Merits of computer Network :

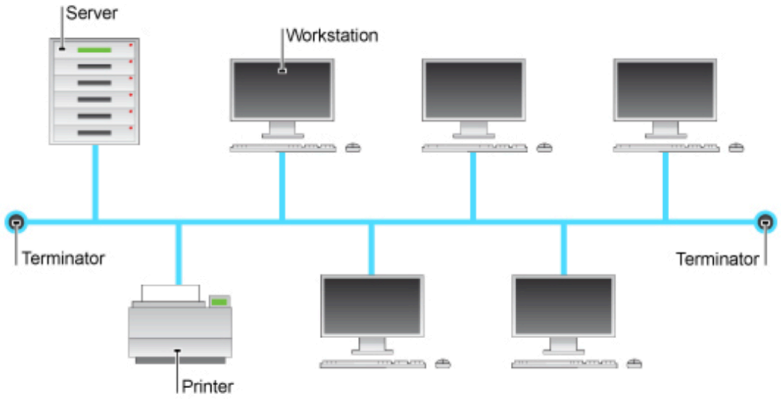
1. Resource Sharing
2. Data sharing and communication.
3. Remote access
4. Centralized Data Management
5. Cost Efficiency
6. Collaboration.
7. Quick and Easy Updates.
8. Easier Maintenance and Troubleshooting.

Demerits:

1. Increased costs.
2. Security Issues / Threats
3. Unavailability of information in case of network failure.

STAR TOPOLOGY	BUS TOPOLOGY
A star topology is a network topology in which all devices are connected to a single central hub or switch.	A bus topology is a network topology in which all devices are connected by a single central connection.
In star topology, if the central core fails, the whole system will get affected, and even you cannot use the Computer Network.	In a Bus topology, if the network cable fails, the whole network will also fail.
The performance and the management of high traffic of the network are dependent on the central hub in a star topology.	When there is a lot of traffic on the network with a Bus topology, the network performance suffers. As a result, it is unable to adequately manage a large volume of traffic.
Any terminator is not included in the star topology.	At both ends of the network, the terminators are included in the bus topology.
Because of the need for extra wires and a central hub for connection, the cost of implementation star topology is high.	As compared to a star topology, bus topology is less costly.
In star topology, the rate of data transmission is fast.	The rate of data transmission in a bus topology is slower than in a star topology.

The nodes in a star architecture communicate through the central hub. The message is forwarded to the receiver node after it arrives at the central hub from the sender.	The process of data transmission in star topology is something different. In a bus topology, the sender's message is sent directly to the recipient



Bus Topology

Mesh Topology

A mesh topology is a type of computer network in which each node (computer or other device) is connected to every other node in the network. This type of network is often used in large organisations or companies because it can handle a large amount of data traffic and can be easily expanded.

Advantage : Very Fault Tolerant.
Disadvantage : Costly (as each are connected to each other), Complex to configure and Manage.

Ring Topology

In computer networking, topology is the arrangement of devices and their connections. Ring topology is a type of network configuration in which each device on the network is connected to two other devices, forming a “ring.” Data travels around the ring in one direction only, from device to device, until it reaches its destination.

Often used in Local Area Network (LANs.)

If one node fails, the network can reroute signals around the failed node using the other nodes as alternate paths. This redundancy can improve reliability and fault tolerance, but it also adds complexity to the network.

Advantage : easy to expand.
Disadvantage: Not suited for large networks.

MAN (Metropolitan Area Network)

A Metropolitan Area Network (MAN) is a type of computer network that covers a larger geographic area than a Local Area Network (LAN) but is smaller in scope compared to a Wide Area Network (WAN). A MAN typically spans a city or a large campus, providing high-speed connectivity to connect multiple LANs within a specific geographic region. MANs are designed to offer efficient data transfer rates over a relatively larger area while maintaining lower latencies compared to WANs.

Active Network Model

The Active Network model, also known as Active Networking, refers to a networking concept where network nodes (such as routers, switches, and other devices) are empowered to execute customized or user-defined programs, scripts, or code directly on the network devices. This enables network devices to perform computations, make decisions, and modify how data packets are processed as they traverse the network.

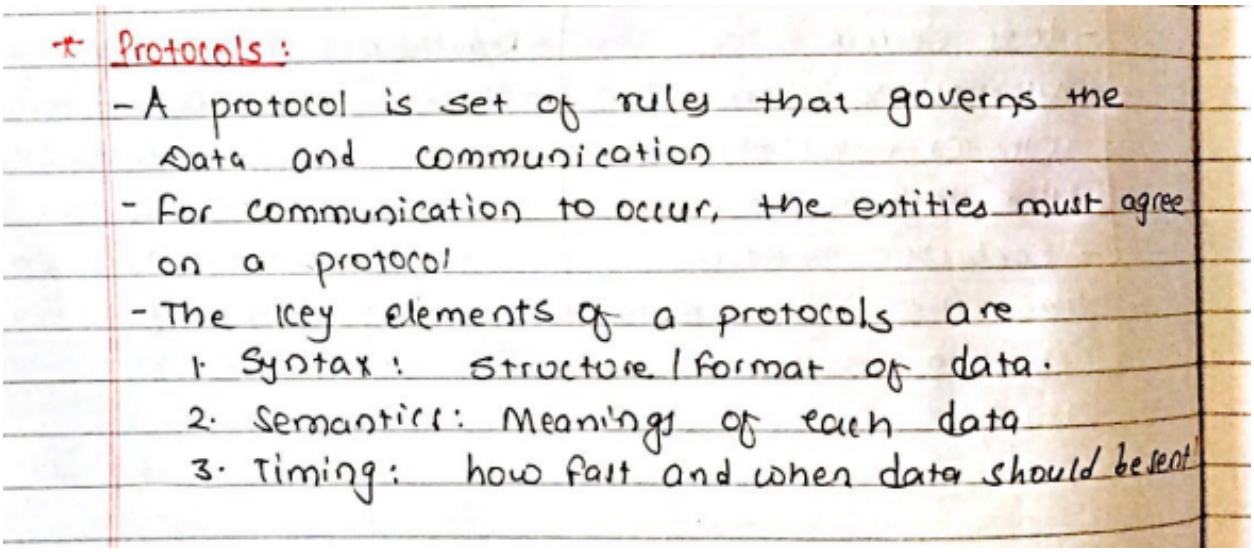
In the Active Network model, the traditional notion of a passive network, where devices simply forward packets based on predefined rules, is expanded to allow network elements to become more intelligent and programmable. This programmability enables the creation of networks that can dynamically adapt to changing conditions, optimize resource utilization, and even perform application-specific functions within the network itself.

Key Features : Node programmability , Customized Behavior, Dynamic Adaptation, Network Optimizations ,Security Enhancements.

Challenges: Security Risks, Complexity, Standardization.

Chapter-2 : Reference Model

Protocols


* Protocols :
- A protocol is set of rules that governs the data and communication
- For communication to occur, the entities must agree on a protocol
- The key elements of a protocols are
  1. Syntax : structure / format of data.
  2. Semantics : Meanings of each data
  3. Timing : how fast and when data should be sent

Interfaces:

In computer networking, an interface refers to a point of interaction between different components, systems, or devices. Interfaces define how these components communicate with each other and exchange data. Interfaces can be physical or logical, and they play a crucial role in establishing connectivity and enabling interactions in a networked environment. Here are a few types of interfaces:

Physical Interfaces: These are hardware connections used to physically connect devices. Examples include Ethernet ports, USB ports, and serial ports.

Network Interfaces: Also known as network adapters or network cards, these are hardware components that allow a device to connect to a network. They are responsible for sending and receiving data packets over the network.

User Interfaces (UI): In a broader sense, a user interface is the point of interaction between a user and a computer system or application. This could include graphical user interfaces (GUIs) or command-line interfaces (CLIs).

API Interfaces: Application Programming Interfaces (APIs) define how software components interact with each other. They provide a set of functions, methods, and protocols that developers can use to integrate different software systems.

Services:

In networking, a service refers to a specific function or capability that a network or networked device provides to its users or other systems. These services can be software-based or hardware-based and are designed to fulfill specific needs within a network environment. Here are a few examples of network services:

Web Services: Services that provide access to resources and functions over the internet using standardized protocols like HTTP. Examples include websites, online applications, and APIs.

File Sharing Services: Services that allow users to share files and documents across a network. Examples include FTP (File Transfer Protocol) and cloud storage services.

Email Services: Services that facilitate the sending, receiving, and storage of electronic mail. Examples include SMTP (Simple Mail Transfer Protocol) and IMAP (Internet Message Access Protocol).

DNS (Domain Name System): A service that translates human-readable domain names into IP addresses, allowing users to access websites using domain names.

DHCP (Dynamic Host Configuration Protocol): A service that automatically assigns IP addresses and other network configuration settings to devices in a network.

Firewall Services: Services that provide network security by monitoring and controlling incoming and outgoing network traffic.

VoIP (Voice over IP) Services: Services that enable voice communication over the internet or a network using IP-based protocols.

Remote Access Services: Services that allow users to access a network or system from a remote location. Examples include VPN (Virtual Private Network) services.

In essence, interfaces define how components interact, and services provide specific functions within a networked environment. Together, interfaces and services form the building blocks of modern computer networks and enable the seamless communication and functionality we experience in our connected world.

Protocol Stack

A protocol stack, also known as a networking stack or communication stack, is a layered architecture used in computer networking and telecommunications to facilitate communication between different devices or systems. Each layer in the stack performs specific functions, and communication between layers is governed by predefined protocols. The concept of a protocol stack is fundamental to how data is transmitted and received across networks.

The protocol stack is typically organized into layers, with each layer handling a specific aspect of communication. The most commonly referenced model for protocol stacks is the OSI (Open Systems Interconnection) model, which consists of seven layers. Another well-known model is the TCP/IP model, which has four layers. Each layer builds upon the services provided by the lower layers, abstracting and simplifying the communication process.

Reason for using Layered Protocol :

- Modularity and Abstraction.
- Interoperability.
- Flexibility and Evolution.
- Standardization.

OSI Layers

Session Layer:

- Maintains sessions of user; (token management, dialup control)
- Synchronization.
- Protocol : NetBIOS

Presentation Layer:

- Data Formats , Data Compression, Encryption.
- Protocol : SSL/TLS

Application Layer :

- Provides various services
- Protocols used : HTTP, HTTPS, SMTP, POP, DNS, FTP etc.

Network Interface Card (NIC)

A NIC (Network Interface Card), also known as a network adapter or network card, is a hardware component that allows a computer or device to connect to a computer network and communicate with other devices. It serves as the bridge between the computer's internal processing and the data transmission and reception on the network.

It handles the conversion of digital data from the computer's internal processing into the appropriate signals for transmission over the network medium (such as Ethernet cables or wireless signals).

NICs supports various networks such as for wired (Ethernet, RJ-45 Connectors) or Wireless networks.

Parameters	OSI Model	TCP/IP Model
Full Form	OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
Layers	It has 7 layers.	It has 4 layers.
Usage	It is low in usage.	It is mostly used.
Approach	It is vertically approached.	It is horizontally approached.
Delivery	Delivery of the package is guaranteed in OSI Model.	Delivery of the package is not guaranteed in TCP/IP Model.
Replacement	Replacement of tools and changes can easily be done in this model.	Replacing the tools is not easy as it is in OSI Model.
Reliability	It is less reliable than TCP/IP Model.	It is more reliable than OSI Model.

It has its own firmware, ethernet controller, memory and soon.

NICs have a unique identifier known as the MAC (Media Access Control) address. This address is typically assigned by the manufacturer and is used to identify the NIC on the network.

Requires Driver to work with Operating System.

In current systems, NIC are integrated on the motherboard itself.

Physical Layer : 1st Layer Device : Repeater, Hub
Data Link Layer: 2nd Layer Device : Bridge, Switch
Network Layer : 3rd Layer Device : Router.

Repeater :

- 1st Layer Device. (i.e. operates on physical Layer)

- Regenerates the signal before its gets weak.
- Regenerates not amplifies.
- Copy the signal bit by bit.
- It is a 2 port device. (one for incoming signal and another one for “boosted” outgoing signal.)
- Has no filtering capacity.

Hub:
- Multiport repeater.
- Connects multiple wires coming from different branches.
- Do not have intelligence to find out the best path.

Bridge:
- Layer 2 device (i.e. operates on data link layer).
- Is a repeater with add on functionality of filtering content by reading the MAC address of source and destination.
- Used to connect two LANs working on same protocol.
- It has 2 port. (I/P port, O/p Port).

Switch
- Layer 2 device (i.e. operators on data link layer).
- Connects multiple network devices within the LANs
- It is a multiport bridge with a buffer and a design that can boost its efficiency (large no. of ports=> less traffic).
- Perform error checking before forwarding data, that makes it more efficient as it does not forward packets that has errors.
- Switches filter and manage broadcast and multicast traffic. Broadcasts are sent to all devices on the network, while multicast traffic is sent to specific groups of devices.
- Unlike hubs, which create a single collision domain, switches create individual collision domains for each connected device. This reduces collisions and improves network efficiency.
- Switches can be cascaded or stacked to accommodate more devices as a network grows, providing scalability to meet increasing demands.

Chapter 3 : Physical Layer

Guided Media:

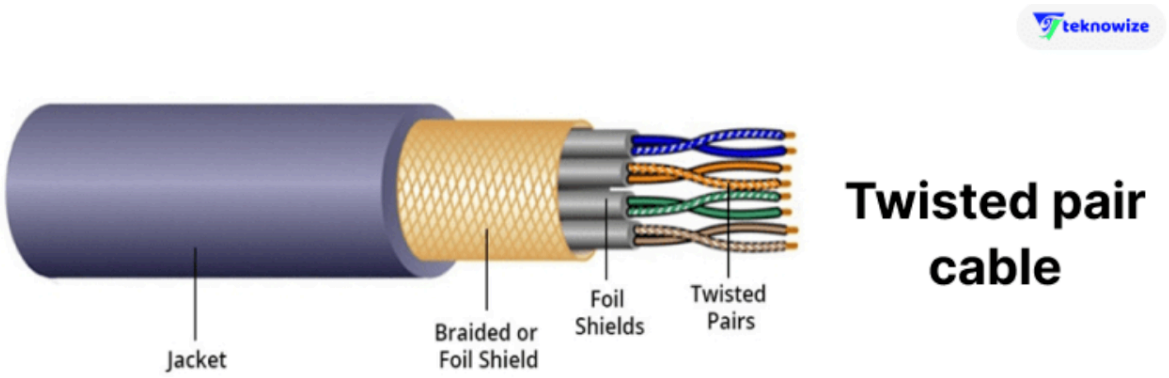
Guided media, also known as wired or bounded media, refer to the physical pathways or channels through which signals are transmitted in a communication network.

Types of Guided Media :

1. Twisted pair Cable:

Twisted pair cable is a type of electrical cable that consists of pairs of insulated copper wires twisted together. It's commonly used for various communication and networking purposes due to its reliability, cost-effectiveness, and ease of installation. Twisted pair cables are used for both data transmission and voice communication.

Unshielded Twisted Pair (UTP): UTP cables do not have any additional shielding to protect against external interference. They are widely used in Ethernet networks and are categorized into different classes based on their performance characteristics (e.g., Cat 6, Cat 6a, Cat 7).
Shielded Twisted Pair (STP): STP cables have additional shielding around the twisted pairs to provide better protection against EMI and crosstalk. They are commonly used in environments with high levels of interference, such as industrial settings.



2. Co-axial Cable :

Coaxial cable, often referred to as coax cable, is a type of electrical cable that consists of a central conductor, an insulating layer, a metallic shield, and an outer insulating layer. Coaxial cables are widely used for various applications, including television, cable internet, telecommunications, and networking.

Advantage : Signal Quality, High bandwidth, Low interference.
Limitations : Bulkiness, Installation complexity.

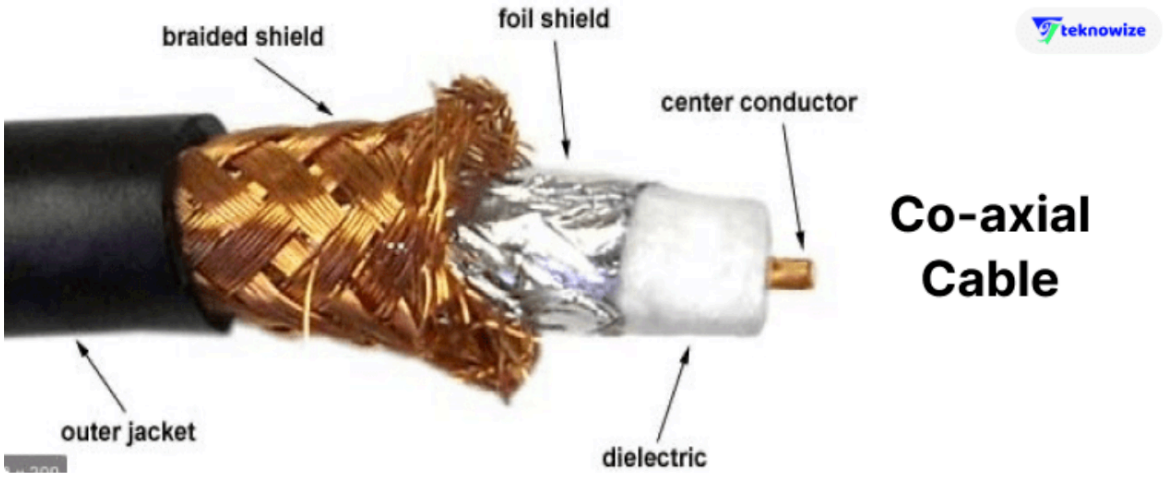
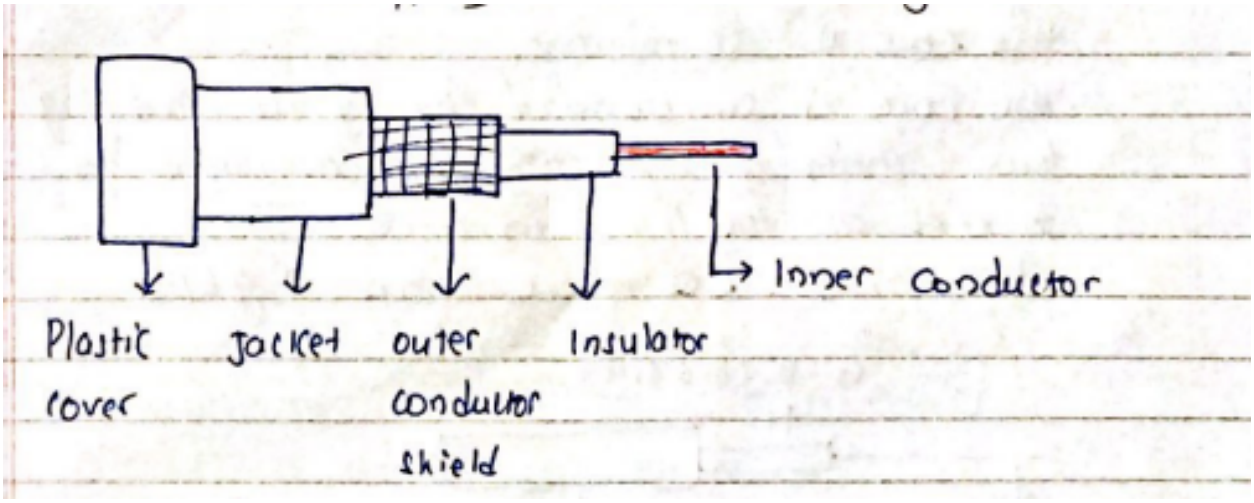


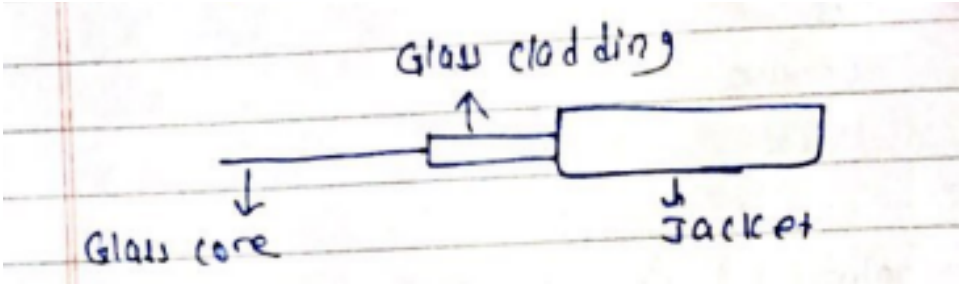
Fig: Co-axial Cable



3. Fiber optic Cable.

Fiber optic cable, commonly known as optical fiber or simply fiber, is a high-performance type of cable used for transmitting data using light signals. It consists of thin strands of glass or plastic fibers that can carry large amounts of data over long distances at high speeds. Fiber optic cables are used in various applications, including telecommunications, internet, networking, and more

Advantages : High bandwidth, Speed, Low signal Loss.
Limitations : installation complexity, Cost



UnGuided Media:

1. Bluetooth
2. Wifi / Wireless LAN

3. Satellites + Its working principle.

A communication satellite is a station in space that receives microwave signals from an earth based stations , amplifies the signals and broadcast signals over a wide area to many earth-based stations.

Applications : tv, radio,weather forecasting, Video conferencing, Global Positioning System (GPS).

A satellite communication system enables long-distance communication by transmitting and receiving signals through satellites orbiting Earth. The system involves transmitting signals from a ground station (uplink) to a satellite and then relaying those signals back to another ground station (downlink).

Satellite Positing :

- Geostationary Earth Orbit (GEO)
- Medium Earth Orbit (MEO)
- Low Earth Orbit (LEO)

A transponder is an electronic device that receives, amplifies, and retransmits signals back to Earth.

The receiving signals are send as electromagnetic wave.

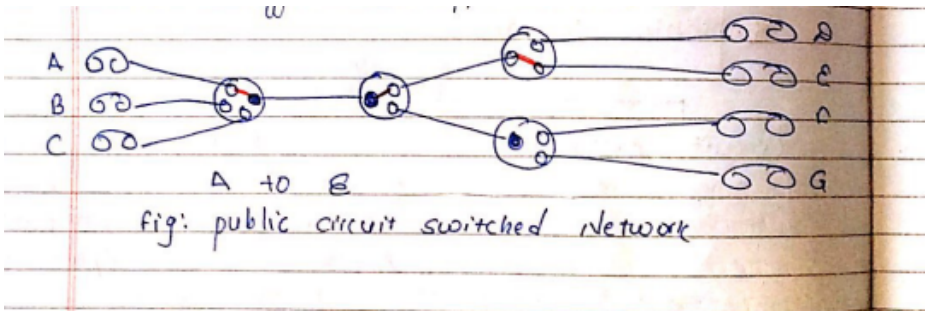
The downlink receives data using dish antenna. Which further process the signal data.

Switching

Switching in the context of computer networks refers to the mechanism used to forward data from a source to a destination within a network. There are three main types of switching: circuit switching, packet switching, and message switching.

Circuit Switching :

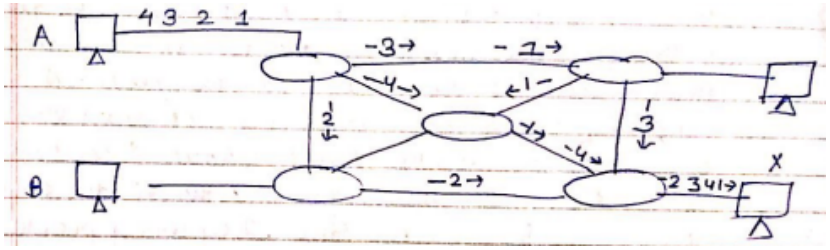
- A complete circuit (dedicated communication path) has to be established between source and destination, before communication.
- Circuit Switching usually uses fixed rate of data transfer.
- The circuit remains reserved for the communication, even if no data is being transmitted, leading to dedicated resources.
- Commonly associated with traditional telephone networks.
- Setup connection takes time. Once the circuit is established, there is low delay and consistent quality. (And transfer is transparent).
- Efficient for continuous, real-time communication (e.g., voice calls).
- Example : Traditional Telephone calls.



Packet Switching :

- Data is divided into smaller packets before transmission.
- Each packet contains user data plus control information.
- Control information contains routing information.
- Packets are individually routed from source to destination on the network using various routing algorithms.
- Packets from multiple sources can share the same network resources, leading to better resource utilization
- Suitable for brusty data transmission (eg: internet browsing, file downloads).
- Robust and adaptable, as the network can find alternative routes if one path is congested or fails.
- Suffers from variable delays and possible packet loss due to network congestion or errors.
- Examples: Internet Protocol (IP) networks (like the internet) use packet switching.

Two types of packet switching : Datagram Approach, Virtual Circuit approach.



Message switching :

- In message switching, messages are treated as a whole and are stored and forwarded in each intermediate node.
- Nodes store and forward messages, allowing for slower links or nodes in the network.
- Each node verifies the message's correctness before forwarding.
- Suitable for environments with high error rates or where real-time communication is not critical.

- Inefficient for large messages or messages requiring quick delivery.
- Delay can be unpredictable due to the storing and forwarding process.
- Examples: Early computer networks like ARPANET used message switching.

In summary:
Circuit Switching is suited for continuous, real-time communication and offers consistent quality, but it's inefficient for data-centric communication.
Packet Switching is widely used in modern networks, accommodating bursty data and dynamic routing, but it can lead to variable delays and possible packet loss.
Message Switching stores and forwards complete messages, making it suitable for less time-sensitive communication, but it can suffer from unpredictable delays and inefficiencies.

Network Performance metrics:

Bandwidth:
Bandwidth refers to the maximum data rate that a network or communication channel can transmit over a given period. It is usually measured in bits per second (bps) and represents the capacity of the channel to carry data.

Throughput:
Throughput is the actual amount of data that can be transmitted over a network or communication channel in a given amount of time. It is a measure of the effective data rate achieved in practice and may be lower than the theoretical bandwidth due to various factors like congestion and network overhead.

Latency:
Latency, also known as delay, is the time it takes for a data packet to travel from the source to the destination in a network. It includes several components such as transmission delay, propagation delay, processing delay, and queuing delay. Lower latency is generally desirable for real-time applications.

Bandwidth-Delay Product:
The bandwidth-delay product is a metric used to measure the amount of data that can be in transit (unacknowledged) in a network at a given time. It is calculated by multiplying the bandwidth of the channel by the round-trip delay time. It represents the maximum amount of data that can be in the network "pipeline" at a given moment.

Jitter:
Jitter refers to the variation in the delay of received data packets. It is the difference in arrival times between packets in a network. Jitter can lead to inconsistent data delivery and is particularly important in real-time applications where a consistent data flow is essential.

In summary:
Bandwidth is the maximum data rate a network can handle.
Throughput is the actual data rate achieved in practice.
Latency is the time it takes for a packet to travel from source to destination.
Bandwidth-Delay Product is the amount of data that can be in transit in the network at a given time.
Jitter is the variation in packet arrival times.

Chapter - 4 : Data Link Layer

Functions of Data Link Layer :
- Framing.
- Physical Addressing (MAC address).
- Error Control (Detection and Correction of Errors).
- Access Control
- Flow Control.

There are two sub-layers of Data-Link Layers
1. Logical Link Control (LLC) : SubLayer:
   - The LLC sub-layer is responsible for link management, flow control, error handling, and addressing within the Data Link Layer.
   - It interacts with the Network Layer above and the MAC sub-layer below to ensure proper communication and reliability.
   - The LLC sub-layer provides services such **as flow control, frame sequencing, acknowledgment, error checking, and addressing.**

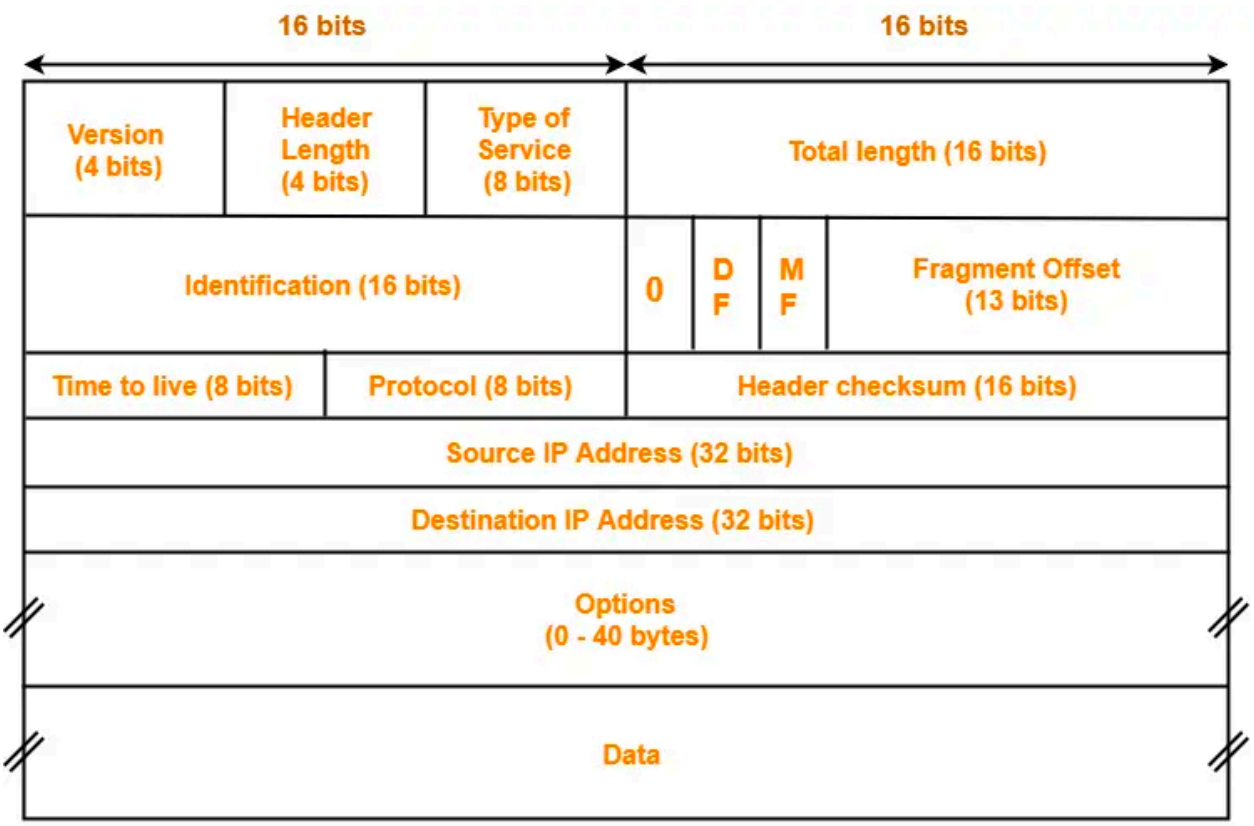
2. Memory Access Control (MAC) SubLayer :
- The MAC sub-layer is responsible for controlling how devices access and use the shared communication medium in a network.
- It manages the physical addressing (MAC addresses) of devices and ensures that data frames are transmitted over the medium without collision.
- Go
- The MAC sub-layer provides services such as **channel access, collision detection, collision avoidance, and frame encapsulation.**

It's important to note that the division of the Data Link Layer into LLC and MAC sub-layers is more relevant to the IEEE 802 networking standards (such as Ethernet and Wi-Fi). Some networking technologies, especially older ones, may not strictly adhere to this sub-layer division.

Framing : https://www.tutorialspoint.com/framing-in-data-link-layer

Chapter -5 : Network/Internet Layer Protocols and Addressing.

IPv4 Header Format



IPv4 Header

DF = Do Not Fragment Bit (either 0 or 1).
MF = More Fragment Big (value either be 0 or 1)

IPv4 Header Format. Description. : https://www.gatevidyalay.com/ipv4-ipv4-header-ipv4-header-format

IPv4 vs IPv6 :

IPv4	IPv6
It is 32bit address	It is 128 bit address
It is divided into 5 classes (Class A to Class E)	It has no division into classes.
It is numeric address consisting of 4 fields (of 8 bit) , each separated by dot.	It is numeric address consisting of 8 fields (of 16 bit), each separated by colon.
Has limited IP	Has several IP address; and created after IPv4
It supports manual and DHCP configuration	It supports manual, DHCP, auto-configuration and renumbering.
IP address is represented in decimal	IP address is represented in hexadecimal.
Does not provide any mechanism for packet flow identification.	Uses flow label field in the header for the packet flow identification.
Cheksum field is available	Checksum field is not aviable.
IPv4 is broadcasting	Ipv6 is multicasting.
Doesn't provide encryption and authentication.	Provides encryption and authentication.

Chapter 6 : Transport Layer and Protocols

TCP vs. UDP

TCP	UDP
Transmission Control Protocol	User Datagram Protocol
Connection Oritented Protcol	Connection Less Protocol
Does not support broadcasting	Supports broadcasting
Stream Type : byte Steam	Steam Type : Message Stream
Gurantees the delivery of packet.	Doesn't guarantee delivery of packages
Protocols : HTTP, HTTPS, SMTP,	Protocols : DNS, DHCP, SNMP,
Header size : 20-60 byte (variable)	Header size: 8 byte fixed
Handshakes signal (SYN, ACK, SYN-ACK)	No Handshakes
Extensive error-checking	Basic error-checking mechanism using checksum

TCP	UDP
Sequencing of data is done	Sequencing is not done, if to be done, it is done by application layer.
Acknowledges are used	No acknowledgements of signals.

DHCP :

Chapter 8 : Application Layers, Servers and Protocols

DHCP :

The Dynamic Host Configuration Protocol (DHCP) is a network protocol used to automatically assign and manage IP addresses, as well as other network configuration parameters, to devices within a network. DHCP simplifies the process of network configuration by automating the assignment of IP addresses, subnet masks, default gateways, DNS server addresses, and other settings. DHCP simplifies network administration by centrally managing and distributing IP address assignments. Here are the key principles of DHCP:

IP Address Allocation: DHCP enables the dynamic allocation of IP addresses to devices on a network. When a device connects to the network, it requests an IP address from a DHCP server.

Lease Duration: DHCP assigns IP addresses for a specific lease duration. After the lease period expires, the device must renew its lease to continue using the same IP address.

DHCP Server: A DHCP server is responsible for maintaining a pool of available IP addresses, leasing them to devices, and managing IP address assignments to prevent conflicts.

DHCP Client: A DHCP client is a device that requests and receives configuration information from a DHCP server. The client typically sends a DHCP request when it joins the network or when its lease is about to expire.

IP Address Conflict Detection: DHCP servers often perform conflict detection to ensure that the IP address they are assigning to a client is not already in use by another device on the network.

Subnet Configuration: DHCP can provide additional configuration information, such as subnet masks, default gateways, DNS server addresses, and more, to clients.

Scalability: DHCP simplifies the management of IP addresses, especially in large networks, by automating the assignment process and reducing the chances of address conflicts.

Reservations: DHCP allows administrators to reserve specific IP addresses for specific devices. This is useful for devices that require consistent IP addresses, such as network printers or servers.

DNS

The Domain Name System (DNS) is a hierarchical naming system that translates human-readable domain names (like www.example.com) into IP addresses (numeric identifiers used to locate devices on a network). DNS plays a fundamental role in the functioning of the internet by enabling users to access resources using familiar domain names. Here's how DNS functions:

Name Resolution: When a user enters a domain name in a web browser, the device sends a DNS query to a DNS resolver to find the corresponding IP address.

DNS Resolver: A DNS resolver is responsible for translating domain names into IP addresses. Resolvers can be configured as local devices, DNS servers of Internet Service Providers (ISPs), or public DNS services like Google DNS or OpenDNS.

Recursive Query: If the resolver doesn't have the IP address in its cache, it sends a recursive query to the DNS hierarchy to find the authoritative DNS server for the domain.

Authoritative DNS Server: The authoritative DNS server is responsible for providing the IP address corresponding to the domain name. It stores the DNS records (such as A, AAAA, CNAME, MX records) that map domain names to IP addresses.

Caching: To improve efficiency, DNS resolvers cache the IP addresses they retrieve. Cached records are stored for a specific duration, known as the Time to Live (TTL).

Email :
SMTP : 25 Port No. (Protocol for sending emails /outgoing emails).

POP	**IMAP**
Post office Protocol	Internet Message Access Protocol
Protocol for retrieving email from email server. (And allows client toto download emails and store them locally).	IMAP is a more advanced protocol for retrieving and managing emails. It allows clients to view emails stored on the server without necessarily downloading them.
POP3 is designed for downloading emails to a single device. Emails are often deleted from the server after downloading, which can result in limited access to emails across multiple devices.	It supports synchronization between the client and server, so changes made on one device are reflected on others.

POP	IMAP
Current version 3; i.e. POP3.Port NO : 110.	Port No : 143
A user cannot organize the emails on the server using POP3.	IMAP allows its users to organize their available emails on the server.
You cannot search for mail content on any mail server using the POP3 protocol. The user needs to download the mail first and then search for the required content.	You can easily search for mail content on any mail server using IMAP without downloading them.
Pop3 is simple and very fast	IMAP is complex and slow as compared to POP3

Chapter 9 : Network management and Security

Network security refers to the practice of protecting computer networks and their resources from unauthorized access, attacks, misuse, and other threats that can compromise the confidentiality, integrity, and availability of data and services. Network security is essential in ensuring the privacy and safety of sensitive information, preventing unauthorized access, and maintaining the smooth operation of networks. It involves a combination of policies, procedures, technologies, and practices designed to safeguard networks and the data they transmit.

Key aspects of network security include:
- Authentication and Authorization.
- Access control.
- Firewalls.
- Intrusion Detection and Prevention System.
- Encryptions.
- Virtual Private Networks.
- Network Monitoring. (SNMP)

SNMP :

Simple Network Management Protocol (SNMP) is an internet standard protocol used to monitor and manage network devices connected over an IP. SNMP is used for

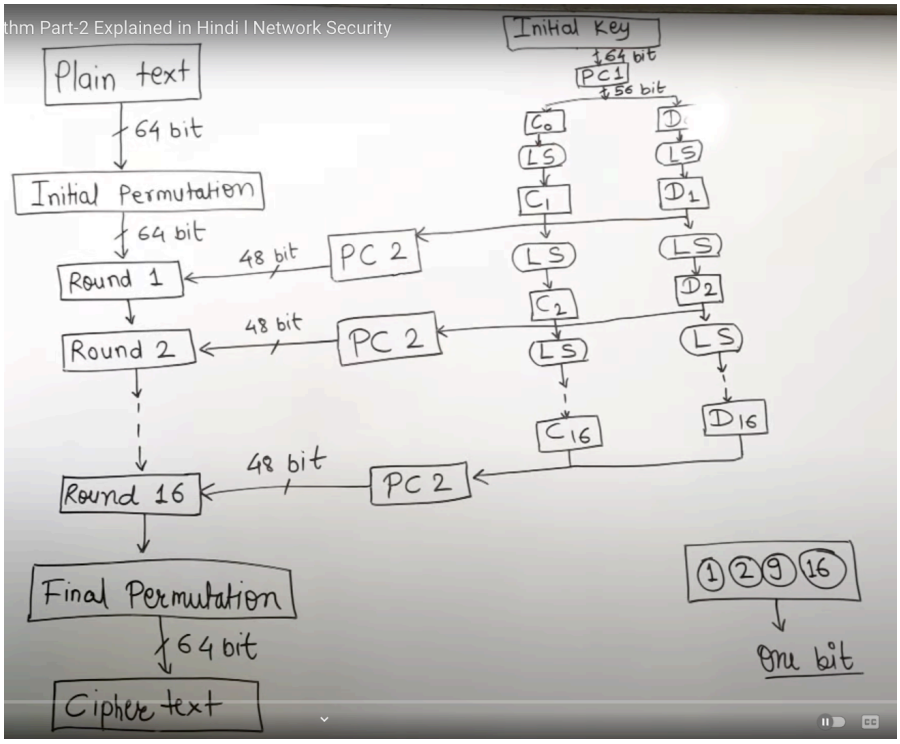
communication between routers, switches, firewalls, load balancers, servers, CCTV cameras, and wireless devices.

Symmetric Key :

Single key is used for encryption and decryption.
Security : relies on same key; so, having one key can access all.
Efficiency : faster than asymmetric cryptography.
Common symmetric key algorithm : Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES).

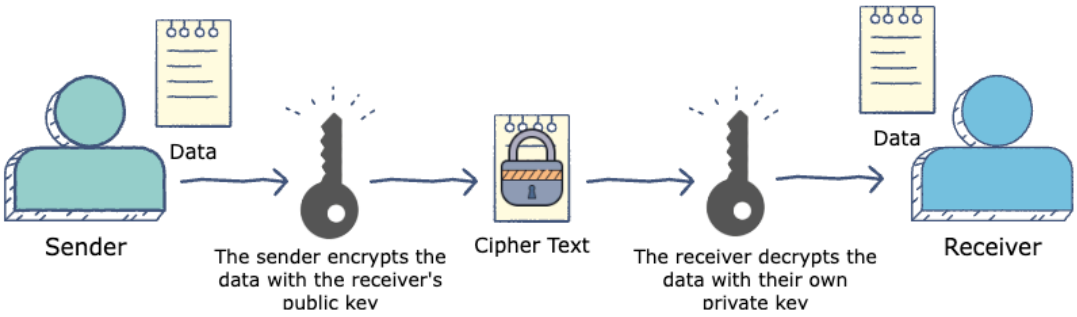
DES:

Input : Plain Text(64 bit)
Output : Cipher Text (64 bit)
Initial Key = 64bit (key considered for algorithm)
PC1 (Permuted Choice 1)
= removes 8 bit and we get 56 bit (64-8); Every 8 bit is discarded.
C0 , D0 ; halfs of the keys
Left Circular shifts.
48bit is subkey for every round
Final Permutation = Inverse of Initial Permutation.



Asymmetric Key :

Two key are used for encryption and decryption. (Private key, and public key)
Security : Private key should be kept secret whereas, public key can be easily distributed.Even if the public key is known, it's computationally infeasible to determine the private key based on it.
Common asymmetric key algorithm : RSA (Rivest-Shamir-Adleman), Diffie-Hellman, and Elliptic Curve Cryptography (ECC).



Operation of RSA:

- Select two large prime numbers x, and y.
- Calculate n = x * y (n is called modulus of encryption and decyption)
- Calculate the totient function; ϕ(n)=(x−1)(y−1)
- Choose a co-prime number e, such that , 1 < e < ϕ(n)
- Thus public key is <e,n>
- Encryption :

  If plainText P is given;

$$C = P^e \bmod n.$$

- Decryption:

Using the private key (n,d) the plaintext can be found as :

5. Calculate d such that $e.d = 1 \bmod \phi(n)$.

d can be found using the ***extended euclidean algorithm***. The pair (n, d) makes up the private key.

$$P = C^d \bmod n.$$

Numerical Example of RSA : https://www.javatpoint.com/rsa-encryption-algorithm

Firewalls:

A firewall is a network security device or software that acts as a barrier between a trusted internal network and potentially untrusted external networks, such as the internet. Its primary purpose is to control and filter incoming and outgoing network traffic based on predetermined security rules. Firewalls play a crucial role in preventing unauthorized access, protecting sensitive data, and defending against various cyber threats. There are several types of firewalls, each with its own features and capabilities:

Packet Filtering Firewall:

Packet filtering firewalls operate at the network layer (Layer 3) of the OSI model.

They examine individual packets of data and determine whether to allow or block them based on predefined rules.

Rules can be based on source and destination IP addresses, port numbers, and protocols.

Packet filtering is efficient but may not provide advanced filtering capabilities.

Stateful Inspection Firewall:

Stateful inspection firewalls operate at the network and transport layers (Layers 3 and 4) of the OSI model.

They maintain a state table that keeps track of active connections and the state of each connection.

Stateful firewalls make decisions based not only on packet attributes but also on the state of the connection, providing better security for various protocols.

Application Layer Firewall (Proxy Firewall):

Application layer firewalls operate at the application layer (Layer 7) of the OSI model.

They act as intermediaries between clients and servers, intercepting and analyzing application-level traffic.

Application layer firewalls can enforce more granular security policies and perform content filtering.

They may also provide additional services such as caching and user authentication.

Next-Generation Firewall (NGFW):

NGFWs combine traditional firewall functionality with advanced features such as intrusion prevention, deep packet inspection, application awareness, and user identity tracking.

They can identify and block advanced threats and provide visibility into applications and user activities.

Proxy Server Firewall:

Proxy server firewalls operate as intermediaries between clients and servers, forwarding requests on behalf of clients.

They can hide internal network details from external clients and provide additional security by blocking direct connections.

Proxy firewalls can also cache content to improve performance.

Network Address Translation (NAT) Firewall:

NAT firewalls translate private IP addresses to a single public IP address, allowing multiple devices to share the same public IP.

NAT provides a level of network security by obfuscating internal IP addresses from external networks.

Chapter -7 : Congestion Control & Quality of Services

Congestion control

Congestion control is a crucial aspect of network management that aims to prevent or reduce network congestion, which occurs when the demand for network resources exceeds its capacity. Congestion can lead to performance degradation and reduced quality of service. Open-loop and closed-loop congestion control are two approaches used to manage and address network congestion:

Open-Loop Congestion Control:
In open-loop congestion control, the network takes proactive measures to prevent congestion before it actually occurs. This approach relies on predictions and estimates of future network load to adjust resource allocation. It's a preventive strategy that tries to avoid congestion altogether. Examples of open-loop congestion control techniques include:

Traffic Shaping: This involves regulating the rate at which traffic enters the network to prevent sudden spikes that could lead to congestion. Traffic shaping smooths out the flow of traffic by limiting its rate.

Admission Control: Before allowing new traffic flows to enter the network, admission control checks if there is sufficient bandwidth and resources available to accommodate the new traffic without causing congestion.

Quality of Service (QoS) Guarantees: By allocating different levels of priority or resources to different types of traffic (such as voice, video, or data), QoS mechanisms ensure that critical traffic receives the necessary resources, reducing the likelihood of congestion.

Closed-Loop Congestion Control:
In closed-loop congestion control, the network detects congestion after it occurs and takes reactive measures to alleviate it. This approach relies on feedback from the network to adjust resource allocation dynamically. Closed-loop congestion control is more responsive to real-time conditions. Examples of closed-loop congestion control techniques include:

Explicit Congestion Notification (ECN): Routers or switches mark packets with an ECN bit when congestion is detected. Receivers respond to ECN-marked packets by reducing their sending rate, allowing the network to recover from congestion.

Queue Management: Routers manage their queues by using algorithms like Random Early Detection (RED) or Active Queue Management (AQM). These algorithms drop or mark packets based on the length of the queue, helping to prevent excessive buildup of packets and congestion.

TCP Congestion Control: Transmission Control Protocol (TCP) is a widely used protocol for reliable data transfer. TCP uses congestion control mechanisms like TCP congestion **window adjustment and slow start** to adapt its sending rate based on network conditions.

Prepared and compiled by Saroj Dahal