WAN or to connect an Ethernet network to a wireless network.

In summary, repeaters and hubs are used to connect multiple devices in a LAN and extend the range of a network. Bridges and switches are used to segment a LAN into smaller parts and improve network performance. Routers are used to connect multiple LANs together or connect a LAN to a WAN. Gateways are used to connect two different types of networks together and translate data between them.

Chapter#5 The Network Layer

Q55. Comparison of Virtual-Circuit and Datagram Networks.

- Both virtual circuits and datagrams have their supporters and their detractors. We will now attempt to summarize both sets of arguments. The major issues are listed in Fig. 5-4, although purists could probably find a counterexample for everything in the figure.

Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Figure 5-4. Comparison of datagram and virtual-circuit networks.

Q56. What is routing algorithm? Define static routing and dynamic routing algorithm.

- A routing algorithm is a computational procedure used by routers to determine the best path for forwarding data packets from a source to a destination in a network. The goal of a routing algorithm is to select the most efficient path to minimize the delay, congestion, and cost of data transmission while avoiding network failures and bottlenecks.

There are two types of routing algorithms:

1. Static routing algorithm: A static routing algorithm is a method of routing that uses a pre-configured routing table to determine the best path for forwarding data packets. In static routing, the routing table is manually configured by a network administrator based on network topology, traffic patterns, and other factors. Once the routing table is set, it does not change unless it is manually updated. Static routing is simple and predictable, but it is not suitable for large, complex, or dynamic networks.
2. Dynamic routing algorithm: A dynamic routing algorithm is a method of routing that uses real-time information to determine the best path for forwarding data packets. In dynamic routing, routers exchange information with each other about network topology, traffic load, and other factors to update their routing tables dynamically. Dynamic routing is more flexible and adaptive than static routing, and it can handle large, complex, and dynamic networks more efficiently. There are several types of dynamic routing protocols, including distance-vector protocols (e.g., RIP), link-state protocols (e.g., OSPF), and hybrid protocols (e.g., EIGRP).

Q57. Describe Shortest Path Algorithm. ***

- Shortest Path Algorithm is a computational algorithm used to determine the shortest path between two nodes in a network. It is a type of routing algorithm used by routers to find the most efficient path for forwarding data packets.

There are several algorithms for finding the shortest path, but the most common ones are Dijkstra's algorithm and Bellman-Ford algorithm.

Dijkstra's algorithm:

- It is a greedy algorithm that selects the closest node first and iteratively updates the distance of each node from the source node until it reaches the destination node.
- It works by maintaining a set of unvisited nodes and a table of the distances from the source node to each node.
- At each iteration, it selects the node with the smallest distance from the source node and updates the distances of its neighboring nodes if a shorter path is found.

1.Graph

A. Node = router

B. Arc = communication line

2.Metric

A. Number of hops

B. Geographic distance

C. Mean queueing and transmission delay

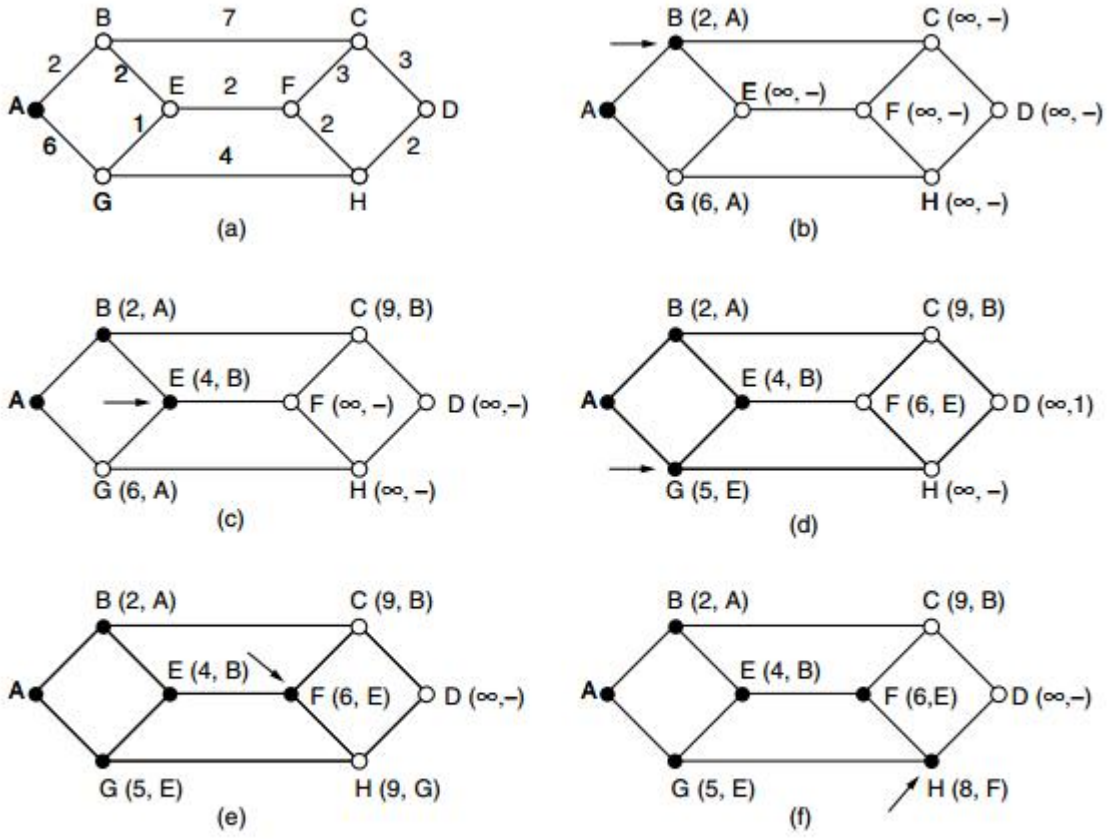


Figure 5-7. The first six steps used in computing the shortest path from *A* to *D*. The arrows indicate the working node.

The concept of a shortest path deserves some explanation. One way of measuring path length is the number of hops. Using this metric, the paths ABC and ABE in Fig. 5-7 are equally long. Another metric is the geographic distance in kilometers, in which case ABC is clearly much longer than ABE (assuming the figure is drawn to scale).

Q58. What is ICMP?

- ICMP stands for Internet Control Message Protocol. It is a network protocol used by routers and other network devices to send error messages and operational information about network conditions.

ICMP is used to:

1. Test and diagnose network connectivity issues: ICMP packets are commonly used to test network connectivity and diagnose network problems, such as detecting packet loss, latency, or congestion.
2. Provide feedback and error messages: ICMP packets are used by routers to send feedback and error messages about network conditions, such as notifying the sender when a packet cannot be delivered due to network errors or when a router or network device is unavailable.
3. Implement network management and monitoring tools: ICMP packets are used by network management and monitoring tools to collect information about network performance and availability, such as measuring response times or monitoring the status of network devices.

ICMP packets are typically encapsulated within IP packets and use different types and codes to convey different messages. For example, ICMP echo requests and replies are used for network testing and diagnostics, while ICMP destination unreachable messages are used for error reporting.

Q59. What is IP address? Illustrate IP address formats. ***

- An IP address is a unique identifier assigned to each device connected to a computer network that uses the Internet Protocol (IP) for communication. It allows devices to communicate with each other over a network, whether it's a local area network (LAN) or the internet.

There are two versions of the Internet Protocol: IPv4 and IPv6. IPv4 addresses are 32-bit numbers, represented in decimal format with four numbers separated by dots. IPv6 addresses are 128-bit numbers, represented in hexadecimal format with eight groups of four hexadecimal digits separated by colons.

Here are examples of both IPv4 and IPv6 address formats:

IPv4 address format: 192.168.1.1

In this example, each number represents 8 bits, so the total size of the address is 32 bits. The address is divided into four octets (groups of eight bits) and represented in decimal format. Each octet can have a value between 0 and 255.

IPv6 address format: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

In this example, each group of four hexadecimal digits represents 16 bits, so the total size of the address is 128 bits. The address is divided into eight groups and represented in hexadecimal format. Leading zeroes can be omitted in each group, and consecutive groups of zeroes can be represented with double colons (::).

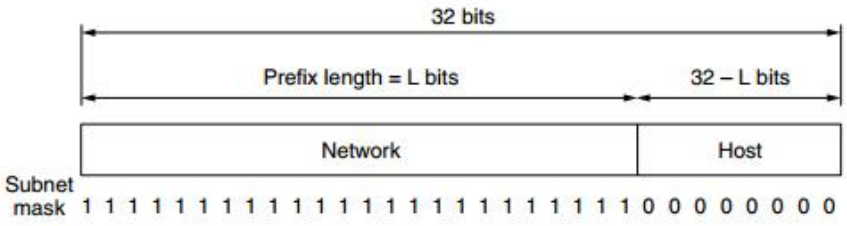


Figure 5-48. An IP prefix and a subnet mask.

IP addresses are assigned to devices either statically or dynamically. Static IP addresses are manually configured, while dynamic IP addresses are assigned by a server using Dynamic Host Configuration Protocol (DHCP).

Q60. Distinguish between IPv4 Vs IPv6. **

- Here is a comparison table between IPv4 and IPv6:

Feature	IPv4	IPv6
Address size	32 bits	128 bits
Address notation	Dotted decimal (e.g. 192.0.2.1)	Colon-hexadecimal (e.g. 2001:0db8:85a3:0000:0000:8a2e:0370:7334)
Address types	Unicast, multicast, broadcast	Unicast, multicast, anycast
Address space	4.3 billion addresses	340 undecillion (3.4 x 10^38) addresses
Address representation	Decimal numbers separated by dots	Eight groups of hexadecimal numbers separated by colons
Address configuration	Static, DHCP	Static, DHCPv6, SLAAC
Fragmentation	Routers perform fragmentation	Endpoints perform fragmentation
Header size	20-60 bytes (variable)	40 bytes (fixed)
Extension headers	Not used	Used for optional features
Security	Optional IPSec support	Built-in IPSec support
QoS support	Limited support	Built-in QoS support

In summary, IPv6 provides a much larger address space, simplified address notation, improved address configuration options, end-to-end fragmentation, built-in security and QoS support, and the use of extension headers for optional features. However, IPv4 is still widely used due to its widespread support and backward compatibility with older systems.

Chapter#6 The Transport Layer

Q61. What is Transport layer? **

- The Transport layer is the fourth layer in the OSI model and the TCP/IP protocol stack. It is responsible for the end-to-end delivery of data between applications running on different hosts. The Transport layer provides services such as segmentation, error control, flow control, and congestion control to ensure that data is transmitted reliably and efficiently.

The Transport layer uses protocols such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) to provide these services. TCP provides reliable, connection-oriented communication, while UDP provides unreliable, connectionless communication with low overhead.

The Transport layer also performs multiplexing and demultiplexing, which means it can handle multiple connections from different applications on the same host and multiplexes the data from different applications into a single stream for transmission. At the receiving end, it demultiplexes the incoming data stream and delivers it to the appropriate application.

Overall, the Transport layer plays a critical role in ensuring that data is transmitted accurately and efficiently between applications running on different hosts, making it an essential component of modern networking.

Q62. Write the services of Transport layer? **

- The Transport layer is the fourth layer of the OSI model and the TCP/IP protocol suite. It provides services that enable communication between applications running on different hosts. The main services provided by the Transport layer include:

1. Connection-oriented communication: The Transport layer can establish a connection between two endpoints before data transfer begins. This ensures reliable data transfer and error recovery.
2. Segmentation and reassembly: The Transport layer can divide large data into smaller segments before transmission and reassemble them at the receiver's end. This helps to optimize network bandwidth and improve data transmission efficiency.

3. Flow control: The Transport layer can regulate the flow of data between two endpoints, preventing the receiver from being overwhelmed with data it cannot process.
4. Error control: The Transport layer uses error detection and correction techniques to ensure that data is transmitted accurately and completely.
5. Multiplexing and demultiplexing: The Transport layer can handle multiple connections from different applications on the same host and multiplexes the data from different applications into a single stream for transmission. At the receiving end, it demultiplexes the incoming data stream and delivers it to the appropriate application.
6. Quality of Service (QoS) management: The Transport layer can provide different levels of service for different types of traffic based on priority or other criteria.

The Transport layer protocols in the TCP/IP protocol suite are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP provides reliable, connection-oriented communication, while UDP provides unreliable, connectionless communication with low overhead.

Q63. Discuss Services Provided to the Upper Layers.

- The ultimate goal of the transport layer is to provide efficient, reliable, and cost-effective data transmission service to its users, normally processes in the application layer. To achieve this, the transport layer makes use of the services provided by the network layer. The software and/or hardware within the transport layer that does the work is called the transport entity. The transport entity can be located in the operating system kernel, in a library package bound into network applications, in a separate user process, or even on the network interface card. The first two options are most common on the Internet. The (logical) relationship of the network, transport, and application layers is illustrated in Fig. 6-1.

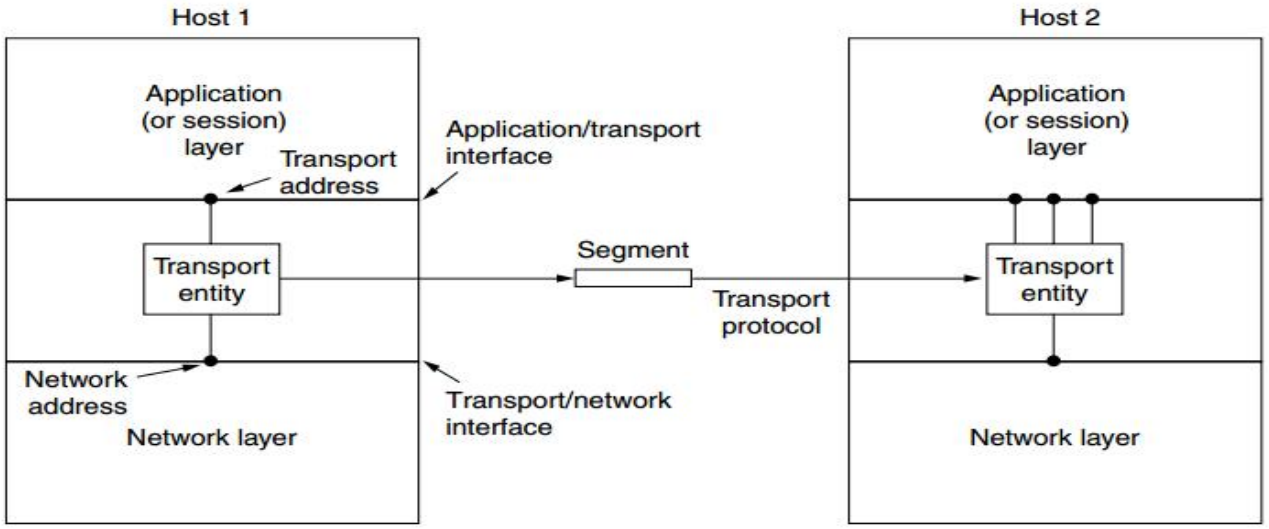


Figure 6-1. The network, transport, and application layers.

Overall, the services provided by the lower layers to the upper layers are essential for the efficient and reliable operation of network applications, ensuring that data is transmitted accurately, efficiently, and securely between applications running on different hosts.

Q64. Discuss Transport Service primitives. **

- Transport Service Primitives are the basic operations or functions provided by the Transport layer to the upper and lower layers of the OSI model or TCP/IP protocol stack. These primitives define the interface between the Transport layer and the layers above and below it, allowing data to be reliably and efficiently transmitted between applications running on different hosts. The most commonly used Transport Service Primitives are:

To get an idea of what a transport service might be like, consider the five primitives listed in table Fig.6-2.

Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	Request a release of the connection

Figure 6-2. The primitives for a simple transport service.

1. Listen: The Listen primitive is used by the Transport layer to wait for incoming connection requests from remote hosts. This primitive is used by the application layer to indicate that it is willing to accept incoming connections.
2. Connect: The Connect primitive is used to establish a connection between two hosts. This primitive is used by the application layer to initiate a connection request.
3. Send: The Send primitive is used by the Transport layer to send data from the local host to the remote host. This primitive is used by the application layer to send data across the network.
4. Receive: The Receive primitive is used by the Transport layer to receive data from the remote host. This primitive is used by the application layer to receive data from the network.
5. Disconnect: The Disconnect primitive is used by the Transport layer to terminate an existing connection between two hosts. This primitive is used by the application layer to indicate that it no longer needs to communicate with the remote host.

Overall, the Transport Service Primitives provide a standardized set of operations for applications to use when communicating across a network. These primitives ensure that data is transmitted accurately, efficiently, and securely between applications running on different hosts.

Q65. What is Addressing? **

- Addressing is the process of identifying a specific network or host on a computer network. In computer networking, every device on the network is assigned an address that is used to route data to and from that device. Addresses are a critical part of network communication because they allow devices to find and communicate with each other, even if they are on different networks or located in different parts of the world.

In the context of the Internet Protocol (IP), addressing refers to the unique numerical identifier assigned to each device on a network, known as the IP address. An IP address is a 32-bit binary number that is represented in dotted decimal notation, where each of the four octets of the IP address is separated by a dot. For example, 192.168.1.1 is an IP address that might be assigned to a device on a local area network.

Q66. What is Error Control and Flow Control? **

- Error control and flow control are two important functions of the data link layer in computer networking.

Error control is the process of detecting and correcting errors that occur during data transmission. When data is sent over a network, it may become corrupted or lost due to noise or interference. Error control mechanisms such as checksums, cyclic redundancy checks (CRC), and error correction codes (ECC) are used to detect and correct errors in the data. If an error is detected, the data is retransmitted until it is successfully received without errors.

Flow control, on the other hand, is the process of managing the rate of data transmission between two devices in a network to prevent data loss or congestion. When data is sent from one device to another, the receiving device may not be able to process the data as quickly as it is received, leading to a buildup of data in the receiver's buffer. Flow control mechanisms such as windowing and buffering are used to manage the flow of data and prevent data loss or congestion.

Overall, error control and flow control are critical functions of the data link layer in computer networking. By detecting and correcting errors and managing the flow of data between devices, these mechanisms help ensure reliable and efficient data transmission over a network.

Or

1. A frame carries an error-detecting code (e.g., a CRC or checksum) that is used to check if the information was correctly received.

2. A frame carries a sequence number to identify itself and is retransmitted by the sender until it receives an acknowledgement of successful receipt from the receiver. This is called ARQ (Automatic Repeat request).

3. There is a maximum number of frames that the sender will allow to be outstanding at any time, pausing if the receiver is not acknowledging frames quickly enough. If this maximum is one packet the protocol is called stop-and-wait. Larger windows enable pipelining and improve performance on long, fast links.

4. The sliding window protocol combines these features and is also used to support bidirectional data transfer.

Q67. Describe UDP. **

UDP stands for User Datagram Protocol, which is a transport layer protocol used for sending and receiving datagrams over an IP network. UDP is a connectionless protocol, which means that there is no handshaking process or session setup between the sender and receiver before data is sent. Instead, the sender simply sends the data in the form of a datagram, which is a basic unit of communication in a network.

The UDP header is a 8-byte header that is added to each UDP datagram. The UDP header is a simple, fixed-length header that provides minimal information about the UDP datagram. Because UDP is a connectionless protocol, there is no need for a complex header with sequence numbers, acknowledgements, or other information that is required by connection-oriented protocols such as TCP. Instead, UDP provides a lightweight, low-overhead mechanism for transmitting data over a network with minimal processing and resource requirements.

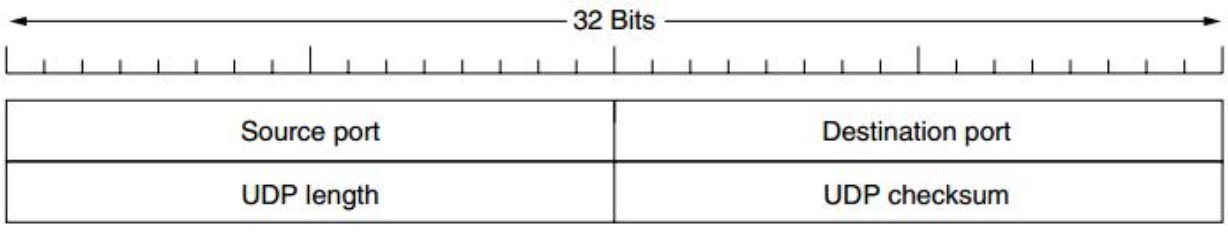


Figure 6-27. The UDP header.

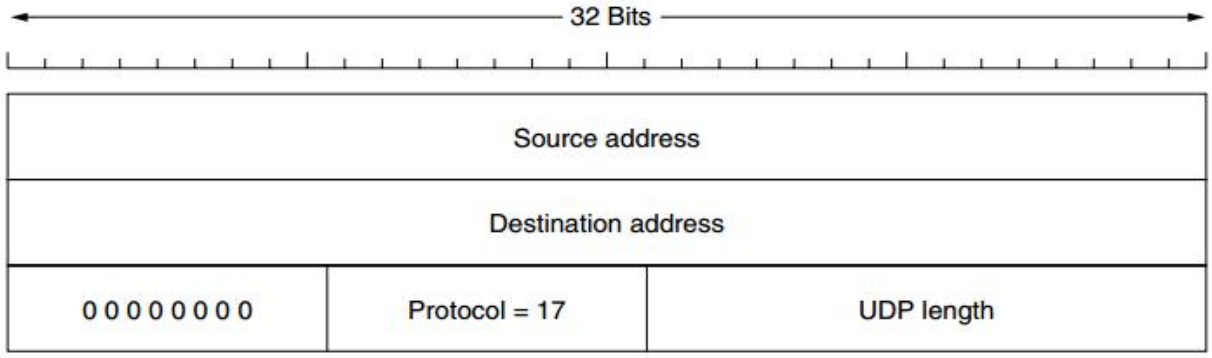


Figure 6-28. The IPv4 pseudoheader included in the UDP checksum.

The source port is primarily needed when a reply must be sent back to the source. By copying the Source port field from the incoming segment into the Destination port field of the outgoing segment, the process sending the reply can specify which process on the sending machine is to get it.

The UDP length field includes the 8-byte header and the data. The minimum length is 8 bytes, to cover the header. The maximum length is 65,515 bytes, which is lower than the largest number that will fit in 16 bits because of the size limit on IP packets.

Q68. What is TCP protocol? ***

- TCP stands for Transmission Control Protocol a communications standard that enables application programs and computing devices to exchange messages over a network. TCP organizes data so that it can be transmitted between a server and a client. It guarantees the integrity of the data being communicated over a network. It then breaks large amounts of data into smaller packets, while ensuring data integrity is in place throughout the process. Example: FTP, HTTP.

Q69. What is TCP, RTP & RTCP Protocol? **

- TCP (Transmission Control Protocol), RTP (Real-time Transport Protocol), and RTCP (Real-time Transport Control Protocol) are all networking protocols used for different purposes.

TCP is a connection-oriented protocol that provides reliable, ordered, and error-checked delivery of data between applications running on hosts communicating over IP networks. It establishes a virtual connection between the source and destination and ensures the data is delivered without errors or loss. TCP is used for applications that require reliable data transfer, such as web browsing, email, and file transfers.

RTP is a protocol used for real-time transmission of multimedia data, such as audio and video, over IP networks. It is designed to work with various multimedia applications and provides end-to-end network transport functions suitable for applications transmitting real-time data. RTP includes features such as packet sequence numbering, time stamping, and payload identification, which help to ensure that the data is delivered in a timely and reliable manner.

RTCP is a protocol that works in conjunction with RTP to provide feedback on the quality of service being provided by RTP. It is used to monitor the transmission statistics and quality of a network connection and provide feedback to both the sender and receiver. RTCP provides information such as packet loss, delay, and jitter, which can be used to adjust the transmission rate or quality of the data.

Overall, TCP, RTP, and RTCP are all important protocols used for different purposes in networking. TCP is used for reliable data transfer, while RTP and RTCP are used for real-time multimedia transmission and monitoring.

Q70. Describe and draw TCP header. **

- Figure 6-36 shows the layout of a TCP segment. Every segment begins with a fixed-format, 20-byte header. The fixed header may be followed by header options. After the options, if any, up to 65,535−20−20=65,495 data bytes may follow, where the first 20 refer to the IP header and the second to the TCP header. Segments without any data are legal and are commonly used for acknowledgements and control messages.

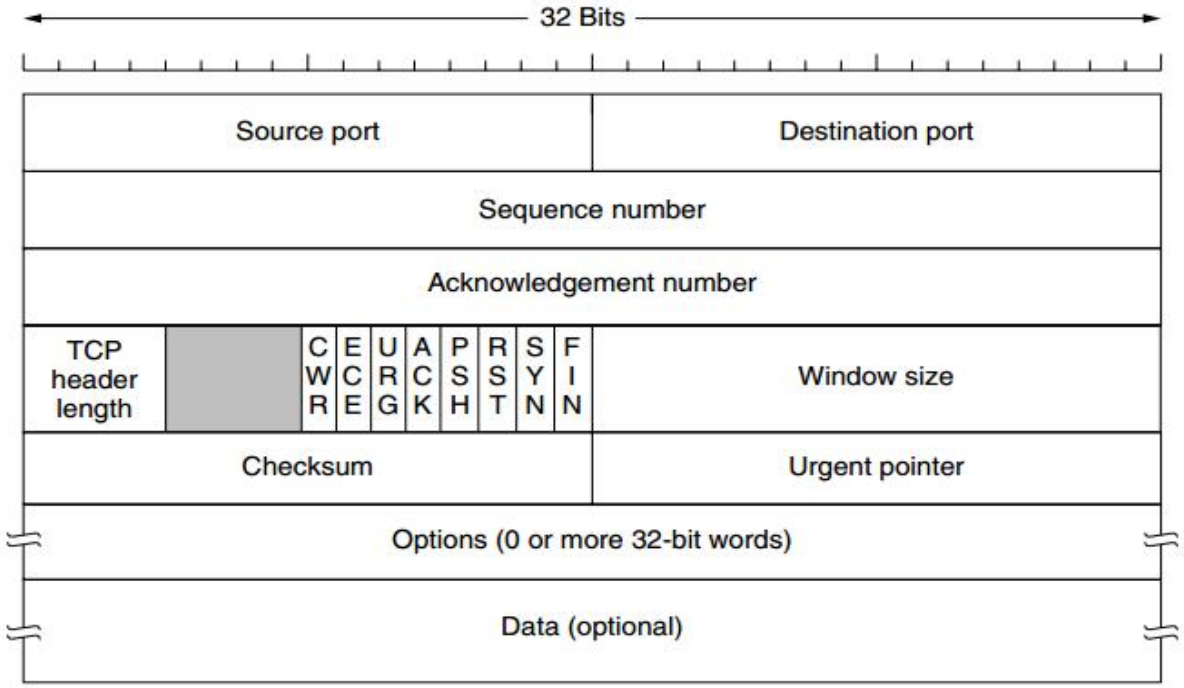


Figure 6-36. The TCP header.

The TCP (Transmission Control Protocol) header is a 20-byte fixed-length header that contains control information for the TCP segment. The following fields are included in the TCP header:

1. Source Port (8 bit) – The source port number identifies the sending port of the application program.
2. Destination Port (8 bit) – The destination port number identifies the receiving port of the application program.
3. Sequence Number (32 bit) – The sequence number identifies the first byte of data in the current TCP segment.
4. Acknowledgment Number (32 bit) – The acknowledgment number identifies the next expected byte of data from the receiving end.
5. Header Length (4 bits) – This field specifies the length of the TCP header in 32-bit words.
6. Reserved (3 bits) – These bits are reserved for future use and are currently set to 0.
7. Control Flags (9 bits) – These bits are used to control the operation of the TCP connection. They include flags such as SYN (synchronize), ACK (acknowledge), FIN (finish), RST (reset), and more.
8. Window Size (32 bit) – This field specifies the number of bytes the sender is willing to receive.
9. Checksum (32 bit) – This field contains a checksum value used for error detection.
10. Urgent Pointer (32 bit) – This field is used to indicate the end of urgent data in the TCP segment.
11. Options (variable) – This field contains optional parameters and flags used to extend or modify the TCP header.

Chapter#7 The Application Layer

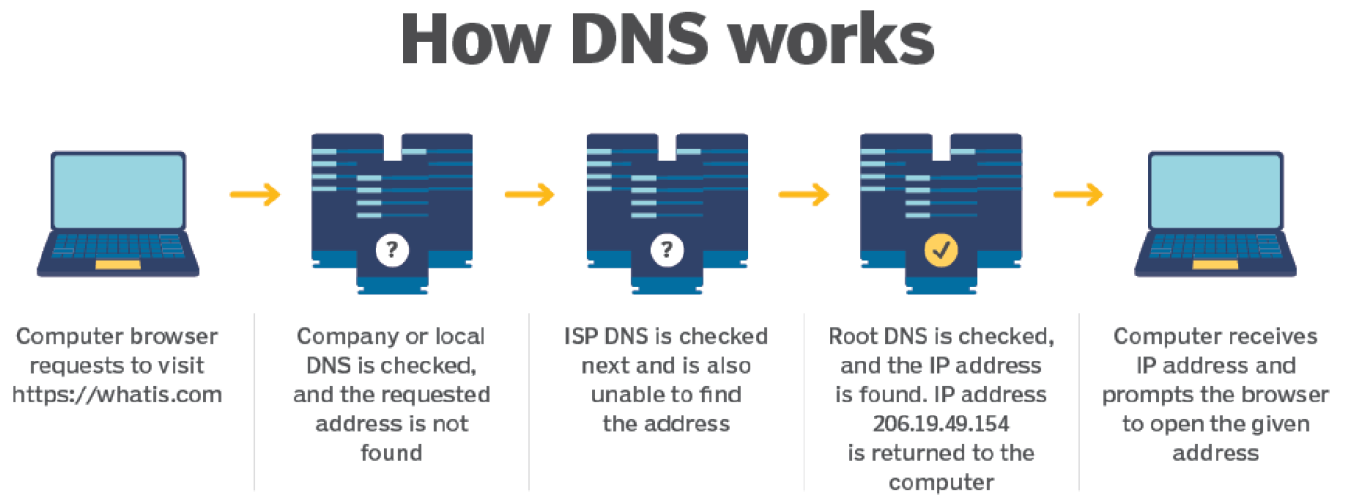
Q71. What is DNS? How DNS works?

Q71. What is DNS? Describe briefly how DNS works? ***

- DNS stands for Domain Name System. It is a distributed naming system used to translate domain names (like www.example.com) into IP addresses (like 192.0.2.1) that computers can understand. DNS provides a way to map human-readable names to machine-readable IP addresses.

When you enter a URL into your web browser, the browser first sends a request to a DNS resolver to look up the IP address associated with that domain name. The DNS resolver then sends a series of requests to DNS servers to try to find the correct IP address.

The DNS system is hierarchical, with a root domain at the top of the hierarchy, followed by a series of top-level domains (TLDs) such as .com, .org, .net, and country code TLDs like .uk, .ca, etc. Each domain can have multiple subdomains, and each subdomain can have multiple records, including A records (which map hostnames to IP addresses), MX records (which specify mail servers for a domain), and others.



Once the DNS resolver has found the correct IP address, it returns that information to the web browser, which then uses the IP address to make a connection to the server hosting the website.

DNS uses a variety of protocols, including the User Datagram Protocol (UDP) and the Transmission Control Protocol (TCP), depending on the specific requirements of the query being made. DNS servers can also use caching to improve performance and reduce the number of requests that need to be made to other DNS servers

Q72. A portion of the Internet domain name space.

- For the Internet, the top of the naming hierarchy is managed by an organization called ICANN (Internet Corporation for Assigned Names and Numbers). ICANN was created for this purpose in 1998, as part of the maturing of the Internet to a worldwide, economic concern. Conceptually, the Internet is divided into over 250top-level domains, where each domain covers many hosts. Each domain is partitioned into subdomains, and these are further partitioned, and so on. All these domains can be represented by a tree, as shown in Fig. 7-1. The leaves of the tree represent domains that have no subdomains (but do contain machines, of course). A leaf domain may contain a single host, or it may represent a company and contain thousands of hosts.

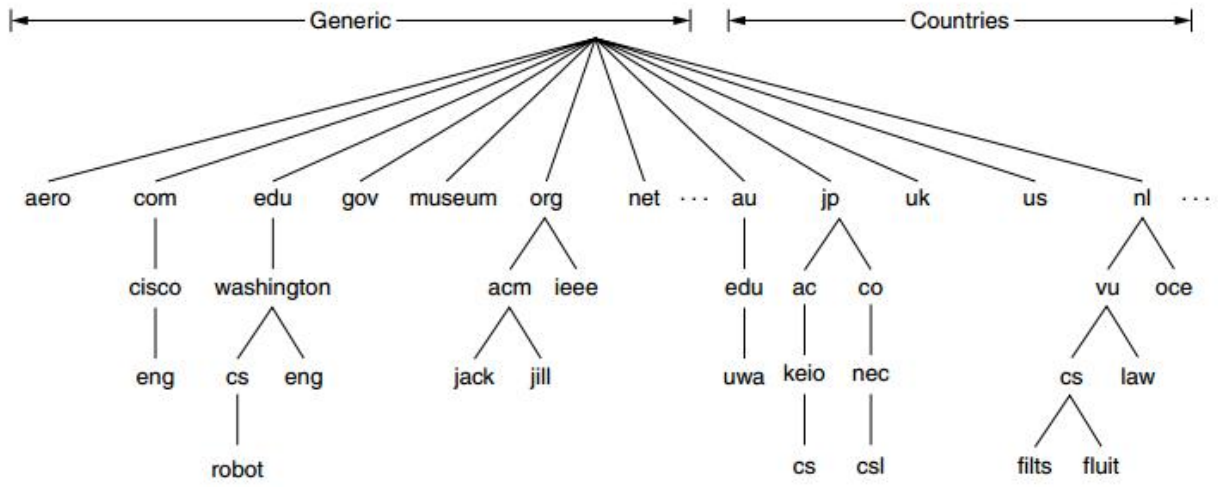


Figure 7-1. A portion of the Internet domain name space.

Q73. List in Generic top-level domains.

- The top-level domains come in two flavors: generic and countries. The generic domains, listed in Fig. 7-2, include original domains from the 1980s and domains introduced via applications to ICANN. Other generic top-level domains will be added in the future.

Domain	Intended use	Start date	Restricted?
com	Commercial	1985	No
edu	Educational institutions	1985	Yes
gov	Government	1985	Yes
int	International organizations	1988	Yes
mil	Military	1985	Yes
net	Network providers	1985	No
org	Non-profit organizations	1985	No
aero	Air transport	2001	Yes
biz	Businesses	2001	No
coop	Cooperatives	2001	Yes
info	Informational	2002	No
museum	Museums	2002	Yes
name	People	2002	No
pro	Professionals	2002	Yes
cat	Catalan	2005	Yes
jobs	Employment	2005	Yes
mobi	Mobile devices	2005	Yes
tel	Contact details	2005	Yes
travel	Travel industry	2005	Yes
xxx	Sex industry	2010	No

Figure 7-2. Generic top-level domains.

Q74. Mention DNS Resource record.

There are many kinds of DNS records. The important types DNS Resource Records are listed in Fig. 7-3.

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text

Figure 7-3. The principal DNS resource record types.

Q75. What is name server? Explain with example how a resolver look-up a remote name in DNS name space. ***

- A name server, also known as a DNS server, is a server that is responsible for translating domain names into IP addresses. When a client makes a DNS query, the query is sent to a name server, which then looks up the IP address associated with the domain name and returns it to the client.

Here is an example of how a resolver looks up a remote name in the DNS name space:

1. The client sends a DNS query to its local resolver, asking for the IP address associated with a particular domain name, such as www.example.com.
2. The local resolver checks its cache to see if it already has the IP address for that domain name. If it does, it returns the IP address to the client.
3. If the local resolver does not have the IP address in its cache, it sends a query to a root name server, asking for the IP address of the TLD (top-level domain) server for the .com domain.
4. The root name server responds with the IP address of the .com TLD server.

5. The local resolver sends a query to the .com TLD server, asking for the IP address of the authoritative name server for the example.com domain.
6. The .com TLD server responds with the IP address of the authoritative name server for the example.com domain.
7. The local resolver sends a query to the authoritative name server for the example.com domain, asking for the IP address of www.example.com.
8. The authoritative name server responds with the IP address of www.example.com.
9. The local resolver caches the IP address and returns it to the client.
10. The client uses the IP address to connect to the web server hosting the website at www.example.com.

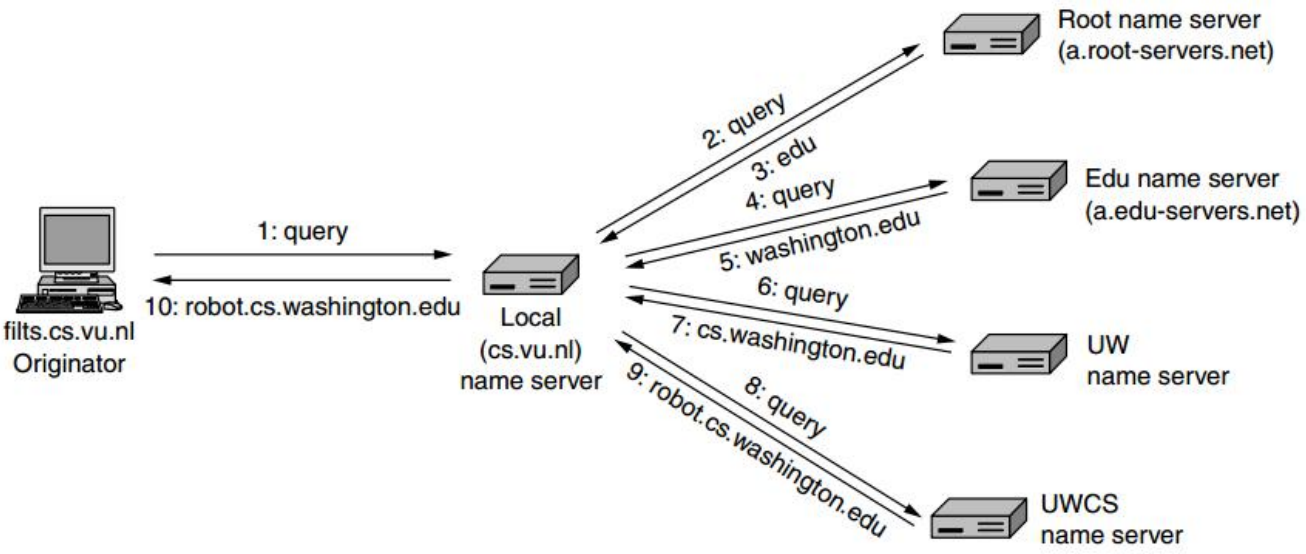


Figure 7-6. Example of a resolver looking up a remote name in 10 steps.

In this way, the DNS system allows users to access websites using human-readable domain names, while the underlying network infrastructure uses IP addresses to route traffic between servers and clients.

Q76. What is E-mail? What is SMTP? **

- Email (short for electronic mail) is a method of exchanging messages between people using electronic devices connected to the internet or other networks. It is a widely used form of communication that allows individuals and businesses to send and receive messages, files, and other data across different locations and time zones.

SMTP (Simple Mail Transfer Protocol) is a protocol used for sending and receiving email messages over the internet. It is responsible for transferring emails from a sender's email client to a recipient's email server, and then to the recipient's email client. SMTP is a text-based protocol that uses a set of commands and responses to communicate between email servers and clients.

Q77. Draw the Email system showing the SMTP protocol environment? ***

- I can describe the components of an email system and how SMTP fits into it.

An email system typically consists of:

1. User agent: This is the email client used by the sender to compose, send, and receive emails. Examples include Gmail, Outlook, and Apple Mail.
2. Mail server: This is a computer that handles the storage, transmission, and delivery of email messages. It consists of two components: the Mail Transfer Agent (MTA) and the Mail Delivery Agent (MDA).
3. Domain Name System (DNS) server: This server resolves domain names to IP addresses. It helps in identifying the email servers that are responsible for handling emails for a particular domain.
4. SMTP protocol: This is the protocol used for sending and receiving emails between email servers. When a user sends an email, the email client communicates with the SMTP server to send the email message to the recipient's email server.

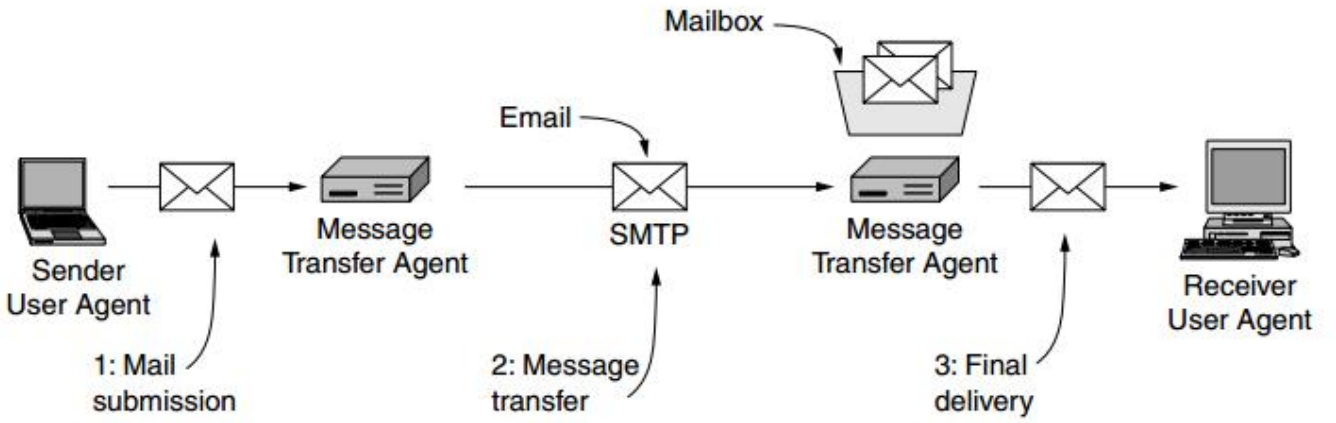


Figure 7-7. Architecture of the email system.

In the SMTP environment, the email client sends the email message to the SMTP server using the SMTP protocol. The SMTP server then communicates with the recipient's email server using the SMTP protocol to transfer the email message. Once the email message is delivered to the recipient's email server, it is stored in the mailbox until the recipient accesses it using their email client.

Q78. Differentiate between Paper Mail and E-mail. ***

- Paper mail and e-mail are two modes of communication, but they differ in various aspects, as listed below:

Paper Mail	E-mail
Physical delivery	Electronic delivery
Delivery time is longer	Delivery time is almost instantaneous
Delivery can be delayed or lost in transit	Delivery is reliable
Sender needs physical access to a mailbox	Sender needs internet access
Can be more expensive for long distance or international delivery	Generally cheaper, regardless of distance
Limited to text, images, and physical objects	Supports various file formats, including text, images, audio, and video
Requires postage fees	Free for most services
Difficult to track delivery status	Delivery status can be easily tracked
Not easily searchable or filterable	Messages can be easily searched and filtered
Limited storage space	Large storage space
Environmental impact due to paper and transportation	More eco-friendly due to electronic delivery
Requires physical storage space for paper documents	Electronic documents can be stored on various devices and cloud storage platforms

In summary, while paper mail and e-mail share some similarities as modes of communication, they differ in terms of speed, cost, physicality, security, storage, retrieval, and environmental impact.

Q79. Define IMAP & What is WWW? **

- IMAP stands for Internet Message Access Protocol. It is a protocol used by email clients to retrieve email messages from a mail server. Unlike POP3, which downloads messages to the client and typically deletes them from the server, IMAP allows messages to remain on the server, allowing users to access their email from multiple devices and locations.

WWW stands for World Wide Web. It is a system of interconnected documents and resources, accessed through the internet, that are identified by Uniform Resource Locators (URLs) and can be displayed in web browsers. The WWW is a part of the broader internet and allows users to access a wide range of information, media, and services. It is the foundation of the modern internet and has transformed the way people access and share information.

Q80. Define SMTP & IMAP. **

- SMTP (Simple Mail Transfer Protocol) is an Internet standard protocol used for the transmission of email messages from one server to another over the internet. SMTP is responsible for sending messages from the sender's mail client to the recipient's mail server.

IMAP (Internet Message Access Protocol) is a standard protocol used by email clients to retrieve and manage email messages from a mail server. Unlike POP3, which downloads and deletes messages from the server, IMAP allows users to access and manage their email messages on the server in real-time. IMAP is widely used by modern email clients for accessing email messages.

Q81. Explain the architectural framework of www with diagram. ***

- The World Wide Web (WWW) is a collection of interconnected documents and other resources that can be accessed through the internet. It is built on top of the internet infrastructure and provides a way for users to access information from anywhere in the world. The architectural framework of the WWW includes the following components:

1. Web Browsers: A web browser is a software application used to access and view web pages. Popular web browsers include Google Chrome, Mozilla Firefox, and Microsoft Edge.
2. Web Servers: A web server is a computer program that responds to requests from web browsers and serves web pages to clients. Examples of popular web servers include Apache and Microsoft IIS.
3. Hypertext Transfer Protocol (HTTP): HTTP is the protocol used to transfer data over the web. It defines how web browsers and web servers communicate with each other.
4. Uniform Resource Locators (URLs): URLs are used to identify resources on the web, such as web pages, images, and videos. They consist of several parts, including the protocol (http or https), the domain name, and the path to the resource.
5. HyperText Markup Language (HTML): HTML is the markup language used to create web pages. It defines the structure and content of a web page, including text, images, and links.
6. Cascading Style Sheets (CSS): CSS is a style sheet language used to define the visual presentation of a web page. It allows web developers to separate the content of a web page from its presentation, making it easier to create and maintain complex websites.
7. JavaScript: JavaScript is a scripting language used to add interactivity to web pages. It can be used to create dynamic effects, such as pop-up menus, image galleries, and animations.

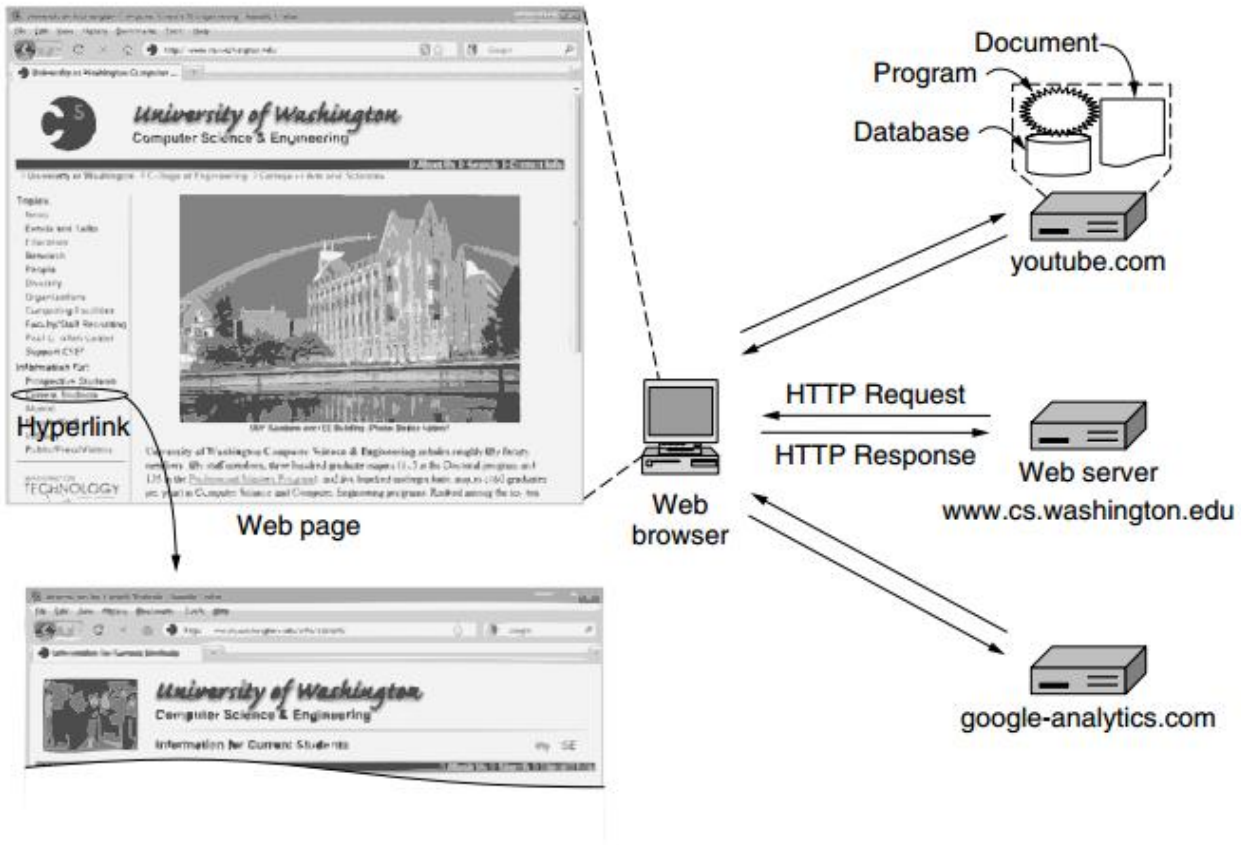


Figure 7-18. Architecture of the Web.

Q82. What is URL? Write the steps that occur when a URL is selected in the browser. ***

- URL stands for Uniform Resource Locator. It is a string of characters that provides the address of a resource on the internet, such as a webpage, an image, or a file.

This URL consists of three parts: the protocol (http), the DNS name of the host (www.cs.washington.edu), and the path name (index.html). When a user clicks on a hyperlink, the browser carries out a series of steps in order to fetch the page pointed to. When a user selects a URL in a browser, the following steps occur:

1. The browser determines the URL (by seeing what was selected).
2. The browser asks DNS for the IP address of the server www.cs.washington.edu.
3. DNS replies with DNS IP 128.208.3.88.
4. The browser makes a TCP connection to IP 128.208.3.88 on port 80, the well-known port for the HTTP protocol.
5. It sends over an HTTP request asking for the page/index.html.
6. The www.cs.washington.eduserver sends the page as an HTTP response, for example, by sending the file/index.html.

7. If the page includes URLs that are needed for display, the browser fetches the other URLs using the same process. In this case, the URLs include multiple embedded images also fetched from www.cs.washington.edu, an embedded video from youtube.com, and a script fromgoogle-analytics.com.
8. The browser displays the page/index.html as it appears in the graphical view
9. The TCP connections are released if there are no other requests to the same servers for a short period.

Q83. What is URL? Show some common URL Schemes.

URL stands for Uniform Resource Locator. It is a string of characters that provides the address of a resource on the internet, such as a webpage, an image, or a file.

The URL design is open-ended in the sense that it is straightforward to have browsers use multiple protocols to get at different kinds of resources. In fact, URLs for various other protocols have been defined. Slightly simplified forms of the common ones are listed in Fig. 7-19.

Name	Used for	Example
http	Hypertext (HTML)	http://www.ee.uwa.edu/~rob/
https	Hypertext with security	https://www.bank.com/accounts/
ftp	FTP	ftp://ftp.cs.vu.nl/pub/minix/README
file	Local file	file:///usr/suzanne/prog.c
mailto	Sending email	mailto:JohnUser@acm.org
rtsp	Streaming media	rtsp://youtube.com/montypython.mpg
sip	Multimedia calls	sip:eve@adversary.com
about	Browser information	about:plugins

Figure 7-19. Some common URL schemes.