6B22ICSC: Computer Networks

Lecture Notes

Remya P K

LaTeX Prepared by Abhinav Raj

Contents

Unit I

1. Introduction to the Internet

1.1 Computer Networks

- A network is a group of two or more computer systems (Multiple gadgets, also called hosts), which are connected through multiple channels for the purpose of sending and receiving data (records/media) in a shared environment.
- The Internet is a group of computer systems connected from all around the world.
- The Internet protocol suite is a framework defined by the Internet standards. Methods are divided into a layered set of protocols in this architecture.

1.1.1 Working of the internet

- The internet is a global computer network that connects various devices and sends a lot of information and media.
- It uses an Internet Protocol (IP) and Transport Control Protocol (TCP)-based packet routing network.
- TCP and IP work together to ensure that data transmission across the internet is consistent and reliable, regardless of the device or location.

1.1.2 Protocols

- A network protocol is an accepted set of rules that govern data communication between different devices in the network.
- It determines what is being communicated, how it is being communicated, and when it is being communicated.

1.1.3 Access Network

- An access network is a type of network that physically connects an end system to the immediate router (also known as the "edge router") on a path from the end system to any other distant end system.
- Examples of access networks are ISP, home networks, enterprise networks, ADSL, mobile network, FTTH, etc.

1.1.4 Layered architecture of network

- TCP/IP-1970 Transmission Control Protocol Internet Protocol
- ISO-OSI-1983 International Organization for Standardization OSI, Open Systems Interconnection

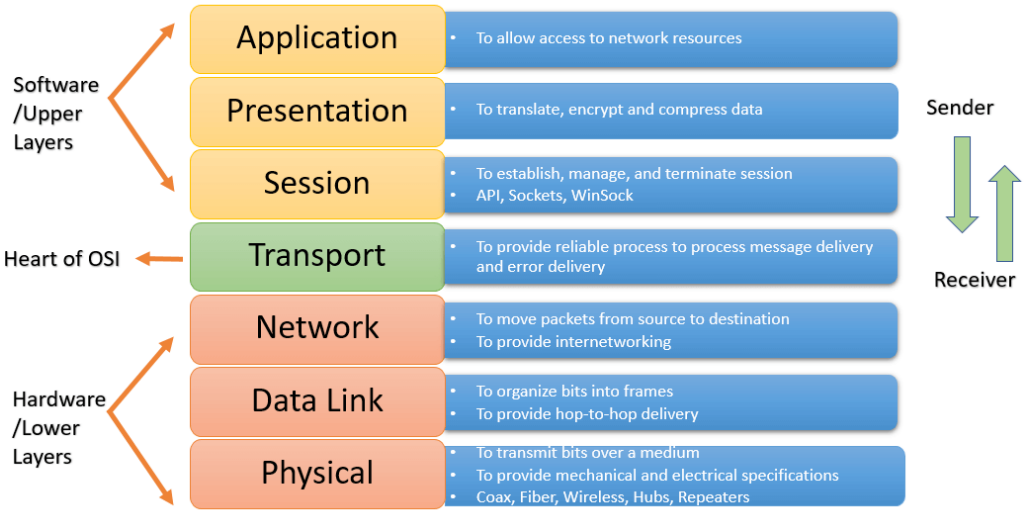


Figure 1.1: OSI Diagram

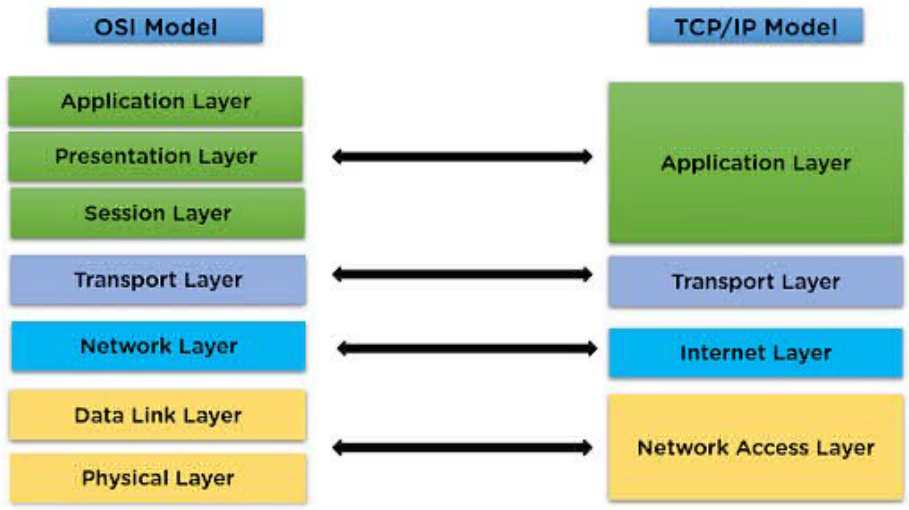
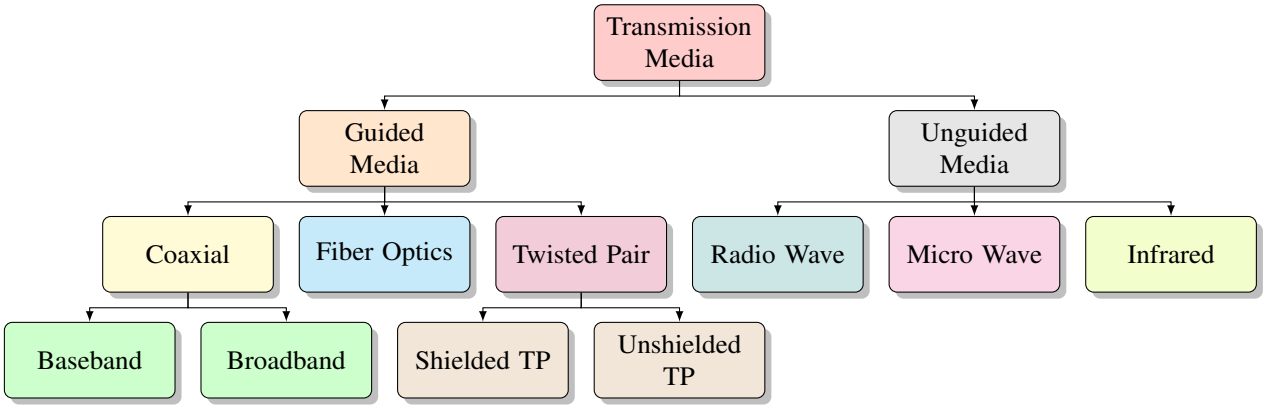


Figure 1.2: OSI Vs TCP

1.2 Types of Transmission Media

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver, i.e., it is the channel through which data is sent from one place to another.



1.2.1 Guided Media

- Guided Media is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.
- Features:
  - High Speed
  - Secure
  - Used for comparatively shorter distances

There are three types of guided media. They are

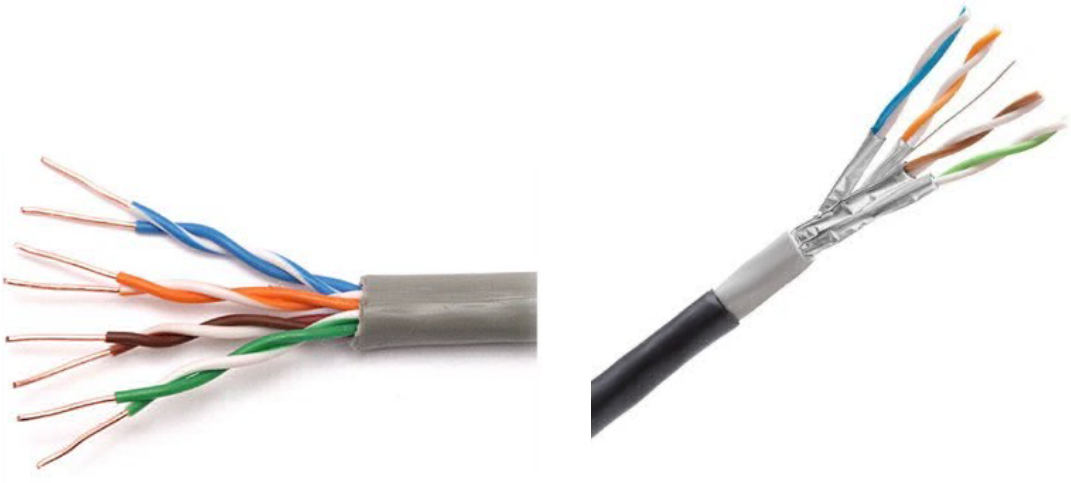
Twisted Pair Cable

- It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath.
- They are the most widely used Transmission Media.
- They are two types of Twisted pair.

1. **Unshielded Twisted Pair (UTP):**
   - UTP consists of two insulated copper wires twisted around one another.
   - This type of cable has the ability to block interference and does not depend on a physical shield for this purpose.
   - It is used for telephonic applications.
2. **Shielded Twisted Pair (STP):**
   - This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference.
   - It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

Advantages and Disadvantages of UTP

- **Advantages :**
  - Least expensive
  - Easy to install
  - High-speed capacity



(a) UTP (b) STP

Figure 1.3: Twisted Pair Cable

- **Disadvantages :**
  - Susceptible to external interference
  - Lower capacity and performance in comparison to STP
  - Short-distance transmission due to attenuation
- **Applications :** Used in telephone connections and LAN networks

Advantages and Disadvantages of STP

- **Advantages:**
  - Better performance at a higher data rate in comparison to UTP
  - Eliminates crosstalk
  - Comparatively faster
- **Disadvantages:**
  - Comparatively difficult to install and manufacture
  - More expensive and Bulky
- **Applications :** Most frequently used in extremely cold climates, where the additional layer of outer covering makes it perfect for withstanding such temperatures or for shielding the interior components.

Coaxial Cable

It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes:
Baseband mode (dedicated cable bandwidth) and **Broadband mode** (cable bandwidth is split into separate ranges).

Advantages and Disadvantages of Coaxial Cable

- **Advantages:**
  - High Bandwidth
  - Better noise Immunity
  - Easy to install and expand
  - Inexpensive

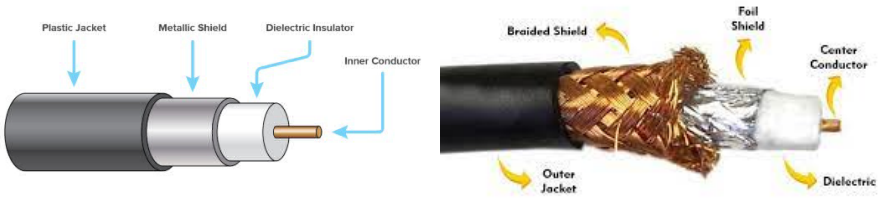


Figure 1.4: Coaxial Cable

- **Disadvantages:**
  - Single cable failure can disrupt the entire network
- **Applications :** Radio frequency signals are sent over coaxial wire. It can be used for cable television signal distribution, digital audio (S/PDIF), computer network connections (like Ethernet), and feedlines that connect radio transmitters and receivers to their antennas.

Optical Fiber Cable

It uses the concept of refraction of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.

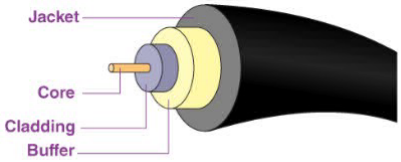


Figure 1.5: Optical Fibre Cable

Advantages and Disadvantages of Optical Fiber Cable

- **Advantages:**
  - Increased capacity and bandwidth
  - Lightweight
  - Less signal attenuation
  - Immunity to electromagnetic interference
  - Resistance to corrosive materials
- **Disadvantages:**
  - Difficult to install and maintain
  - High cost
  - Fragile
- **Applications:**
  - Medical Purpose: Used in several types of medical instruments.
  - Defence Purpose: Used in transmission of data in aerospace.
  - For Communication: This is largely used in the formation of internet cables.
  - Industrial Purpose: Used for lighting purposes and safety measures in designing the interior and exterior of automobiles.

1.2.2 Unguided Media

- It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.
- Features:
  - The signal is broadcasted through the air
  - Less Secure
  - Used for larger distances

Types of Signals Transmitted Through Unguided Media

- **Radio Waves :** These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range: 3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission. Further Categorized as
  - Terrestrial
  - Satellite.
- **Microwaves :** It is a line of sight transmission, i.e., the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range: 1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.
- **Infrared :** Infrared waves are used for very short-distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range: 300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

1.3 Switching

Switching is a technique used to transmit data between networks. It is achieved by using switches that connect multiple LAN networks. There are two types -

- Packet Switching
- Circuit Switching

1.3.1 Packet Switching

Store-and-Forward Switching:

- Switching data packets by the switching device that receives the data frame and then checks for errors before forwarding the packets.
- It supports the efficient transmission of non-corrupted frames. It is generally used in telecommunication networks.
- The switching device waits to receive the entire frame and then stores the frame in the buffer memory.
- Then the frame is checked for errors by using CRC (Cyclic Redundancy Check). If the error is found, then the packet is discarded; else, it is forwarded to the next device.

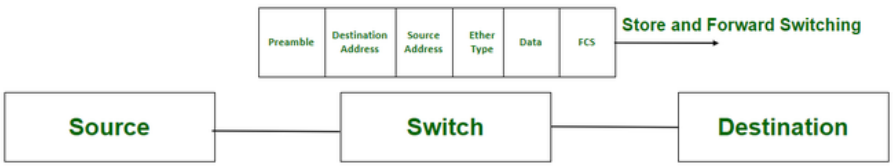


Figure 1.6: Store-and-Forward Switching

Cut-through Switching:

- Switching data packets by the switching device that forwards the packets as soon as the destination address is available without waiting for the rest of the data to arrive.
- It supports low latency and high-speed transmission and requires less storage space. It is used in fiber channel transmission.
- Data transmission starts as soon as the destination address field arrives at the switching device.
- Then the device performs a lookup operation to check whether the destination address is valid or not.
- If the address is found valid and the link to the destination is available, then the switching device starts to transmit the packets to the destination without waiting for the rest of the frame to arrive.

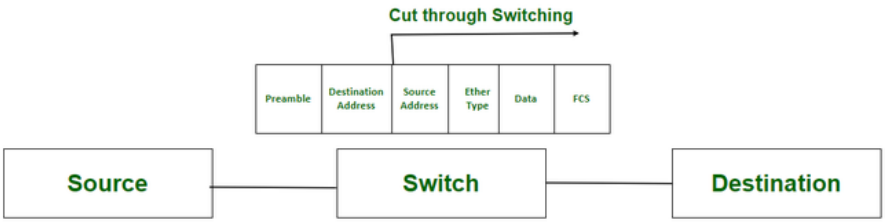


Figure 1.7: Cut-through Switching

Advantages

One of the main advantages of packet switching is that it allows multiple packets to be transmitted simultaneously across the network, making more efficient use of network resources than circuit switching.

Disadvantages

However, packet switching can also introduce delays into the transmission process, impacting the performance of network applications.

Types of Delays in Packet Switching

- **Transmission Delay** : This is the time it takes to transmit a packet over a link. It is affected by the size of the packet and the bandwidth of the link.
- **Propagation Delay** : This is the time it takes for a packet to travel from the source to the destination. It is affected by the distance between the two nodes and the speed of light.
- **Processing Delay** : This is the time it takes for a packet to be processed by a node, such as a router or switch. It is affected by the processing capabilities of the node and the complexity of the routing algorithm.
- **Queuing Delay** : This is the time a packet spends waiting in a queue before it can be transmitted. It is affected by the number of packets in the queue and the priority of the packets.

1.3.2 Circuit Switching

In circuit switching, network resources (bandwidth) are divided into pieces, and bit delay is constant during a connection. The dedicated path/circuit established between sender and receiver provides a guaranteed data rate, allowing data to be transmitted without any delays once the circuit is established.

Types

- FDM (Frequency Division Multiplexing)
- TDM (Time Division Multiplexing)

Frequency Division Multiplexing

Frequency Division Multiplexing (FDM) divides into multiple bands. It is used when multiple data signals are combined for simultaneous transmission via a shared communication medium. The total bandwidth is divided into non-overlapping frequency sub-bands, each carrying a different signal. Practical use includes radio spectrum and optical fiber to share multiple independent signals.

Time Division Multiplexing

Time Division Multiplexing (TDM) divides into frames. It is a method of transmitting and receiving independent signals over a common signal path. TDM is used for long-distance communication links and handles heavy data traffic loads from end-users. TDM is also known as a digital circuit-switched method.

Drawbacks of Circuit Switching

- Inefficient use of resources
- Vulnerability to failures
- Delay and latency
- High cost
- Lack of flexibility
- Limited mobility
- Limited capacity

1.4 Throughput

In data transmission, network throughput is the amount of data moved successfully from one place to another in a given time period. Network throughput is typically measured in bits per second (bps), as in megabits per second (Mbps) or gigabits per second (Gbps).

Packet Loss in Package-Switched Networks

Basically, this means that when sending a lot of packets into a queue at a high rate (or at the same time), packet loss will be experienced as the queue will be maxed out and the router will drop packets. This will start a “chain-reaction” of increasing the rate of incoming packets, as the dropped packets will need to be retransmitted to the router.

1.5 Network devices

Network devices are essential components in the infrastructure of computer networks, serving various functions to enable efficient communication and data transfer. **Routers** are pivotal in directing data packets between different networks, determining optimal transmission paths based on IP addresses. **Switches** connect multiple devices within a local area network (LAN), using MAC addresses to forward data packets only to the intended recipients, thereby reducing network congestion. **Modems** facilitate network connectivity by converting digital signals from computers into analog signals for transmission over telephone lines or cable systems. **Repeaters** amplify or regenerate signals to extend network connections over longer distances, maintaining signal integrity. **Bridges** interconnect multiple network segments or LANs, facilitating communication between them. Together, these devices form the backbone of modern communication networks, ensuring seamless data exchange and connectivity.

1.5.1 Hub

A hub is a networking device that connects multiple PCs to a single network, operating on the OSI physical layer.

Device	Layer in OSI Model	Function
Hub	Physical layer	To connect a network of personal computers together, they can be joined through a central hub.
Switch	Data Link Layer	Allows connecting multiple devices, managing ports, creating VLANs for security, and operates at Layer 2 of the OSI model.

Table 1.1: Comparison between Hub and Switch

1.5.2 Bridge

A bridge connects multiple network segments at the data link layer.

Criteria	Switch	Bridge
Packet Forwarding	Hardware-based using ASICs	Software-based
Switching Method	Store-and-Forward; Fragment-Free; Cut-Through	Store-and-Forward
Error Checking	Can perform error checking	Can not perform error checking
Buffers	Has buffers	Maybe not have a buffer

Table 1.2: Comparison between Switch and Bridge

1.5.3 Switch

A switch connects multiple devices on a single computer network, operating on the OSI data link layer. A switch stores **MAC addresses (48 bits)** in its lookup table and maintains its own address.

1.5.4 Router

A router is used to connect to the internet. A router stores **IP addresses (32 bits)** in its routing table and maintains its own address.

1.5.5 Repeater

A repeater is used to repeat signals received by a router.

Feature	Router	Repeater
Function	Connects different networks	Extends the range of a network
OSI Layer	Network Layer (Layer 3)	Physical Layer (Layer 1)
Device Type	Networking device	Signal booster
Range	Covers larger areas	Limited coverage area
Complexity	More complex	Simple
Example Use Case	Connects home network to the internet	Extends Wi-Fi range in a large building

Table 1.3: Comparison between routers and repeaters

1.5.6 Socket

A socket is one endpoint of a two-way communication link between two programs running on the network. The socket mechanism provides a means of inter-process communication (IPC) by establishing named contact points between which the communication takes place.

- Like 'Pipe' is used to create pipes and sockets is created using 'socket' system call.
- The socket provides bidirectional FIFO Communication facility over the network.
- A socket connecting to the network is created at each end of the communication.
- Each socket has a specific address. This address is composed of an IP address and a port number.

Function Call	Description
`socket()`	To Create a socket
`bind()`	It's a socket identification like a telephone number to contact
`listen()`	Ready to receive a connection
`connect()`	Ready to act as a sender
`accept()`	Confirmation, it is like accepting to receive a call from a sender
`write()`	To send data
`read()`	To receive data
`close()`	To close a connection

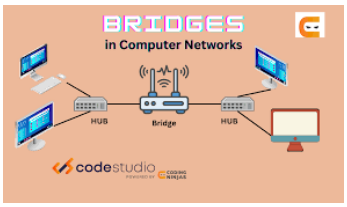
Table 1.4: Socket Function Calls

Types of Sockets

- **Datagram socket :** This is a type of network that has a connectionless point for sending and receiving packets, similar to a mailbox. The letters (data) posted into the box are collected and delivered (transmitted) to a letterbox (receiving socket).
- **Stream socket :** This type of network socket provides a reliable, connection-oriented communication channel. It ensures that data is delivered in the correct order and without loss. Stream sockets are typically used for applications that require a continuous stream of data, such as audio and video streaming.

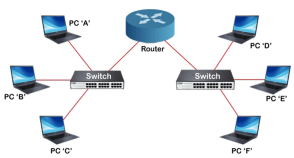
(a) Hub

(b) Switch



(c) Bridge

(d) Hub



(e) Switch

Figure 1.8: Network Devices

1.6 OSI Layers

The OSI (Open Systems Interconnection) model defines seven layers, each responsible for specific functions in network communication.

1.6.1 Layer 1 - Physical Layer

This layer deals with the physical connection between devices. It defines the physical media, such as cables or wireless transmission, and the electrical and mechanical specifications for data transmission.

Functions

- **Bit synchronization :** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver, providing synchronization at the bit level.
- **Bit rate control :** The Physical layer also defines the transmission rate, i.e., the number of bits sent per second.
- **Physical topologies :** The Physical layer specifies how different devices/nodes are arranged in a network, such as bus, star, or mesh topology.
- **Transmission mode :** The Physical layer also defines how data flows between the two connected devices. Various transmission modes possible are Simplex, half-duplex, and full-duplex.
- Data in the Physical layer is referred to as **Bits**.
- **Hub, Repeater, Modem, and Cables** are Physical Layer devices.

1.6.2 Layer 2 - Data Link Layer

The data link layer handles the reliable transmission of data across a physical link. It provides error detection and correction, as well as framing, addressing, and flow control.

- This layer is responsible for the node-to-node delivery of the message.
- The main function of this layer is to ensure error-free data transfer from one node to another, over the physical layer.
- When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.
- Packet in the Data Link layer is referred to as **Frame**.
- Data Link layer is handled by the **NIC** (Network Interface Card) and device drivers of **host machines**.
- **Switch & Bridge** are Data Link Layer devices
- The Data Link Layer is divided into two sublayers:
  - Logical Link Control (LLC)
  - Media Access Control (MAC)

Functions

- **Framing :** Provides a way for a sender to transmit a set of bits that are meaningful to the receiver.
- Physical addressing: Adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.
- **Error control :** Detects and retransmits damaged or lost frames.
- **Flow Control :** Coordinates the amount of data that can be sent before receiving an acknowledgment.
- **Access control :** Determines which device has control over the channel at a given time.

1.6.3 Layer 3 - Network Layer

This layer is responsible for routing packets between different networks. It determines the best path for data to travel from the source to the destination, considering factors such as network congestion and available bandwidth.

- The network layer works for the transmission of data from one host to the other located in different networks (**source to destination delivery**).
- It also takes care of **packet routing**
- The sender & receiver's **IP addresses** are placed in the header by the network layer.
- Segment in the Network layer is referred to as **Packet**.
- Network layer is implemented by networking devices such as **routers**.

Functions

- **Routing :** Determines suitable routes from source to destination.
- **Logical Addressing :** Defines an addressing scheme to identify each device on the Internetwork uniquely.
- The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

1.6.4 Layer 4- Transport Layer

The transport layer ensures the reliable delivery of data between end systems. It provides error detection and correction, flow control, and segmentation and reassembly of data to support larger messages.

- Provides services to the application layer and takes services from the network layer.
- The data in the transport layer is referred to as **Segments**.
- Responsible for the **End to End Delivery** of the complete message.
- Provides **acknowledgment of successful data transmission** and re-transmits data if an error is found.
- Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.
- The transport layer is called as **Heart of the OSI model**.

Functions

1. **Sender's Side**:
   - Receives formatted data from upper layers.
   - Performs segmentation of data into manageable units.
   - Implements flow and error control mechanisms for reliable transmission.
   - Adds source and destination port numbers to the header for proper addressing.
2. **Receiver's Side**:
   - Reads the port number from the header of received data.
   - Forwards the data to the respective application based on the destination port.
   - Performs sequencing to arrange received segments in the correct order.
   - Reassembles the segmented data into the original message for delivery to the application layer.

Services Provided

1. **Connection-Oriented Service**
   - It is a three-phase process that includes:
     (a) Connection Establishment
     (b) Data Transfer
     (c) Termination/disconnection

- In this type of transmission, the receiving device sends an acknowledgment back to the source after a packet or group of packets is received.
- This type of transmission is reliable and secure.

2. **Connectionless Service**
   - It is a one-phase process and includes Data Transfer.
   - In this type of transmission, the receiver does not acknowledge receipt of a packet.
   - This approach allows for much faster communication between devices.
   - Connection-oriented service is more reliable than connectionless service.

1.6.5 Layer 5 - Session Layer

The session layer establishes, maintains, and terminates connections between applications. It allows applications on different devices to communicate with each other by managing sessions and synchronizing data exchange.

- Responsible for the establishment of connection, maintenance of sessions, authentication, and ensures security.
- Implementation of 3 layers(session,presentation and application) is done by the network application itself. These are also known as Upper Layers or Software Layers.
- The data in the session layer is referred to as **Message**.

Functions

- **Session establishment, maintenance, and termination :** The layer allows the two processes to establish, use and terminate a connection.
- **Synchronization :** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- **Dialog Controller :** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

1.6.6 Layer 6 - Presentation Layer

This layer is responsible for data representation and encryption. It translates data formats between the application layer and the network, ensuring that data is in a usable format for the recipient and providing encryption and decryption services for secure communication.

- Also called the **Translation layer**.
- Manipulates data from the application layer to required format for transmission over the network.
- The data in the presentation layer is referred to as **Message**.

Functions

- **Translation :** For example, ASCII to EBCDIC.
- **Encryption/Decryption :** Data encryption translates the data into another form or code.
- The encrypted data is known as the ciphertext and the decrypted data is known as plain text.
- A key value is used for encrypting as well as decrypting data.
- **Compression :** Reduces the number of bits that need to be transmitted on the network.

1.6.7 Layer 7- Application Layer

The application layer provides network services directly to end users. It includes protocols for services such as file transfer, email, and remote login, allowing users to access network resources and communicate with other users and applications.

- These applications produce the data, which has to be transferred over the network.
- Serves as a window for the application services to access the network and display received information to the user. Example: Application – Browsers, Skype Messenger, etc.
- The data in the session layer is referred to as **Message**.
- The application Layer is also called **Desktop Layer**.

Functions

- Network Virtual Terminal
- FTAM- File Transfer Access and Management
- Mail Services
- Directory Services

Features

- To ensure smooth communication, application layer protocols are implemented the same on the source host and destination host.
- The Application Layer protocol defines a process for both parties involved in communication.
- These protocols define the type of message being sent or received from either the source host or destination host.
- These protocols not only define the basic syntax of messages and the method of transmission, but also specify the expected responses and interactions with the next level.

Layer No	Layer Name	Responsibility	Information Form	Device
7	Application Layer	Helps in identifying the client and synchronizing communication.	Message	-
6	Presentation Layer	Data from the application layer is extracted and manipulated in the required format for transmission.	Message	-
5	Session Layer	Establishes Connection, Maintenance, Ensures Authentication, and Ensures security.	Message	Gateway
4	Transport Layer	Take Service from Network Layer and provide it to the Application Layer.	Segment	Firewall
3	Network Layer	Transmission of data from one host to another, located in different networks.	Packet	Router
2	Data Link Layer	Node to Node Delivery of Message.	Frame	Switch, Bridge
1	Physical Layer	Establishing Physical Connections between Devices.	Bits	Hub, Repeater, Modem, Cables

Table 1.5: OSI Layers

1.7 Application Layer Protocols

The application layer provides several protocols which allow any software to easily send and receive information and present meaningful data to its users. Some of the commonly used protocols include:

→ **Telnet :** Telnet stands for Telecommunications Network. This protocol is used for managing files over the Internet. It allows Telnet clients to access the resources of Telnet servers. Telnet typically uses port number 23.

→ **FTP (File Transfer Protocol) :** FTP is used for transferring files from one device to another. It promotes sharing of files via remote computer devices with reliable, efficient data transfer. FTP uses port number 20 for data access and port number 21 for data control.

→ **HTTP (Hypertext Transfer Protocol) :** HTTP is the foundation of data communication for the World Wide Web. It defines the structure of messages and how they are transmitted, allowing for the retrieval of linked resources from across the web. HTTP typically uses port number 80.

→ **SMTP (Simple Mail Transfer Protocol) :** SMTP is used to transfer electronic mail from one user to another. It provides a mail exchange between users on the same or different computers and supports sending messages containing text, voice, video, or graphics. SMTP typically uses port number 25.

→ **POP3 (Post Office Protocol version 3) :** POP3 is an application-layer protocol used by email clients to retrieve email from a mail server. It allows users to download their email messages to their local device for offline access. POP3 typically uses port number 80.

→ **DHCP (Dynamic Host Configuration Protocol) :** DHCP provides IP addresses to hosts. Whenever a host tries to register for an IP address with the DHCP server, DHCP server provides lots of information to the corresponding host. Port Numbers: 67 (for server), 68 (for client)

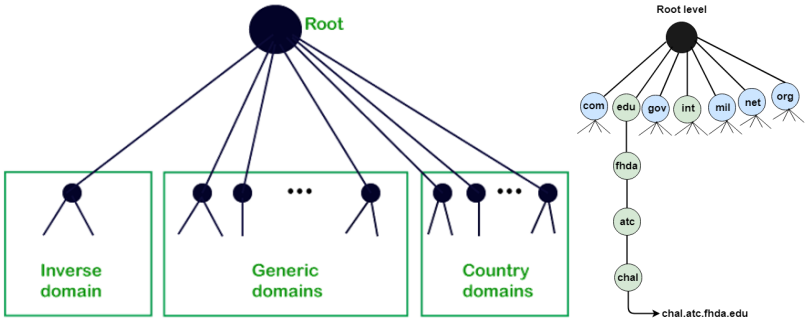
→ **DNS (Domain Name System) :** DNS translates domain names into corresponding IP addresses, enabling users to access resources on the Internet using user-friendly names instead of numerical IP addresses. DNS typically uses port number 53.

Port #	Protocol	Type	Description
20	FTP	TCP	File Transfer Protocol - data
21	FTP	TCP	File Transfer Protocol - control
22	SSH	TCP/UDP	Secure Shell for secure login
23	Telnet	TCP	Unencrypted login
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP/UDP	Domain Name Server
67/68	DHCP	UDP	Dynamic Host Configuration Protocol
80	HTTP	TCP	HyperText Transfer Protocol
123	NTP	UDP	Network Time Protocol
161,162	SNMP	TCP/UDP	Simple Network Management Protocol
389	LDAP	TCP/UDP	Lightweight Directory Authentication Protocol
443	HTTPS	TCP/UDP	HTTP with Secure Socket Layer

Table 1.6: Common Ports and Protocols

1.7.1 Domain Name System (DNS)

The DNS service translates user-chosen domain names into corresponding IP addresses. For instance, if a user selects the domain name "www.example.com", DNS translates it into the corresponding IP address (e.g., 192.36.20.8). DNS serves as a directory service, facilitating the mapping between a host's name and its numerical address on the network. This mapping enables users to access resources on the Internet using user-friendly names, enhancing reliability compared to using IP addresses directly. DNS also manages how application processes running on different systems communicate by facilitating the exchange of messages between them. Each node in a tree structure represents a domain name, and a full domain name is a sequence of symbols separated by dots.



- **Generic Domains :** Generic domains define registered hosts according to their generic behavior. Each node in a tree defines the domain name, which is an index to the DNS database. It uses three-character labels, and these labels describe the organization type.
- **Country Domain :** The country domain format is the same as a generic domain, but it uses two-character country abbreviations (e.g., "us" for the United States) in place of three-character organizational abbreviations.
- **Inverse Domain :** The inverse domain is used for mapping an address to a name. It is used to determine whether the client is on the authorized list by sending a query to the DNS server.

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

Table 1.7: Generic Domain Labels

1.7.2 Simple Mail Transfer Protocol (SMTP)

SMTP, or Simple Mail Transfer Protocol, serves as a foundational set of communication guidelines facilitating the transmission of electronic mail over the internet. It functions as a program designed for sending messages to other computer users based on their email addresses. SMTP enables mail exchange between users, whether they are on the same or different computers. Notably, it supports the sending of single messages to one or multiple recipients, encompassing various forms of content such as text, voice, video, or graphics. Additionally, SMTP can send messages across networks beyond the internet. Its primary purpose lies in establishing communication rules between servers. Servers employing SMTP have mechanisms for identifying themselves and specifying the nature of communication they intend to conduct. Furthermore, they possess error-handling capabilities, such as responding to incorrect email addresses with appropriate error messages.

1.7.3 FTP (File Transfer Protocol)

FTP is a standard Internet protocol provided by TCP/IP for transmitting files from one host to another. It is mainly used for transferring web page files from their creators to servers that act as hosts for other computers on the Internet. FTP provides reliable and efficient data transfer and promotes the sharing of files via remote computer devices.

1.8 Video Streaming

Video streaming involves the continuous transmission of video files from a server to a client. It enables users to view videos online without having to download them. Video streaming can include movies, TV shows, YouTube videos, and live streamed content. Unlike downloading, where a copy of the entire file is saved onto a device's hard drive before playback, streaming allows the video to be played in real-time without copying and saving the entire file locally.

1.8.1 How Streaming Works

Just like other data that's sent over the Internet, audio and video data is broken down into data packets. Each packet contains a small piece of the file, and an audio or video player in the browser on the client device takes the flow of data packets and interprets them as video or audio. Some streaming methods use UDP, and some use TCP. UDP and TCP are transport protocols, meaning they are used for moving packets of data across networks

1.8.2 Streaming vs. Downloading

Streaming is real-time, and it's more efficient than downloading media files. If a video file is downloaded, a copy of the entire file is saved onto a device's hard drive, and the video cannot play until the entire file finishes downloading. If it's streamed instead, the browser plays the video without actually copying and saving it. The video loads a little bit at a time instead of the entire file loading at once, and the information that the browser loads is not saved locally.

1.8.3 Factors that slow down streaming

- On the network side
  1. Network latency
  2. Network congestion
- On the user side
  1. WiFi problems
  2. Slowly performing client devices
  3. Not enough bandwidth

Unit II

2. Transport Layer: Protocols & Control

2.1 Transport Layer

The Transport Layer is the fourth layer in the OSI (Open Systems Interconnection) model. It provides end-to-end communication services for applications running on different hosts. The primary functions of the Transport Layer include ensuring data integrity, providing reliable data transfer, managing flow control, and controlling congestion in the network. It also handles multiplexing and demultiplexing of data streams.

2.1.1 Key Functions

End-to-End Communication

The Transport Layer ensures that data is transmitted from the source to the destination application correctly and in the right order. It provides a logical communication channel between application processes on different hosts.

Error Detection and Correction

The Transport Layer uses error detection and correction mechanisms to ensure the integrity of the data being transmitted. It detects errors in the transmitted data and requests retransmission if errors are found.

Flow Control

Flow control mechanisms prevent the sender from overwhelming the receiver with too much data at once. This ensures that the receiver can process the received data at a manageable rate.

Congestion Control

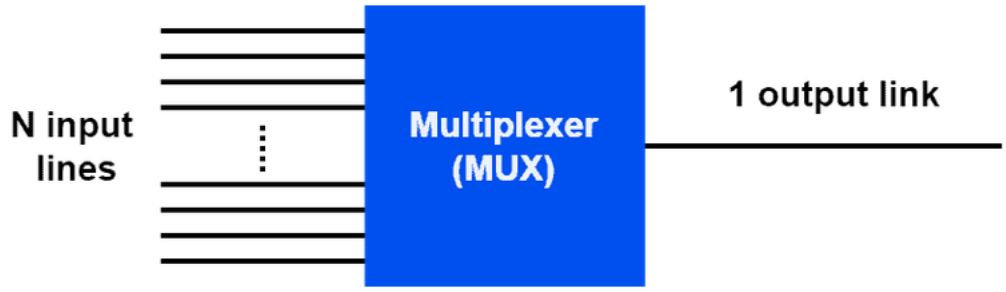
Congestion control techniques are used to prevent network congestion by controlling the rate at which data is sent into the network.

2.2 Multiplexing and Demultiplexing

Multiplexing and demultiplexing are crucial processes within the Transport Layer that enable efficient data transmission over a network. These processes ensure that data from multiple applications can be sent and received using a single network connection, optimizing the use of available bandwidth.

2.2.1 Multiplexing

Multiplexing is the process of combining multiple signals or data streams into one. This allows multiple applications or users to share the same communication channel or network link, which is particularly important in modern networks where bandwidth is a valuable resource.



Types of Multiplexing

There are several types of multiplexing techniques used in communication systems:

- **Time Division Multiplexing (TDM)**: This technique divides the time into several slots, each dedicated to a different data stream. For example, in a TDM system, each user's data might be transmitted in a specific time slot within a repeating time frame.
- **Frequency Division Multiplexing (FDM)**: This method assigns different frequency bands to different data streams. Each user transmits at a different frequency, allowing multiple signals to be sent simultaneously over the same medium without interference.

2.2.2 Time Division Multiplexing (TDM)

Time Division Multiplexing is a technique where the available bandwidth of a communication channel is divided into time slots. Each input signal is assigned to a specific time slot, and these slots are transmitted sequentially.

How TDM Works

1. **Division into Time Slots**: The total available time on the communication channel is divided into equal time slots.
2. **Assignment to Signals**: Each time slot is assigned to a different data stream.
3. **Sequential Transmission**: Data from each signal is transmitted in its assigned time slot in a repeating cycle.

Example of TDM

Consider a scenario with four data streams (A, B, C, D). In TDM:

- The communication channel is divided into four time slots.
- Data from stream A is transmitted in the first slot, B in the second, C in the third, and D in the fourth.
- This cycle repeats continuously, allowing all four streams to share the same channel.

Advantages of TDM

- **Efficient Use of Bandwidth**: Maximizes the utilization of the available channel by ensuring that all time slots are filled.
- **Simplicity**: Easy to implement and manage, especially in digital communication systems.
- **Flexibility**: Can be adjusted to handle varying data rates by changing the duration of time slots.

Disadvantages of TDM

- **Latency**: There can be a delay for each signal as it waits for its time slot.
- **Synchronization**: Requires precise synchronization between the transmitter and receiver to ensure the correct time slot is used.

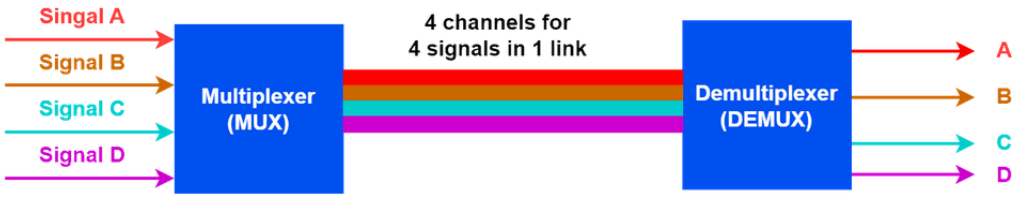
2.2.3 Frequency Division Multiplexing (FDM)

Frequency Division Multiplexing divides the available bandwidth of a communication channel into multiple frequency bands, each carrying a separate data stream simultaneously.

How FDM Works

1. **Division into Frequency Bands**: The total bandwidth is divided into several non-overlapping frequency bands.
2. **Assignment to Signals**: Each frequency band is assigned to a different data stream.
3. **Simultaneous Transmission**: All data streams are transmitted simultaneously on their respective frequency bands.

Example of FDM



Consider a scenario with four data streams (A, B, C, D). In FDM:

- The communication channel is divided into four frequency bands.
- Data from stream A is transmitted on the first band, B on the second, C on the third, and D on the fourth.
- All four streams are transmitted at the same time without interfering with each other.

Advantages of FDM

- **Simultaneous Transmission**: Multiple signals can be sent at the same time, reducing latency.
- **No Synchronization Required**: Unlike TDM, FDM does not require precise time synchronization.
- **Continuous Data Streams**: Suitable for continuous signals like radio and TV broadcasts.

Disadvantages of FDM

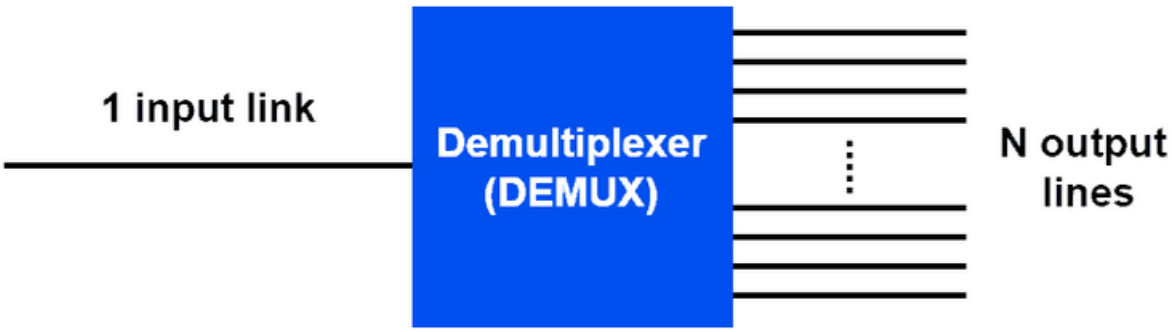
- **Interference**: Frequency bands must be carefully spaced to avoid interference.
- **Complexity**: Requires more complex filters and circuitry to separate frequency bands.
- **Bandwidth Limitation**: The total available bandwidth is divided, potentially limiting the data rate of each signal.

Advantages	Disadvantages
Allows multiple data streams to be transmitted over a single channel	Can be complex. Hence, require specialized equipment and expertise to implement
Reduces the cost of transmitting data	Can limit the flexibility of a system. Therefore, as all data streams must be compatible with the same channel
Reduces the amount of time required to transmit data	If the multiplexing system fails, all data streams transmitted over the channel will be affected
Allows more data to be transmitted over a given bandwidth	Can increase latency, as data streams may have to wait to be transmitted over the channel

Table 2.1: Advantages and Disadvantages of Multiplexing

2.2.4 Demultiplexing

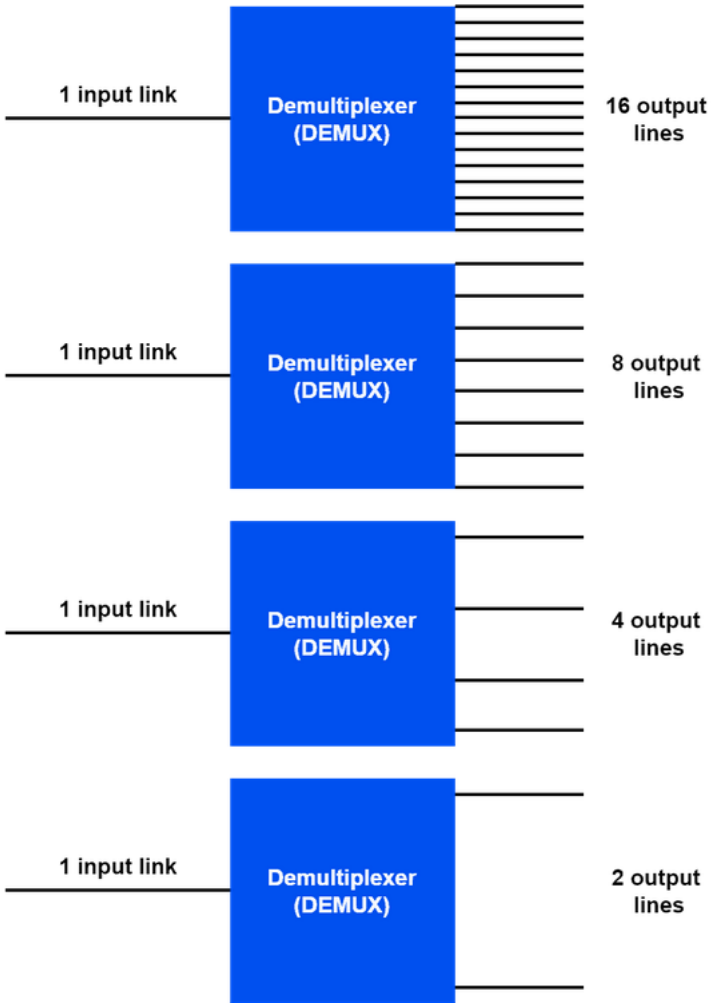
Demultiplexing is the reverse process of multiplexing. It involves extracting and separating the individual data streams from the combined signal received at the destination.



How Demultiplexing Works

Demultiplexing involves the following steps:

1. **Receiving Combined Signal**: The combined signal, which includes data from multiple sources, is received.
2. **Separation of Data Streams**: The combined signal is analyzed and separated into individual data streams based on the multiplexing technique used.
3. **Delivery to Applications**: The separated data streams are directed to their respective applications or processes.



Importance of Demultiplexing

Demultiplexing is essential for ensuring that data reaches the correct application or user:

- **Accurate Data Delivery**: Ensures that each data stream is delivered to the intended recipient without errors.
- **Efficient Network Utilization**: Works in conjunction with multiplexing to maximize the efficiency of the network.
- **Support for Multiple Applications**: Enables the simultaneous support of multiple applications over the same network connection.

Challenges in Demultiplexing

While demultiplexing is crucial, it also presents several challenges:

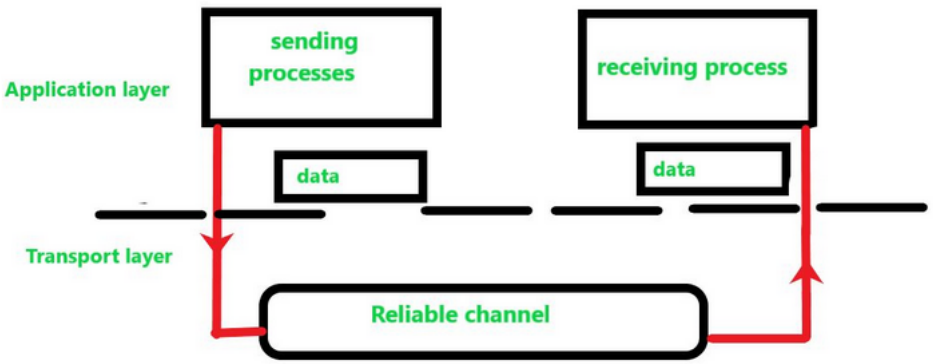
- **Synchronization**: Ensuring that the data streams are synchronized correctly, especially in TDM systems where timing is critical.
- **Interference**: In FDM and WDM systems, ensuring that there is no interference between the different frequency bands or wavelengths.
- **Complexity**: The more sophisticated the multiplexing technique, the more complex the demultiplexing process.

Advantages	Disadvantages
Allows data streams to be separated and sent to their respective destinations, ensuring data isolation	Can limit the scalability of a system. Hence, adding or removing data streams may require significant changes to the system
Reduces the likelihood of errors occurring	Equipment can be costly, particularly during data transmission
Allows a system to be easily scaled up or down, as new data streams can be added or removed from the system without affecting the existing data streams	May not provide sufficient security for all data streams. Therefore, different data streams may require different security protocols
Allows different security protocols to be applied to different data streams, enhancing the overall security of the system for systems with large numbers of data streams	Provides limited scalability and complex to implement

Table 2.2: Advantages and Disadvantages of Multiplexing

2.3 Reliable Data Transfer

Reliable data transfer is a crucial aspect of communication in computer networks, ensuring that data sent from a source to a destination is delivered accurately and in the correct order. Various protocols and mechanisms are employed to achieve this reliability, addressing issues such as data corruption, packet loss, and out-of-order delivery.



2.3.1 Mechanisms for Reliable Data Transfer

- **Error Detection and Correction**: Mechanisms such as checksums, cyclic redundancy checks (CRC), and forward error correction (FEC) are used to detect and correct errors that occur during data transmission.
- **Acknowledgments (ACKs)**: The receiver sends an acknowledgment to the sender upon successfully receiving a data packet. This helps the sender confirm that the packet was received correctly.

- **Retransmission**: If the sender does not receive an acknowledgment within a certain timeframe (timeout), it assumes that the packet was lost or corrupted and retransmits it.
- **Sequence Numbers**: Each packet is assigned a unique sequence number, which allows the receiver to reorder packets that arrive out of order and detect missing packets.
- **Flow Control**: Flow control mechanisms, such as sliding window protocols, manage the rate of data transmission to prevent overwhelming the receiver and ensure efficient use of network resources.
- **Congestion Control**: Congestion control algorithms adjust the rate of data transmission based on network congestion levels to avoid packet loss and ensure smooth data flow.

2.3.2 Protocols for Reliable Data Transfer

- **Transmission Control Protocol (TCP)**: TCP is a widely-used transport layer protocol that provides reliable, connection-oriented data transfer. It uses sequence numbers, acknowledgments, and retransmission mechanisms to ensure data integrity and order.
- **Selective Repeat and Go-Back-N ARQ**: These are specific types of sliding window protocols that enhance reliability by managing the retransmission of erroneous or lost packets.

2.4 Transport Layer Protocols (TLP)

Transport Layer Protocols (TLP) are a crucial component of the OSI (Open Systems Interconnection) model, responsible for facilitating communication between applications running on different hosts. They ensure the reliable transmission of data across networks and provide various services such as error detection, flow control, and multiplexing.

2.4.1 Types of Transport Layer Protocols

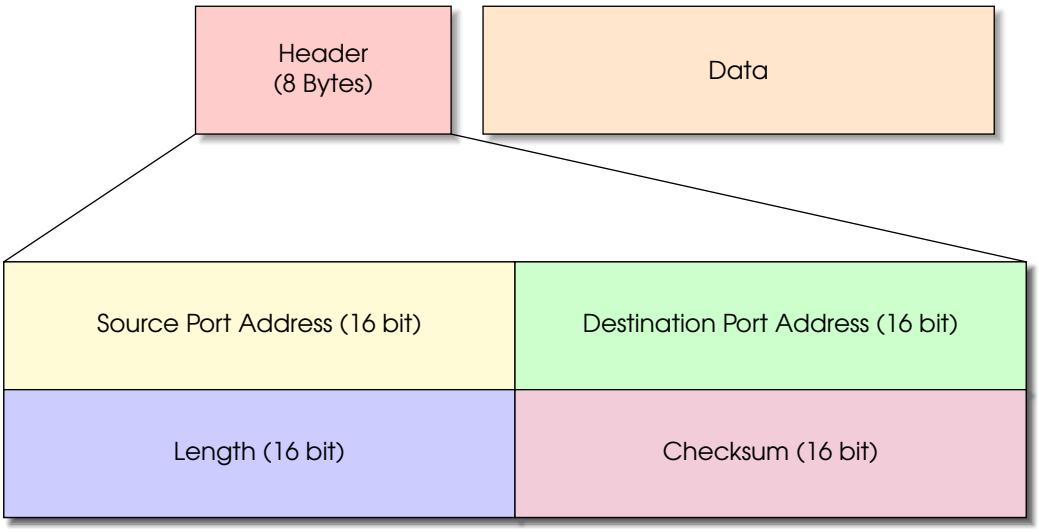
1. **User Datagram Protocol (UDP):**
   - UDP is a connectionless protocol that provides a simple and lightweight communication mechanism.
   - Unlike TCP, UDP does not guarantee packet delivery or order, making it suitable for applications where speed and low latency are more important than reliability.
   - UDP is commonly used for real-time applications like video streaming, online gaming, and VoIP (Voice over Internet Protocol).
2. **Transmission Control Protocol (TCP):**
   - TCP is a connection-oriented protocol that offers reliable, ordered delivery of data packets between communicating hosts.
   - It ensures data integrity through features like acknowledgment of received packets, retransmission of lost packets, and sequencing of data.
   - TCP is widely used for applications where data integrity and reliability are paramount, such as web browsing, email transfer (SMTP), and file transfer (FTP).

2.5 User Datagram Protocol (UDP)

UDP is a connectionless protocol that provides a simpler but less reliable form of data transmission. It is suitable for applications that require fast, efficient transmission, such as streaming and gaming.

2.5.1 UDP Segment Structure

A UDP segment consists of a header and data. The header contains the following fields:



- **Source Port (16 bits)**: Identifies the port number of the application that is sending the data segment.
- **Destination Port (16 bits)**: Identifies the port number of the application that is receiving the data segment.
- **Length (16 bits)**: Specifies the length of the UDP segment, including the header and data.
- **Checksum (16 bits)**: Used for error-checking the header and data. It is optional in IPv4 but mandatory in IPv6.

2.5.2 Uses of UDP

UDP is suitable for applications that require low latency and can tolerate some data loss. Examples include:

- **Online Gaming**: Low-latency and real-time communication.
- **Streaming Media**: Real-time audio and video transmission.
- **Voice over IP (VoIP)**: Real-time voice communication.

2.5.3 Advantages and Disadvantages of UDP

Advantages

- **Speed**: Faster due to low overhead and no connection establishment.
- **Simplicity**: Easier to implement and manage.
- **Broadcast Support**: Can broadcast to multiple recipients.
- **Low Latency**: Suitable for time-sensitive applications.

Disadvantages

- **No Reliability**: No guarantee of data delivery or order.
- **No Congestion Control**: Can cause network congestion.
- **No Flow Control**: No mechanism to prevent sender from overwhelming the receiver.
- **Vulnerability to Attacks**: Susceptible to packet spoofing and other attacks.

2.6 Transmission Control Protocol (TCP)

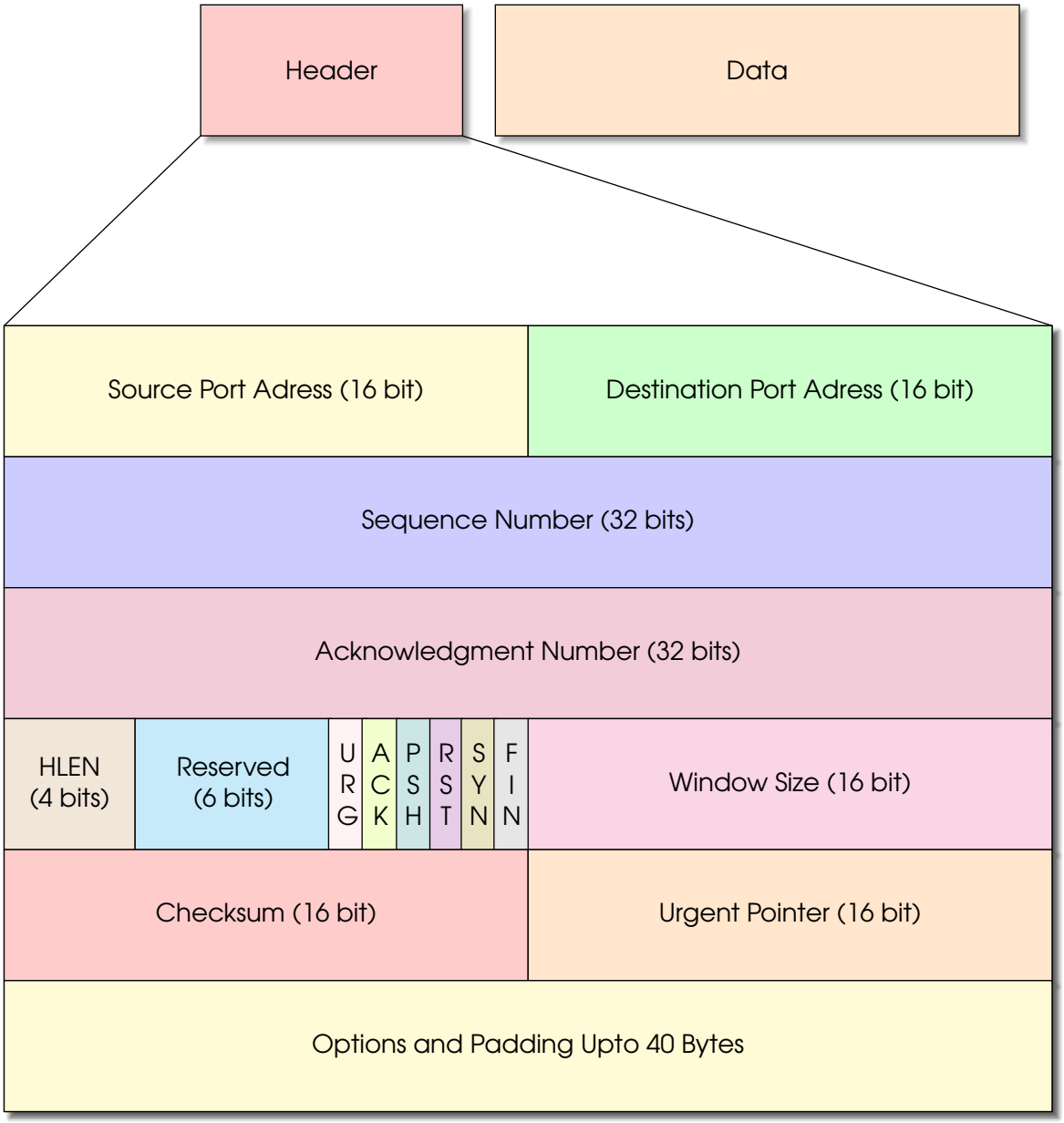
TCP is a connection-oriented protocol that provides reliable communication. It ensures that data is delivered accurately and in the correct order. Below are the main features and components of TCP:

2.6.1 Features of TCP

- **Connection-oriented**: TCP establishes a connection before transmitting data.
- **Reliable**: Ensures that data reaches its destination without errors, duplication, or loss.
- **Flow Control**: Manages the rate of data transmission between sender and receiver to prevent overwhelming the receiver.
- **Congestion Control**: Reduces the rate of data transmission when network congestion is detected.
- **Error Detection and Correction**: Uses checksums for error detection and retransmits lost or corrupted data.

2.6.2 TCP Segment Structure

A TCP segment consists of a header and data. The header contains important information for managing the communication process.



- **Source Port (16 bits)**: Identifies the port number of the application that is sending the data segment. It helps the receiving end know which application sent the data.
- **Destination Port (16 bits)**: Identifies the port number of the application that is receiving the data segment. It directs the data to the correct application on the receiving side.
- **Sequence Number (32 bits)**: This field contains the sequence number of the first byte of data in this segment. It is crucial for ensuring data is delivered in the correct order, allowing the receiver to reassemble the data stream accurately.
- **Acknowledgment Number (32 bits)**: If the ACK flag is set, this field contains the value of the next sequence number that the sender of the segment is expecting to receive. It is used to confirm receipt of data and to acknowledge the bytes received successfully.
- **HLEN (4 bits)**: Specifies the size of the TCP header in 32-bit words. It indicates where the data payload begins. This field allows the receiver to identify the start of the actual data.
- **Reserved (6 bits)**: Reserved for future use and should be set to zero. This field is intended to accommodate future enhancements to the protocol.
- **Control Flags (6 bits)**: These flags control various aspects of the TCP connection, and they can be set individually or in combination. The primary flags include:
  - **URG**: Urgent Pointer field significant.
    - **Purpose**: Indicates that the data in this segment should be processed immediately as it is urgent.
    - **Use Case**: When a higher priority needs to be given to certain data within a segment, such as interrupt signals in a remote login session.
    - **Details**: The Urgent Pointer field specifies an offset from the sequence number, indicating the last byte of urgent data.
  - **ACK**: Acknowledgment field significant.
    - **Purpose**: Indicates that the Acknowledgment field contains a valid acknowledgment number.
    - **Use Case**: Essential for confirming receipt of data, especially in establishing and maintaining the connection.
    - **Details**: Every segment after the initial SYN must have this flag set. It acknowledges receipt of data by specifying the next sequence number expected.
  - **PSH**: Push function.
    - **Purpose**: Requests that the receiving TCP layer pass the data to the application immediately.
    - **Use Case**: Used when data needs to be transmitted and processed quickly, such as in real-time applications.
    - **Details**: It forces the data to be sent immediately rather than waiting for a buffer to fill up.
  - **RST**: Reset the connection.
    - **Purpose**: Resets the connection.
    - **Use Case**: Used to abort a connection due to an error or when an unresponsive connection is detected.
    - **Details**: It effectively terminates the connection and informs the peer that something went wrong.
  - **SYN**: Synchronize sequence numbers.
    - **Purpose**: Synchronizes sequence numbers to establish a connection.
    - **Use Case**: Used during the initial handshake process (SYN, SYN-ACK, ACK).

        - **Details**: The first segment in the three-way handshake has this flag set. It helps synchronize the sequence numbers between the sender and receiver.
    - **FIN**: No more data from the sender.
        - **Purpose**: Indicates that the sender has finished sending data.
        - **Use Case**: Used during the termination phase of a connection.
        - **Details**: The FIN flag is set to signal the end of data transmission. The receiving side acknowledges this with an ACK and can also send a FIN to terminate the connection from its side.
- **Window Size (16 bits)**: Specifies the number of bytes that the sender is willing to receive. It is used for flow control to prevent the sender from overwhelming the receiver with too much data at once.
- **Checksum (16 bits)**: Used for error-checking the header and data. It helps ensure the integrity of the data by allowing the receiver to verify that the segment has not been corrupted during transmission.
- **Urgent Pointer (16 bits)**: If the URG flag is set, this field indicates the offset from the sequence number to the last urgent data byte. It helps prioritize urgent data in the stream.
- **Options (variable)**: Optional parameters, such as maximum segment size. These options provide additional capabilities and optimizations for the TCP connection.

2.7 TCP Connection Management

TCP (Transmission Control Protocol) employs a set of procedures for managing connections between hosts. These procedures ensure reliable and orderly communication. The key aspects of TCP connection management include:

2.7.1 Three-Way Handshake

TCP uses a three-way handshake process to establish a connection:

1. **SYN (Synchronize):** The sender initiates the connection by sending a SYN segment to the receiver, indicating its desire to establish a connection.
2. **SYN-ACK (Synchronize-Acknowledgment):** Upon receiving the SYN segment, the receiver responds with a SYN-ACK segment, acknowledging the sender's request and indicating its readiness to establish a connection.
3. **ACK (Acknowledgment):** Finally, the sender acknowledges the receiver's response with an ACK segment, completing the connection establishment process.

2.7.2 Connection State Management

TCP maintains various connection states to manage the connection lifecycle:

- **Established:** Data transfer occurs between the sender and receiver.
- **Fin-Wait:** The sender has sent a FIN (finish) segment to the receiver, indicating its intention to terminate the connection.
- **Time-Wait:** Both sender and receiver have sent FIN segments, and they wait for any remaining packets to arrive before fully closing the connection.

2.7.3 Graceful Connection Termination

TCP ensures a graceful shutdown process when terminating connections to prevent data loss and ensure orderly termination. This involves both parties exchanging FIN segments and waiting in the TIME-WAIT state to ensure all data is properly transmitted before fully closing the connection.

2.8 Sliding Window Protocol

The sliding window protocol is a method used for controlling the flow of data between two devices in a network. It ensures efficient, reliable, and orderly delivery of data frames. The primary goal is to manage the amount of data that can be sent without receiving an acknowledgment, thus enhancing the performance of the network communication.

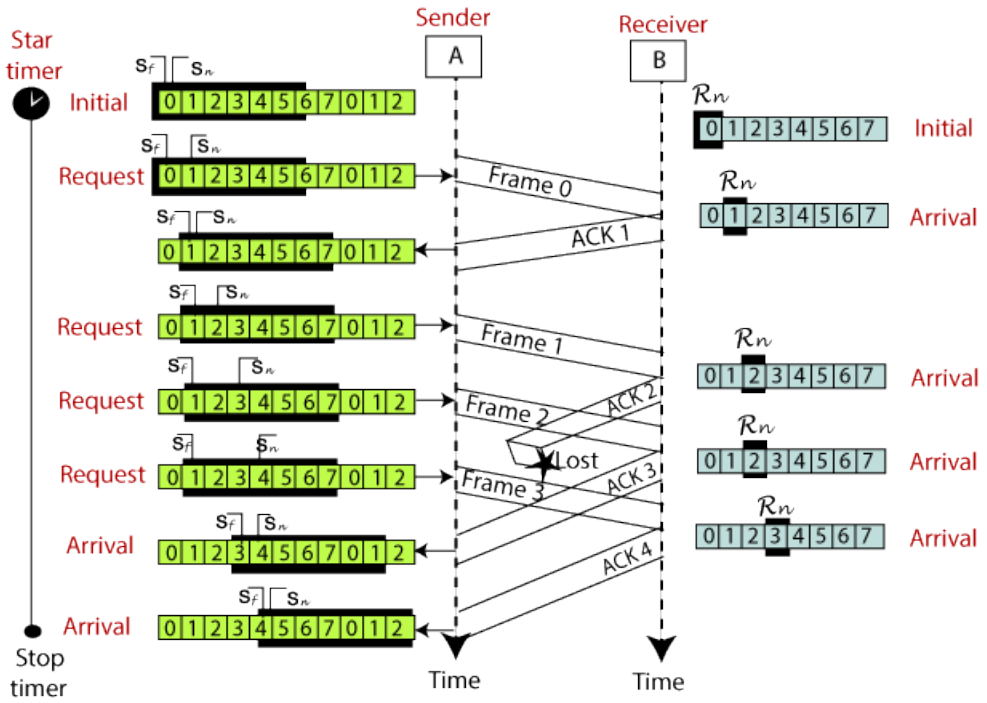
2.8.1 Overview

The sliding window protocol allows the sender to send multiple frames before needing an acknowledgment for the first frame. It uses a window that slides over the data frames to keep track of sent and acknowledged frames. This window mechanism helps to control the flow of data, ensuring that the sender does not overwhelm the receiver.

2.8.2 Types of Sliding Window Protocols

There are two main types of sliding window protocols: Go-Back-N ARQ and Selective Repeat ARQ.

Go-Back-N ARQ



- The sender can send several frames specified by a window size, without waiting for an acknowledgment for each individual frame.
- If an error is detected in a frame (either due to corruption or loss), all subsequent frames are retransmitted from the erroneous frame onwards.
- This method is suitable for environments with fewer errors and requires a simpler implementation on the receiver's end.
- **Example:** If the sender has a window size of 5 and sends frames 1 to 5, and frame 3 is lost, the sender will go back and retransmit frames 3, 4, and 5 after detecting the loss.

Selective Repeat ARQ

- The sender retransmits only the frames that were received in error, rather than all frames after an error, as in Go-Back-N.
- This requires more complex logic on the receiver to handle frames that may arrive out of order.
- It provides a more efficient use of bandwidth, especially in environments where errors are frequent, as only erroneous frames are retransmitted.
- **Example:** If frames 1, 2, 4, and 5 are received correctly, but frame 3 is lost, the sender will only retransmit frame 3.

2.8.3 Sliding Window Mechanism

This involves both the sender and receiver maintaining a window that represents the range of frames that can be sent or received without needing immediate acknowledgment. The size of this window can significantly affect the performance and efficiency of data transmission.

Sender's Window

- The sender's window size determines how many frames can be sent before the sender must wait for an acknowledgment.
- As acknowledgments are received, the window slides forward, allowing the sender to transmit additional frames.
- **Example:** If the sender's window size is 4, the sender can send frames 0, 1, 2, and 3. Upon receiving an acknowledgment for frame 0, the window slides to allow sending frame 4.

Receiver's Window

- The receiver's window size determines how many frames can be received and buffered before an acknowledgment must be sent.
- The receiver's window also slides forward as frames are processed and acknowledged.
- **Example:** If the receiver's window size is 4, the receiver can buffer frames 0 to 3. If frame 0 is processed and acknowledged, the window slides to allow buffering of frame 4.

2.8.4 Sliding Window Protocol Example

- **Sender's Window**:
  - Assume the window size is 4.
  - The sender can send frames 0, 1, 2, and 3.
  - After sending frame 3, the sender must wait for an acknowledgment for frame 0 before sending frame 4.
- **Receiver's Window**:
  - The receiver can receive and buffer frames 0 to 3.
  - If frame 0 is received correctly, it is acknowledged, and the receiver's window slides to allow the reception of frames 4, 5, 6, and 7.
- **Handling Errors**:
  - If frame 1 is lost during transmission, the receiver only acknowledges frame 0.
  - **Go-Back-N ARQ**: The sender will retransmit frames 1, 2, and 3 upon detecting the loss of frame 1.
  - **Selective Repeat ARQ**: The sender will retransmit only frame 1, since frames 2 and 3 were received correctly.

2.8.5 Advantages and Disadvantages

Go-Back-N ARQ

- **Advantages**:

  - Simpler to implement compared to Selective Repeat ARQ.
  - Lower computational requirements on the receiver's end.
- **Disadvantages**:
  - Inefficient in terms of bandwidth usage, especially in error-prone environments, as it retransmits multiple frames even if only one frame is lost.

Selective Repeat ARQ

- **Advantages**:
  - More efficient in terms of bandwidth, as only erroneous frames are retransmitted.
  - Better performance in environments with higher error rates.
- **Disadvantages**:
  - More complex to implement due to the need for maintaining a buffer and handling out-of-order frames.
  - Higher computational and memory requirements on the receiver's end.

Go-Back-N ARQ	Selective Repeat ARQ
If a frame is corrupted or lost, all subsequent frames have to be sent again.	Only the corrupted or lost frame is sent again.
If there is a high error rate, it wastes a lot of bandwidth.	There is low bandwidth loss.
It is less complex.	It is more complex because it requires sorting and searching, and also requires more storage.
It does not require sorting.	Sorting is done to get the frames in the correct order.
It does not require searching.	The search operation is performed.
It is used more.	It is used less because it is more complex.

Table 2.3: Comparison of Go-Back-N ARQ and Selective Repeat ARQ

2.9 Congestion Control

Congestion control is a fundamental aspect of network management aimed at regulating the flow of data to prevent network congestion and maintain optimal performance. It involves the implementation of various mechanisms and algorithms to manage traffic and resource allocation in computer networks.

2.9.1 Causes of Congestion Control

Congestion in computer networks can arise due to various factors, including:

- **High Traffic Volume**: When the volume of data being transmitted exceeds the capacity of the network infrastructure, leading to congestion.

- **Limited Network Resources**: Insufficient bandwidth, processing power, or memory can result in congestion, as the network struggles to handle the amount of traffic.
- **Packet Loss**: Occurs when packets are dropped or discarded during transmission due to network congestion, errors, or faulty equipment. Packet loss exacerbates congestion by requiring retransmission, further clogging the network.
- **Bottlenecks**: Points in the network topology where the flow of traffic is constricted or slowed down, often due to a mismatch in bandwidth capacities between network components. Bottlenecks can occur at routers, switches, or other network devices, leading to localized congestion.

Understanding these causes is crucial for implementing effective congestion control strategies in computer networks.

2.9.2 Approaches to Congestion Control

There are several approaches to managing congestion in computer networks, each with its own advantages and disadvantages:

- **Traffic Shaping**: Traffic shaping regulates the flow of data to prevent congestion by controlling the rate at which packets are transmitted. This approach prioritizes certain types of traffic while limiting others, ensuring that network resources are allocated efficiently.
- **Prioritization**: Prioritization assigns different priority levels to packets based on their importance or type. Critical data, such as real-time video or voice traffic, may be given higher priority to ensure timely delivery, while non-essential traffic is deprioritized.
- **Admission Control**: Admission control limits the number of new connections or sessions that can be established in the network, preventing overload and ensuring that existing connections receive adequate resources. This approach helps maintain quality of service by avoiding congestion-induced performance degradation.
- **Congestion Avoidance Algorithms**: Congestion avoidance algorithms dynamically adjust transmission rates based on network conditions to prevent congestion before it occurs. These algorithms monitor network congestion signals, such as packet loss or delay, and adapt the transmission rate accordingly to maintain optimal performance.

By employing these approaches, network administrators can effectively manage congestion and maintain high-quality communication services.

2.9.3 TCP Congestion Control

TCP (Transmission Control Protocol) implements sophisticated congestion control mechanisms to ensure reliable and efficient data transmission over congested networks. Some key algorithms include:

- **Slow Start**: Slow start is an algorithm used by TCP to gradually increase the transmission rate of data until congestion is detected. It begins by sending a small number of packets and doubles the transmission rate for each successful acknowledgment, rapidly ramping up the throughput until congestion occurs.
- **Congestion Avoidance**: Congestion avoidance adjusts the transmission rate based on the perceived level of network congestion. TCP monitors congestion signals, such as packet loss or delay, and dynamically adjusts the transmission rate to prevent overloading the network. This algorithm aims to maintain optimal performance while avoiding congestion-induced packet loss.
- **Fast Retransmit**: Fast retransmit is a mechanism used by TCP to quickly retransmit lost packets without waiting for a timeout. When TCP receives multiple duplicate acknowledgments for the same packet, it infers that the packet was lost and immediately retransmits it, speeding up the recovery process and reducing latency.

- **Fast Recovery**: Fast recovery complements fast retransmit by resuming transmission after packet loss without waiting for a timeout. TCP enters the fast recovery state upon detecting multiple duplicate acknowledgments, allowing it to continue sending new data while waiting for the retransmitted packet to be acknowledged. This approach minimizes the impact of packet loss on TCP performance and improves throughput.

These congestion control mechanisms play a vital role in ensuring the stability, efficiency, and fairness of TCP-based communication in modern computer networks.

Unit III

3. Network Layer: Forwarding & Routing

3.1 Network Layer

The Network Layer is responsible for transferring network packets from the source to the destination. It operates at both the source and destination hosts. At the source, it accepts packets from the transport layer, encapsulates them in datagrams, and delivers them to the data link layer for transmission. At the destination, it decapsulates the datagrams to extract the packets and delivers them to the transport layer.

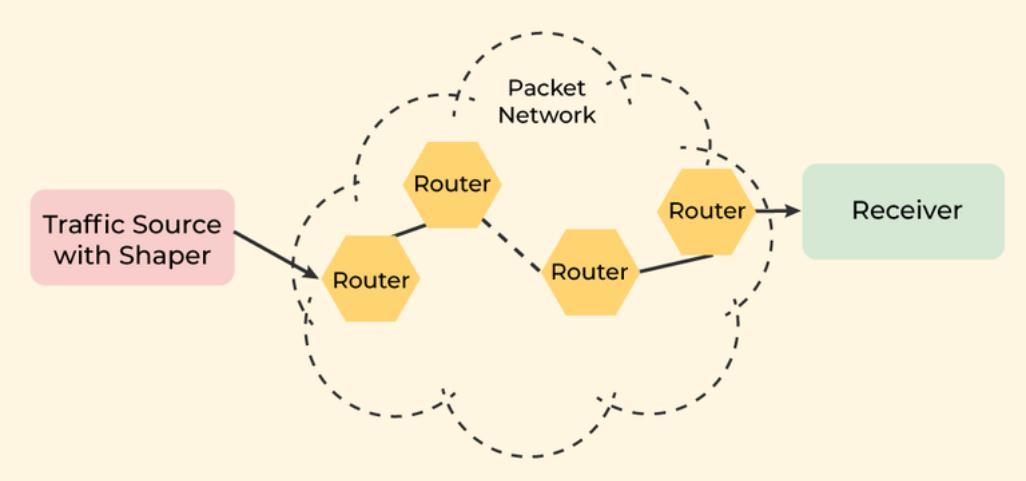
3.1.1 Features of the Network Layer

1. **Data Transfer**: The Network Layer ensures that data packets are transferred from the source to the destination without altering the data.
2. **Fragmentation**: If packets are too large for transmission, the Network Layer fragments them into smaller packets.
3. **Routing**: It determines the optimal path for data packets to travel from the source to the destination among multiple routes available in the network.
4. **Addressing**: The Network Layer adds source and destination addresses to data packets, ensuring they reach the correct endpoint.

3.1.2 Services Offered by the Network Layer

The Network Layer provides several key services:

1. **Packetizing**: This involves encapsulating data received from upper layers into network layer packets (datagrams) at the source. The source host adds a header, including source and destination addresses, to the payload and sends the packet to the data link layer. At the destination, the datagram is decapsulated to retrieve the payload, which is then delivered to the appropriate upper layer protocol.



2. **Forwarding**: Forwarding refers to the process routers use to send incoming packets to the appropriate next hop toward their destination. When a router receives a packet, it forwards it to the next network or router based on its routing table.
3. **Routing**: Routing involves determining the best path for packets to take from the source to the destination. Routers use routing algorithms to decide the optimal path for packet delivery.
4. **Logical Addressing**: Unlike physical addresses used by the data link layer, logical addresses (IP addresses) are used by the Network Layer to uniquely identify source and destination systems across different networks. The network layer adds these logical addresses to the packet headers.
5. **Internetworking**: The Network Layer provides a logical connection between different types of networks, enabling them to communicate with each other effectively.

3.2 Network Service Model

The network service model defines how data is transferred across the network. It determines the methods and protocols used to ensure data is delivered efficiently and reliably. There are two main types of service models:

3.2.1 Connection-Oriented Service

A connection-oriented service requires a connection to be established between the source and destination before any data is transferred. This type of service is characterized by the following features:

- **Establishment Phase:** A connection setup phase is needed before any data transfer can occur. This phase involves handshaking between the source and the destination to establish a dedicated path for communication.
- **Reliable Delivery:** Once the connection is established, the data is transferred reliably. The network ensures that all packets are delivered in the correct order and without any loss.
- **Sequenced Delivery:** Packets are delivered in the same order in which they were sent, ensuring data integrity and correctness.
- **Flow Control and Error Control:** Mechanisms are in place to manage the rate of data transfer and to detect and correct errors that may occur during transmission.
- **Example:** Transmission Control Protocol (TCP) is a common example of a connection-oriented service. TCP ensures reliable and sequenced delivery of data over the internet by

establishing a connection before data transfer and using acknowledgments and retransmissions.

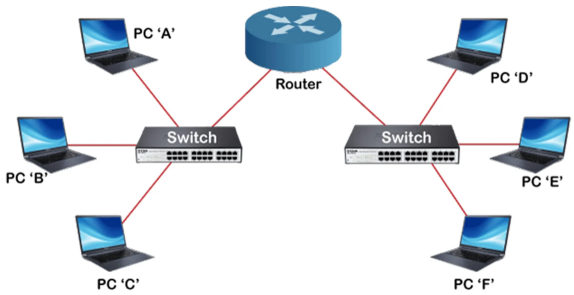
3.2.2 Connectionless Service

In a connectionless service, data is sent without establishing a prior connection between the source and the destination. Each data packet is treated independently and may take different paths to reach the destination. This type of service is characterized by the following features:

- **No Setup Phase:** There is no need for a connection setup phase. Data can be sent immediately without any preliminary handshaking.
- **Independent Packets:** Each packet, often referred to as a datagram, is treated independently. There is no inherent guarantee that packets will be delivered in order, or even that they will be delivered at all.
- **Best-Effort Delivery:** The network makes a best-effort attempt to deliver packets but does not guarantee delivery, order, or data integrity. This model is simpler and has less overhead compared to connection-oriented services.
- **No Flow Control or Error Control:** The network does not manage the rate of data transfer, and there are no mechanisms to detect or correct errors in the data packets.
- **Example:** The Internet Protocol (IP) is an example of a connectionless service. IP routes each datagram independently based on the destination address in the packet header, without establishing a connection or ensuring packet order and reliability.

3.3 Routers

A router is a critical networking device that serves as a gateway, passing data between one or more local area networks (LANs). Routers use the Internet Protocol (IP) to send IP packets containing data and the IP addresses of sending and destination devices located on separate networks. Operating at the network layer (Layer 3) of the OSI model, routers play a vital role in the functioning of both local and wide area networks.



3.3.1 Functions of Routers

Routers are responsible for several key functions within a network:

- **Data Packet Forwarding:** Routers receive data packets from one network, analyze the destination address, and forward the packets to the appropriate network. This process involves determining the optimal path for the packet to reach its destination.
- **Network Interconnection:** Routers connect different networks together, enabling communication between devices on separate networks. This allows for the creation of larger and more complex network architectures.

- **Routing Table Management:** Routers maintain a routing table that contains information about network paths and the best routes to various destinations. This table is regularly updated to reflect changes in the network topology.
- **Path Determination:** Using routing algorithms and protocols, routers determine the most efficient path for data packets to travel from the source to the destination. This ensures optimal use of network resources and reduces latency.

3.3.2 Features of Routers

Routers have several important features that distinguish them from other networking devices such as hubs, bridges, and switches:

- **Layer 3 Device:** Routers operate at the network layer (Layer 3) of the OSI model. This allows them to understand and process IP addresses, making intelligent forwarding decisions based on the network layer information.
- **Network Connectivity:** Routers connect multiple networks together, enabling communication between devices on different networks. This is essential for creating large-scale network infrastructures such as the internet.
- **IP Packet Handling:** Routers transfer data in the form of IP packets. They use the destination IP address specified in each packet to determine the best route for delivery.
- **Routing Tables:** Each router maintains a routing table that is periodically updated based on the changes in the network. The routing table contains information about the network topology and the routes to various destinations.
- **Routing Protocols:** Routers use routing protocols to communicate with other routers and update their routing tables. Common routing protocols include OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol).
- **Cost and Complexity:** Routers are generally more expensive and complex than other networking devices such as hubs, bridges, and switches. This is due to their advanced functionality and the critical role they play in managing and directing network traffic.

3.3.3 Types of Routers

There are different types of routers designed for various network environments and requirements:

- **Home Routers:** Used in residential settings to connect home networks to the internet. They typically offer basic routing functions and wireless connectivity.
- **Enterprise Routers:** Designed for large organizations, these routers handle higher data volumes and provide advanced features such as enhanced security, load balancing, and support for multiple routing protocols.
- **Core Routers:** Operate within the core of large networks, such as the internet backbone. They manage high-speed data transfers and connect large-scale networks.
- **Edge Routers:** Positioned at the edge of networks, these routers connect internal networks to external networks, such as connecting a corporate LAN to the internet.

Routers are essential for efficient and reliable network communication, ensuring that data packets reach their intended destinations through the most efficient routes possible.

3.4 Internet Protocol (IP)

The Internet Protocol (IP) is a fundamental component of the Internet protocol suite, responsible for delivering packets from the source host to the destination host. Each packet, known as a datagram, is treated independently, and routers use the destination IP address in the packet header to determine

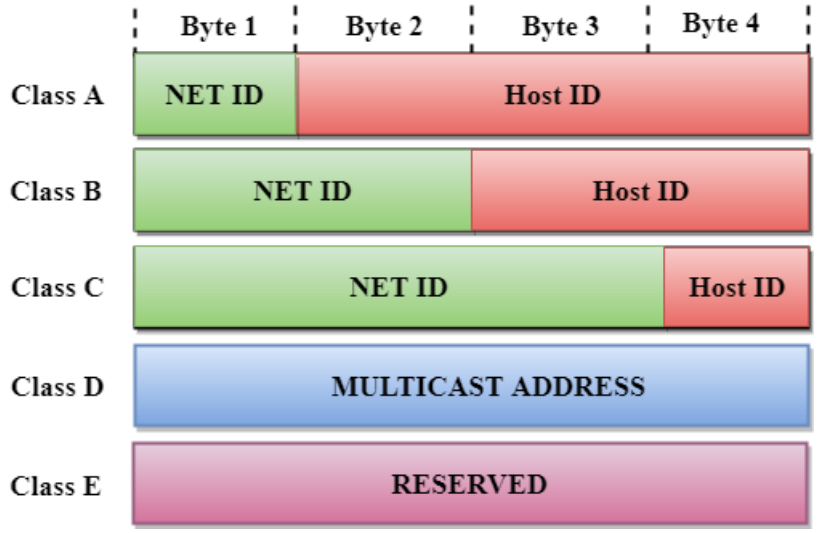
the best path for forwarding. IP's primary function is routing, which enables internetworking and essentially establishes the Internet.

3.5 Classful Addressing

Classful addressing is an early method used to allocate IP addresses. In this scheme, an IP address is 32 bits long and is divided into five different classes: A, B, C, D, and E. Each class is identified by the leading bits in the address and has specific characteristics regarding the division of the address space.

An IP address is split into two main parts:

- **Network ID**: Identifies the specific network and is used for routing.
- **Host ID**: Identifies a specific device within that network.



Each class has a specific range of IP addresses, determining the number of networks and hosts available within that class.

3.5.1 Class A

Class A addresses are used for very large networks.

- **Network ID**: The first 8 bits.
- **Host ID**: The remaining 24 bits.

In Class A, the first bit is always set to 0, leaving 7 bits for the network ID, which allows for 128 possible networks. Each network can have up to 16,777,214 hosts.

$$\text{Total number of networks in Class A} = 2^7 = 128$$

$$\text{Total number of hosts per network in Class A} = 2^{24} - 2 = 16,777,214$$

The address range for Class A is from 0.0.0.0 to 127.255.255.255, but usable addresses range from 1.0.0.0 to 126.255.255.255 (excluding 127.x.x.x used for loopback testing).

3.5.2 Class B

Class B addresses are assigned to medium to large-sized networks.

- **Network ID**: The first 16 bits.
- **Host ID**: The remaining 16 bits.

In Class B, the first two bits are set to 10, leaving 14 bits for the network ID, which allows for 16,384 possible networks. Each network can have up to 65,534 hosts.

$$\text{Total number of networks in Class B} = 2^{14} = 16,384$$

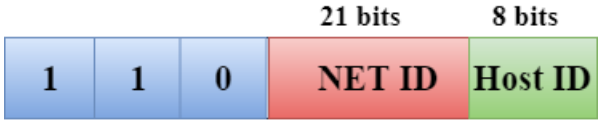
$$\text{Total number of hosts per network in Class B} = 2^{16} - 2 = 65,534$$

The address range for Class B is from 128.0.0.0 to 191.255.255.255.

3.5.3 Class C

Class C addresses are used for small-sized networks.

- **Network ID**: The first 24 bits.
- **Host ID**: The remaining 8 bits.



In Class C, the first three bits are set to 110, leaving 21 bits for the network ID, which allows for 2,097,152 possible networks. Each network can have up to 254 hosts.

$$\text{Total number of networks in Class C} = 2^{21} = 2,097,152$$

$$\text{Total number of hosts per network in Class C} = 2^{8} - 2 = 254$$

The address range for Class C is from 192.0.0.0 to 223.255.255.255.

3.5.4 Class D

Class D addresses are reserved for multicast groups. These addresses are used to send data to multiple destinations simultaneously.

- **Address Range**: The first four bits are set to 1110.

Class D does not follow the traditional network and host ID format and does not support subnetting. The address range for Class D is from 224.0.0.0 to 239.255.255.255.

3.5.5 Class E

Class E addresses are reserved for experimental purposes and future use. These addresses are not intended for general use.

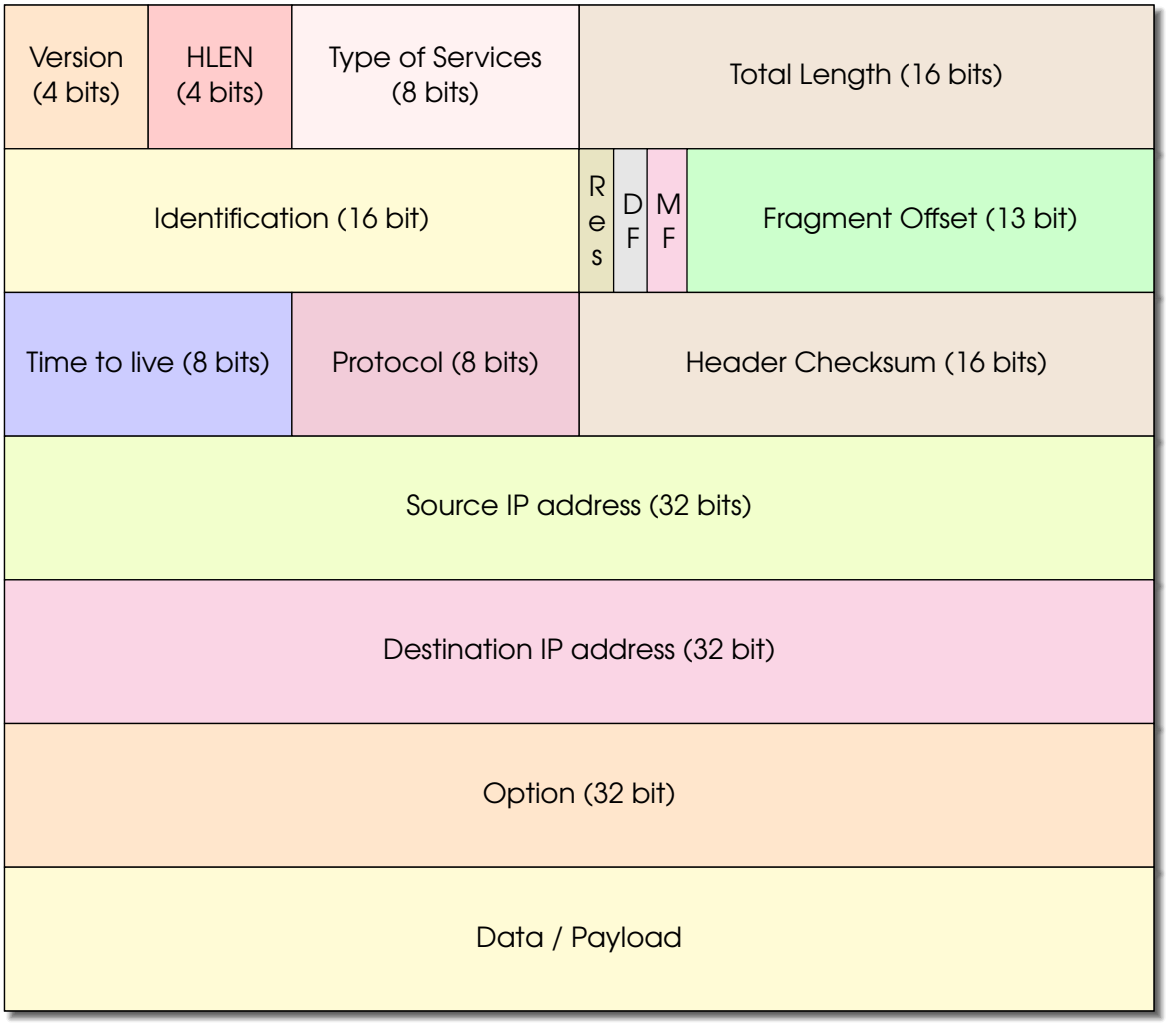
- **Address Range**: The first four bits are set to 1111.

Similar to Class D, Class E does not support subnetting. The address range for Class E is from 240.0.0.0 to 255.255.255.255.

3.6 Datagram Format

A datagram is the basic unit of data transfer in a packet-switched network, such as the Internet. The structure of an IP datagram is divided into two main parts: the header and the payload.

3.6.1 Header



The header contains metadata required for routing and delivery. It consists of several fields, each serving a specific purpose:

- **Version:** (4 bits) Specifies the IP version (e.g., IPv4 or IPv6).
- **Header Length:** (4 bits) Indicates the length of the IP header in 32-bit words.
- **Type of Service (ToS):** (8 bits) Specifies the quality of service and priority of the datagram.
- **Total Length:** (16 bits) The total length of the datagram, including the header and payload, in bytes.
- **Identification:** (16 bits) A unique identifier for the datagram, used for reassembling fragmented packets.
- **Flags:** (3 bits) Controls or identifies fragments. The most significant bit is reserved, the second bit is the "Don't Fragment" (DF) flag, and the third bit is the "More Fragments" (MF) flag.
- **Fragment Offset:** (13 bits) Specifies the position of the fragment in the original datagram.
- **Time to Live (TTL):** (8 bits) Limits the lifetime of the datagram to prevent it from circulating indefinitely. It is decremented by each router it passes through.
- **Protocol:** (8 bits) Indicates the higher-level protocol (e.g., TCP, UDP) used in the payload.
- **Header Checksum:** (16 bits) A checksum on the header to ensure integrity.
- **Source IP Address:** (32 bits) The IP address of the sender.
- **Destination IP Address:** (32 bits) The IP address of the receiver.
- **Options:** (variable length) Optional fields for additional control and routing information.

3.6.2 Payload

The payload contains the actual data being transferred from the source to the destination. This can be any kind of data, such as part of an email, a web page, or a video stream. The size of the payload is determined by subtracting the header length from the total length of the datagram.

The header provides the necessary information for routers and other network devices to forward the datagram to its destination, while the payload contains the end-user data.

3.7 IPv4 Addressing

IPv4 addressing involves the allocation of unique addresses to devices within a network. Key components of IPv4 addressing include:

- **Dynamic Host Configuration Protocol (DHCP):** This protocol automatically assigns IP addresses to devices connected to a network, simplifying network administration and management.
- **Network Address Translation (NAT):** NAT allows multiple devices within a local network to share a single public IP address. It helps conserve IP addresses and enhances security by masking internal IP addresses from external networks.
- **Internet Control Message Protocol (ICMP):** ICMP is used for error messaging and operational inquiries within an IP network. It facilitates communication between network devices for diagnosing network issues and troubleshooting.

3.8 IPv4 Protocol

IPv4 is a connectionless protocol designed for packet-switched networks. It follows a best-effort delivery model, where delivery guarantees, sequencing, and prevention of duplicate delivery are not assured. Internet Protocol Version 4 (IPv4) is the fourth iteration of the Internet Protocol and remains widely used in data communication across various network types. IPv4 establishes a logical connection between network devices by providing unique identification for each device.

3.9 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a network management protocol that automates the assignment of IP addresses to devices within a network, facilitating communication using Internet Protocol (IP). DHCP simplifies network administration by dynamically managing IP configurations, eliminating the need for manual address assignments. Here's a breakdown of DHCP's functionality:

- **Automatic Address Assignment:** DHCP automatically assigns IP addresses to devices connecting to a network, streamlining network configuration without requiring user intervention.
- **Centralized Management:** It centrally manages IP address provisioning for all devices added or removed from the network, enhancing administrative control and reducing configuration overhead.
- **Configuration Management:** DHCP configures essential network parameters such as subnet mask, default gateway, and DNS server addresses on client devices, ensuring seamless connectivity.

3.9.1 How DHCP Works

DHCP operates as a client-server protocol, with DHCP servers managing a pool of available IP addresses and distributing configuration information to DHCP clients. The DHCP lease process involves the following steps:

1. A client device connects to the network and broadcasts a request for an IP address.
2. The DHCP server responds with an IP address and associated configuration details, including lease duration.
3. Upon lease expiration, the client may request a renewal, and the server may assign a new IP address based on administrator-defined policies.

3.9.2 Components of DHCP

Key components of DHCP include:

- **DHCP Server:** Manages IP address allocation and configuration information.
- **DHCP Client:** Receives configuration details from the DHCP server.
- **IP Address Pool:** Range of available IP addresses for assignment.
- **Subnet:** Segmented portion of the IP network.
- **Lease:** Time duration for which a client holds an assigned IP address.
- **DHCP Relay:** Forwards client messages to DHCP servers across networks.

3.9.3 Benefits of DHCP

DHCP offers several benefits:

- **Centralized Administration:** Simplifies IP configuration management through centralized administration.
- **Dynamic Configuration:** Automates host configuration, eliminating manual intervention.
- **Seamless Connectivity:** Ensures accurate and timely IP configuration for devices without user intervention.
- **Flexibility and Scalability:** Facilitates easy adaptation to network changes and scalability.

3.10 Network Address Translation (NAT)

Network Address Translation (NAT) is a mechanism used to enable multiple devices within a private network to access the Internet through a single public IP address. NAT performs translation of IP addresses and port numbers, allowing devices with private IP addresses to communicate over the Internet using a shared public IP address. Here's how NAT works and its various types:

3.10.1 Working of NAT

NAT operates on a border router, translating local (private) IP addresses to global (public) IP addresses when packets leave the local network, and vice versa when packets enter the network. This translation ensures seamless communication between devices within the private network and external hosts on the Internet.

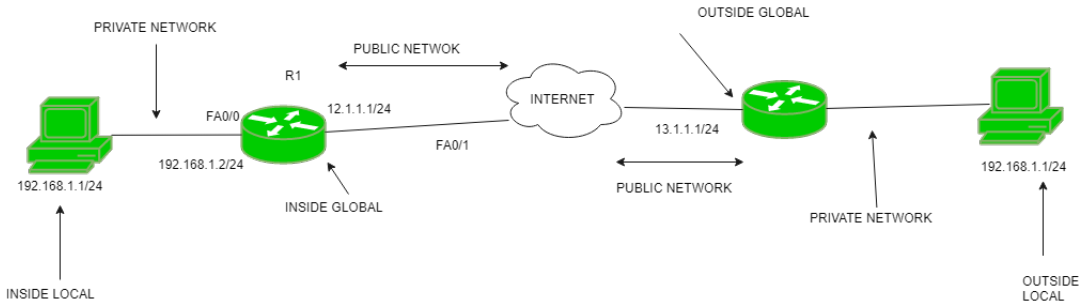
To prevent address exhaustion, NAT dynamically assigns and manages IP addresses from a pool of available addresses. If the pool is exhausted, packets may be dropped, and an ICMP message is sent to the destination.

3.10.2 Port Number Masking

NAT also masks port numbers to differentiate traffic originating from different devices within the private network. By masking port numbers, NAT maintains accurate routing and prevents packet confusion.

3.10.3 NAT Inside and Outside Addresses

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization. These are the network Addresses in which the translation of the addresses will be done.



- **Inside Local Address**: An IP address that is assigned to a host on the inside (local) network. The address is probably not an IP address assigned by the service provider, i.e., these are private IP addresses. This is the inside host seen from the inside network.
- **Inside Global Address**: An IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
- **Outside Local Address**: This is the actual IP address of the destination host in the local network after translation.
- **Outside Global Address**: This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

3.10.4 NAT Address Types

- **Static NAT:** Maps a single private IP address to a public IP address, facilitating one-to-one address translation. Commonly used for web hosting but not suitable for large-scale network deployments due to cost implications.

- **Dynamic NAT:** Translates multiple private IP addresses to a pool of public IP addresses. Only a fixed number of private addresses can be translated to public addresses at a given time, leading to potential packet drops if the pool is exhausted.
- **Port Address Translation (PAT):** Also known as NAT overload, allows multiple private IP addresses to share a single public IP address. Port numbers are used to distinguish traffic, enabling cost-effective Internet connectivity for large user bases.

3.10.5 Advantages of NAT

- **IP Address Conservation:** NAT conserves globally registered IP addresses by allowing multiple devices to share a single public address.
- **Enhanced Privacy:** NAT hides the internal network structure, providing privacy and security for devices within the network.
- **Simplified Network Evolution:** NAT eliminates the need for address renumbering when network configurations change, simplifying network management.

3.10.6 Disadvantages of NAT

- **Increased Latency:** NAT introduces switching delays, impacting network performance.
- **Application Compatibility Issues:** Certain applications may not function correctly with NAT enabled due to address translation.
- **Complexity with Tunneling Protocols:** NAT complicates the implementation of tunneling protocols such as IPsec.
- **Violation of Protocol Layers:** NAT, being a network layer device, interferes with port numbers (transport layer), leading to potential protocol violations.

3.11 Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is a crucial network layer protocol designed for diagnosing communication errors by facilitating error control mechanisms. Unlike IP, which lacks built-in error and control message capabilities, ICMP fills this gap by providing error reporting and management queries.

3.11.1 Uses of ICMP

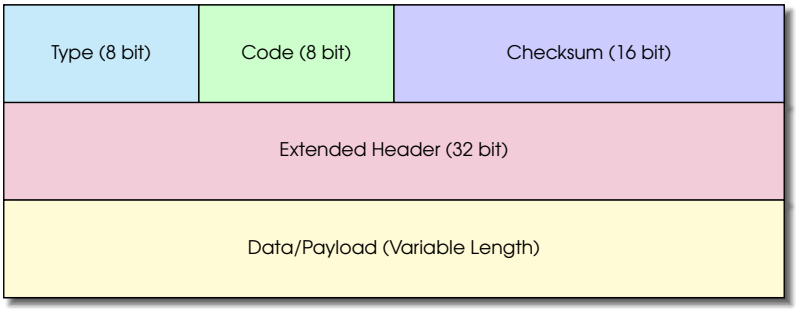
ICMP serves multiple purposes in network communication:

- **Error Reporting:** ICMP is responsible for reporting errors encountered during data transmission. For instance, if a device encounters an unreachable destination or encounters errors processing a packet, ICMP generates error messages to inform the sender.
- **Network Diagnosis:** ICMP utilities such as traceroute and ping aid in network diagnosis. Traceroute maps the route between devices by tracing the path from one router to another, while ping measures the round-trip time for data to reach the destination and return.

3.11.2 How ICMP Works

ICMP operates independently of transport layer protocols like TCP or UDP and does not require a connection to be established before sending messages. It functions as a connectionless protocol, contrasting with connection-oriented protocols like TCP. ICMP packets, transmitted in the form of datagrams, contain an IP header with ICMP data, resembling independent data entities.

3.11.3 ICMP Packet Format



ICMP packets consist of a header followed by data, with the header containing three fields:

- **Type (8-bit):** Specifies the type of message being sent, such as echo request, echo reply, destination unreachable, etc.
- **Code (8-bit):** Provides additional information about the error message type.
- **Checksum (16-bit):** Verifies the integrity of the ICMP packet.

After the header, an extended header points out the problem in the IP message, followed by the payload or data of variable length.

3.11.4 ICMP in DDoS Attacks

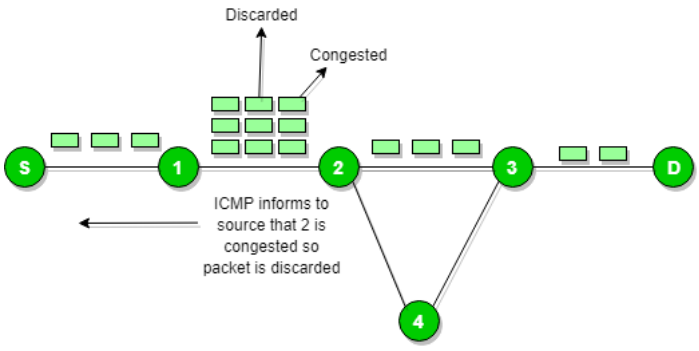
ICMP is also exploited in Distributed Denial of Service (DDoS) attacks:

- **Ping of Death Attack:** Overloading a target with oversized ping packets to trigger buffer overflows and freeze the target machine.
- **ICMP Flood Attack:** Flooding a target with excessive ping requests, overwhelming its resources and causing denial of service.
- **Smurf Attack:** Sending ICMP packets with spoofed source IP addresses to amplify attacks and disrupt network services.

3.12 Types of ICMP Messages

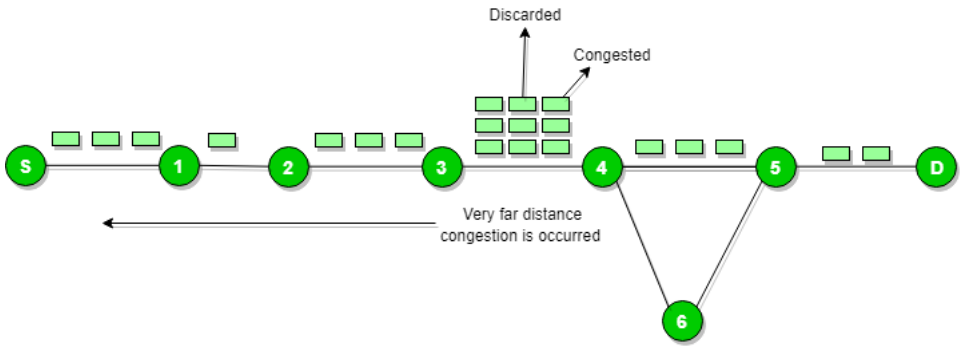
Several types of ICMP messages serve various purposes:

- **Source Quench Message:** Requests a reduction in traffic rate to prevent congestion and packet loss. A source quench message is a request to decrease the traffic rate for messages sent to the host destination. When the receiving host detects that the rate of incoming packets (traffic rate) is too fast, it sends a source quench message to the source to slow down the transmission pace, thereby preventing packet loss.



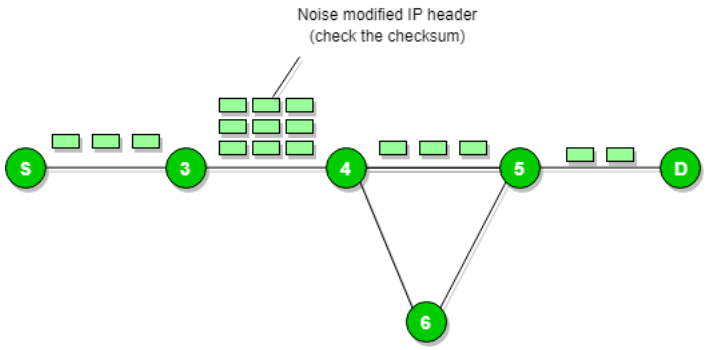
Source Quench Message

ICMP takes the source IP from the discarded packet and informs the source by sending a source quench message. If congestion occurs at a router far away from the source, ICMP sends a hop-by-hop source quench message to every router in the path to reduce the transmission speed.



Source Quench Message with Reduced Speed

- **Parameter Problem:** Indicates issues with packet headers, prompting retransmission requests. Whenever packets arrive at a router, the calculated header checksum should match the received header checksum for the packet to be accepted. If there is a checksum mismatch, the router drops the packet. ICMP takes the source IP from the discarded packet and informs the source by sending a parameter problem message.



Parameter Problem

- **Redirect Message:** Informs hosts about better routes for data transmission. A redirection message requests data packets to be sent on an alternate route. It informs a host to update its routing information to send packets on an alternate route. For example, if a host tries to send data through a router R1, and R1 can send the data through a router R2 with a direct path, R1 will send a redirect message to inform the host about the best route available directly through R2. The host then sends data packets for the destination directly to R2, which forwards the original datagram to the intended destination. However, if the datagram already contains routing information, a redirect message will not be sent, as redirects should only be sent by gateways and not by Internet hosts.

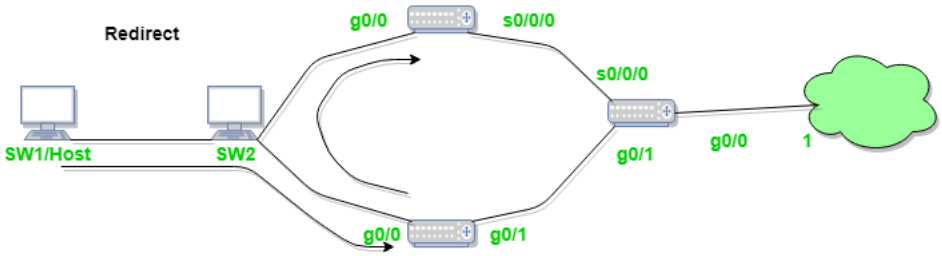
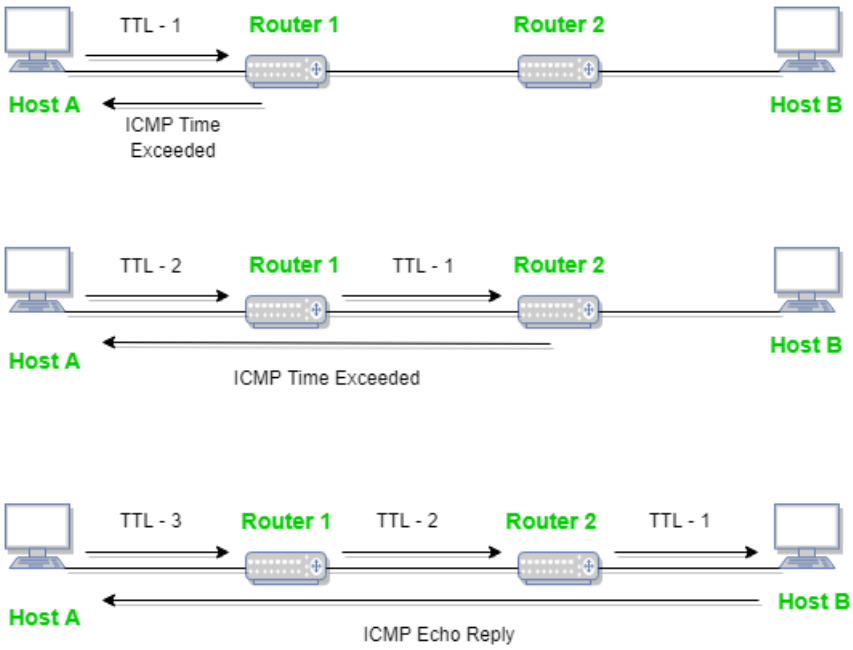


Figure - ICMP redirect Verification CCNP 2.0 100 - 101 (v - 71)

- ICMP Redirect
- ICMP Redirect for host
- ICMP Redirect for network
- How ICMP redirect work
- ICMP Redirect verification step by step

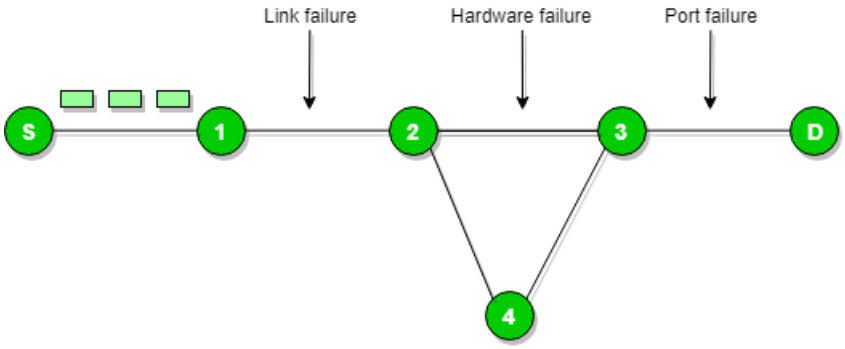
Redirection Message

- **Time Exceeded Message:** Notifies routers or hosts when time limits for packet delivery are exceeded. When some fragments are lost in a network, the router drops the fragments it is holding. ICMP takes the source IP from the discarded packet and informs the source of the discarded datagram due to the Time To Live (TTL) field reaching zero by sending a time exceeded message.



Time Exceeded Message

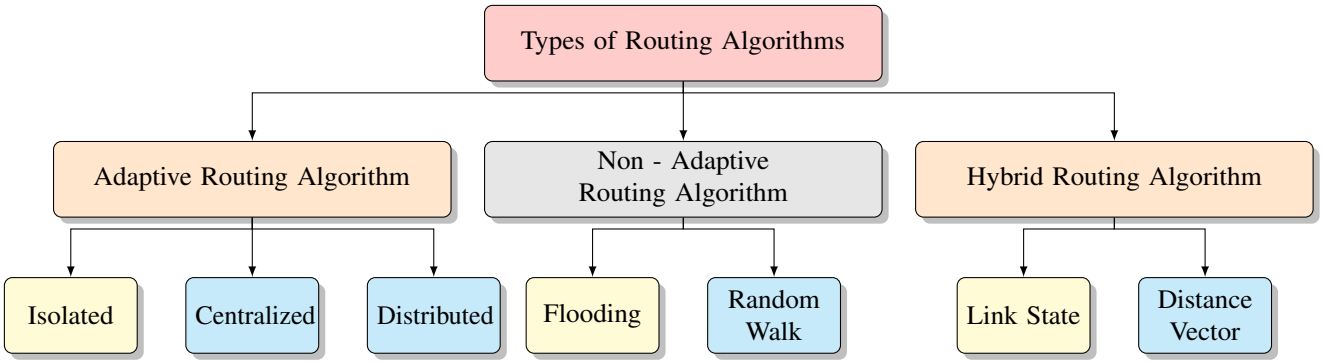
- **Destination Unreachable:** Indicates that the destination is unreachable for some reason. The destination unreachable message is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason. This message can be sent by routers or destination hosts when any type of failure (such as link failure, hardware failure, port failure, etc.) occurs in the network.



Destination Unreachable

3.13 Routing Algorithms

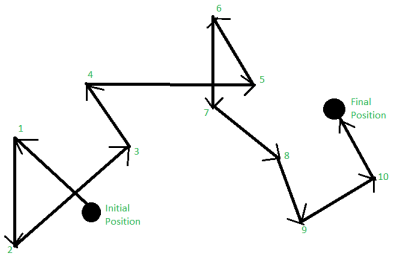
Routing is the backbone of network communication, determining the paths data packets take to reach their destinations efficiently. Let's delve into the classification of routing algorithms and understand their differences.



3.13.1 Classification of Routing Algorithms

Routing algorithms fall into three main categories:

1. **Adaptive Algorithms**: These algorithms dynamically adjust routing decisions based on changes in network topology or traffic load. They use dynamic information like current topology, load, and delay to select routes. Adaptive algorithms can be further categorized into isolated, centralized, or distributed methods.
   - **Isolated**: Each node independently makes routing decisions based on its local information, which can lead to congestion and delay.
   - **Centralized**: A central node holds complete network information and makes all routing decisions, ensuring efficient routing but posing a single point of failure.
   - **Distributed**: Nodes exchange information with neighbors to make routing decisions, allowing for decentralized control but potentially leading to delays in information exchange.
2. **Non-Adaptive Algorithms**: These algorithms maintain fixed routing decisions once established, making them suitable for simpler networks with consistent traffic patterns. They include flooding and random walk methods.
   - **Flooding**: Every incoming packet is sent on every outgoing line except the one it arrived on, potentially causing packet duplication and loops.
   - **Random Walk**: Packets are sent to neighbors randomly, ensuring robustness but potentially leading to inefficient routes.



3. **Hybrid Algorithms**: These combine features of adaptive and non-adaptive algorithms, dividing the network into regions where different algorithms are used. Examples include link-state and distance vector routing.

3.13.2 Difference between Adaptive and Non-Adaptive Routing Algorithms

The primary distinction lies in their adaptability to network changes:

- **Adaptive Algorithms**: Dynamically adjust routing decisions based on network topology or traffic load changes, suitable for large, complex networks.
- **Non-Adaptive Algorithms**: Maintain fixed routing decisions, ideal for smaller, less complex networks.

3.13.3 Difference between Routing and Flooding

Routing involves determining optimal paths for data packets, while flooding forwards packets indiscriminately on all outgoing lines except the one they arrived on, potentially causing loops and duplication.

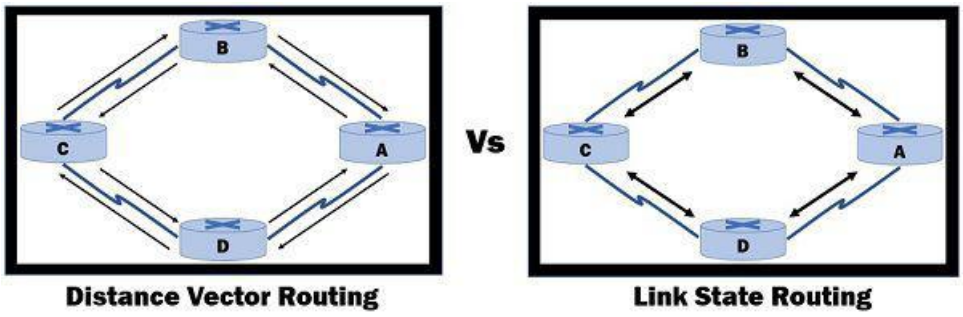
Routing	Flooding
A routing table is required.	No routing table is required.
May give the shortest path.	Always gives the shortest path.
Less Reliable.	More Reliable.
Traffic is less.	Traffic is high.
No duplicate packets.	Duplicate packets are present.

Table 3.1: Comparison of Routing and Flooding

3.13.4 Distance Vector Routing and Link State Routing

Distance Vector Routing dynamically computes distances between a router and its neighbors, periodically sharing this information to update routing tables. It may suffer from issues like count-to-infinity and persistent looping.

Link State Routing shares detailed network maps with all routers, facilitating accurate routing decisions only when there's a change in the network. However, heavy traffic due to flooding can be a challenge.



Distance Vector Routing	Link State Routing
Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwidth required is more due to flooding and sending of large link state packets.
Based on local knowledge, since it updates table based on information from neighbours.	Based on global knowledge, it has knowledge about entire network.
Make use of Bellman Ford Algorithm.	Make use of Dijkstra's algorithm.
Traffic is less.	Traffic is more.
Converges slowly i.e, good news spread fast and bad news spread slowly.	Converges faster.
Count of infinity problem.	No count of infinity problem.
Persistent looping problem i.e, loop will be there forever.	No persistent loops, only transient loops.
Practical implementation is RIP and IGRP.	Practical implementation is OSPF and ISIS.

Table 3.2: Comparison of Distance Vector Routing and Link State Routing

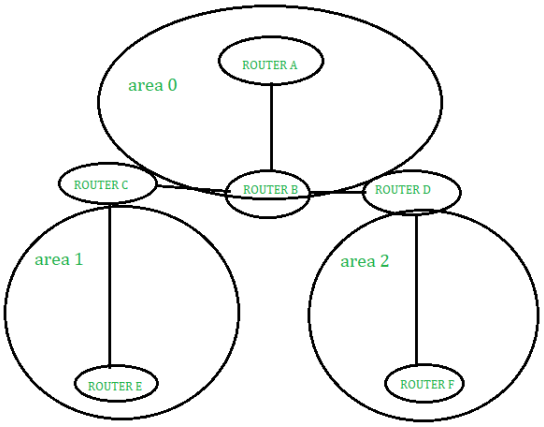
3.14 Routing in the Internet

Internet routing utilizes protocols like OSPF and BGP to determine optimal paths for data transmission across interconnected networks. OSPF is used for routing within an Autonomous System (AS), while BGP facilitates inter-domain routing between different ASes on the Internet.

3.15 Open Shortest Path First (OSPF)

OSPF is a type of hierarchical network topology or design. OSPF prefers the fastest path rather than the shortest path. In Open Shortest Path First, the internet protocol is used. It uses a link-state-routing (LSR) algorithm for its functionality.

OSPF is an Interior Gateway Protocol (IGP), where routers connect networks using the Internet Protocol (IP). It is a router protocol which is used to find the best path for packets when they are passing through the set of connected networks simultaneously. The main disadvantage of OSPF is that it is more complex than other protocols.

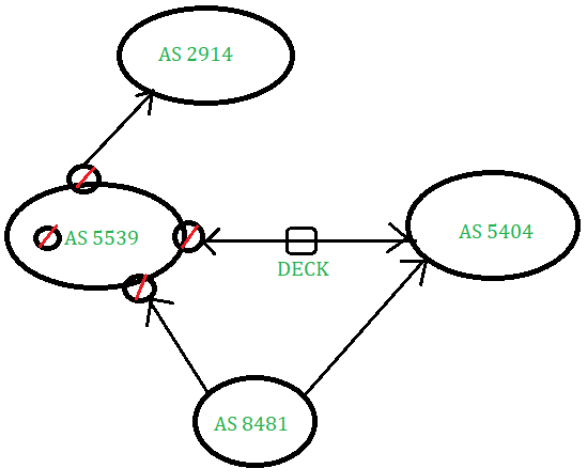


Here, Area 0 is the central area and other two areas are connected to it.

3.16 Border Gateway Protocol (BGP)

BGP is a type of mesh topology or design. Border Gateway Protocol prefers the best path. In Border Gateway Protocol, Transmission Control Protocol is used. The main difference between OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol) is that Open Shortest Path First is an intra-domain routing protocol while Border Gateway Protocol is an inter-domain routing protocol.

For example, if a user in India loads a website with origin servers in Singapore, then this BGP protocol is the one which enables the communication to happen quickly and efficiently. Another example is that if someone submits any data through the internet, then it is the responsibility of the BGP protocol to look after all the available paths in which data can travel.



Here, all prefixes are accepted into AS5539 which gets tagged with a community value:

- 5539:500 = customer
- 5539:100 = peering (decix)
- 5539:250 = upstream (NTT)

Let's see the difference between OSPF and BGP:

OSPF	**BGP**
OSPF stands for Open Shortest Path First.	BGP stands for Border Gateway Protocol.
The implementation of OSPF is easy.	While the implementation of BGP is difficult.
OSPF is a fast concurrence.	While BGP is a slow concurrence.
OSPF is type of hierarchical network topology or design.	While it is the type of mesh topology or design.
It is also called as internal gateway protocol.	While it is called as external gateway protocol.
In OSPF internet protocol is used.	While in this Transmission control protocol is used.
It works in 89 port number.	While it works in 179 port number.
OSPF is a Link State type.	While it is a Vector State type.
In OSPF Dijkstra algorithm is used.	While in this Best path algorithm is used.
OSPF prefers fastest path rather than shortest path.	While It prefers best path.
It requires device resources- CPU and memory.	It relies for the device resources type on the size of routing table, although it scales better.
Its metric is determined by bandwidth.	Its metric is determined using AS path, IGP-Metric, Next Hop, Weight, etc.
It is used mainly for small networks that can be managed centrally.	It is for large networks such as Internet.
OSPF prefers fastest path over shortest path.	It prefers best path.
The training cost involved is less.	The training cost is comparatively more than OSPF.

Table 3.3: Comparison of OSPF and BGP

IV

Unit IV

4. Link Layer: Services and Protocols

4.1 Introduction

The link layer, also known as the data link layer, is the second layer of the OSI model and is responsible for providing reliable data transmission over the physical network medium. It interacts directly with the physical layer and is primarily concerned with transmitting data frames between devices on the same local network.

4.2 Link Layer Services

The Link Layer, also known as Layer 2 of the OSI model, provides several key services for data communication within a local network:

1. **Addressing**: Assigning unique MAC addresses to network interfaces for communication within a local network.
2. **Frame Encoding/Decoding**: Converting data packets from the network layer into frames suitable for transmission over the physical medium, and vice versa.
3. **Error Detection and Correction**: Detecting and correcting errors that occur during data transmission.
4. **Medium Access Control (MAC)**: Controlling access to the physical medium to avoid collisions in shared media networks like Ethernet.
5. **Framing**: Dividing data into frames, adding headers and trailers for transmission, and reassembling received frames.

4.3 Error Detection and Correction Techniques

4.3.1 Parity Checks

Parity checks are a simple form of error detection technique that involve adding an extra bit (parity bit) to each byte of data being transmitted. There are two types of parity checks:

- **Even Parity**: Ensures that the total number of bits with a value of 1 in the byte (including the parity bit) is even.
- **Odd Parity**: Ensures that the total number of bits with a value of 1 in the byte (including the parity bit) is odd.

During transmission, if the parity of the received byte does not match the expected parity, an error is detected. However, parity checks can only detect errors; they cannot correct them.

4.3.2 Checksum Methods

Checksum methods are more sophisticated than parity checks and are commonly used in network protocols like TCP and UDP. A checksum is a calculated value based on the data being transmitted, which is appended to the data itself.

- **Checksum Calculation**: The sender calculates a checksum by performing a mathematical operation (such as addition or XOR) on the data bits.
- **Checksum Verification**: Upon receiving the data, the receiver recalculates the checksum using the same algorithm. If the calculated checksum matches the received checksum, no error is detected; otherwise, an error is indicated.

Checksum methods are more robust than parity checks as they can detect a wider range of errors, but they still have limitations.

4.3.3 CRC (Cyclic Redundancy Check)

CRC is a highly effective error detection technique commonly used in data communication protocols such as Ethernet, Wi-Fi, and Bluetooth. It operates by treating the data to be transmitted as a binary polynomial, which is divided by a fixed divisor polynomial.

- **CRC Calculation**: The sender performs polynomial division on the data using the CRC polynomial as the divisor. The remainder of the division, known as the CRC checksum, is appended to the data.
- **CRC Verification**: Upon receiving the data, the receiver performs the same polynomial division using the received data and the CRC polynomial. If the remainder is zero, no error is detected; otherwise, an error is indicated.

CRC offers several advantages over parity checks and checksum methods, including better error detection capabilities and efficiency.

4.4 Multiple Access Control

In shared media networks, multiple devices may attempt to transmit data simultaneously, leading to collisions. Multiple access control protocols manage access to the shared medium to avoid collisions. These methods are essential for managing shared communication resources efficiently

and avoiding interference or collisions. The primary categories of multiple access protocols include channel partitioning protocols and random access protocols.

4.4.1 Channel Partitioning Protocols

- **Time Division Multiplexing (TDM)**
  - TDM divides the channel into fixed time slots, each allocated to different users or devices.
  - Users take turns transmitting data within their allocated time slots.
  - Example: In a telephone system, each user gets a fraction of the total bandwidth during a specific time slot.
- **Frequency Division Multiplexing (FDM)**
  - FDM divides the channel into multiple frequency bands, with each user assigned a unique frequency band.
  - Users can simultaneously transmit data on their allocated frequency bands.
  - Example: Radio broadcasting, where different radio stations transmit on distinct frequency bands.
- **Code Division Multiple Access (CDMA)**
  - CDMA allows multiple users to transmit data simultaneously over the same frequency band.
  - Each user is assigned a unique code, which is used to modulate their data.
  - Despite sharing the same spectrum, users' transmissions are distinguishable using their unique codes.
  - Example: CDMA is commonly used in cellular networks, where multiple users share the same frequency band for communication.

4.4.2 Random Access Protocols

- **Slotted ALOHA**
  - Slotted ALOHA divides time into discrete slots and requires users to transmit only at the beginning of a time slot.
  - If two or more users attempt to transmit simultaneously, collisions occur, and the data is lost.
  - Efficiency: $1/e \approx 0.37$, where e is the base of the natural logarithm.
  - Example: Early satellite communication systems used Slotted ALOHA for multiple access.
- **Pure ALOHA**
  - Pure ALOHA allows users to transmit data at any time, without slot synchronization.
  - Collisions can occur if multiple users transmit simultaneously, resulting in data loss.
  - Efficiency: $1/(2e) \approx 0.18$.
  - Example: Pure ALOHA was used in the early versions of Ethernet networks.
- **Carrier Sense Multiple Access (CSMA)**
  - CSMA protocol requires users to listen to the channel before transmitting to avoid collisions.
  - If the channel is sensed as idle, the user can transmit; otherwise, it defers transmission.
  - CSMA alone does not prevent collisions completely but reduces their probability.
  - Example: Wi-Fi networks use CSMA to manage multiple users accessing the wireless medium.
- **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**
  - CSMA/CD is used in Ethernet networks to detect collisions and handle them appropriately.

- If a collision is detected during transmission, the device stops transmitting, waits for a random backoff time, and retries.
- This protocol helps in efficient sharing of the Ethernet medium by minimizing collision-related delays.
- Example: Traditional Ethernet networks employ CSMA/CD for multiple access.

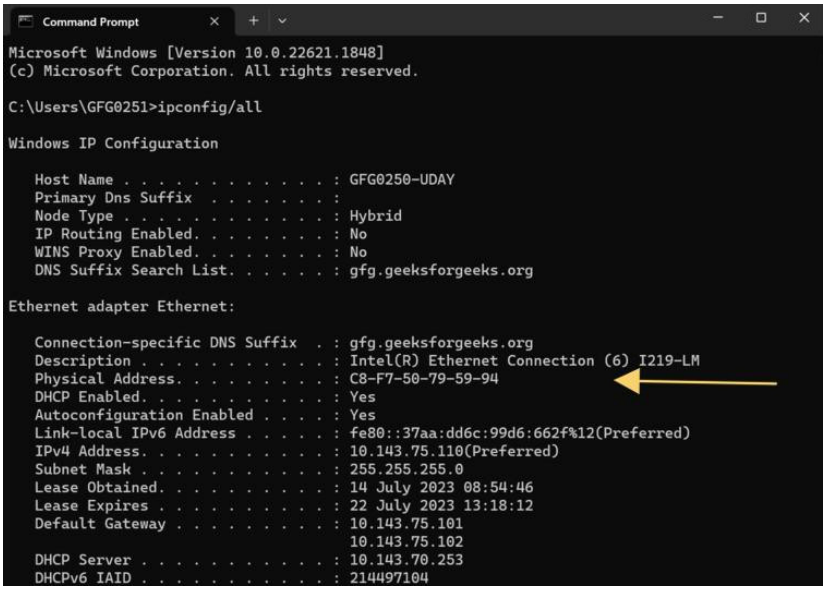
CSMA/CD	CSMA/CA
Effective after a collision	Effective before a collision
Used in wired networks (802.3)	Commonly used in wireless networks (802.11)
Reduces recovery time	Minimizes possibility of collision
Resends data frame after collision	Transmits intent to send before data transmission
More efficient than simple CSMA	Similar to simple CSMA
Detects collision on shared channel	Avoids collision on shared channel
Works in MAC layer	Works in MAC layer

Table 4.1: Comparison of CSMA/CD and CSMA/CA

4.5 Link Layer Addressing

Link layer addressing is an essential part of the network communication process, specifically within the data link layer of the OSI model. This layer is responsible for node-to-node data transfer and error detection/correction.

4.5.1 MAC Addresses



- **Definition:** Media Access Control (MAC) addresses are unique identifiers assigned to network interfaces for communications on the physical network segment.

- **Format:** MAC addresses are 48-bit numbers, typically represented as six pairs of hexadecimal digits (e.g., `00:1A:2B:3C:4D:5E`).
- **Types:**
  - **Unicast:** A unique address assigned to a single network interface card (NIC).
  - **Multicast:** Addresses used to send data to a group of devices.
  - **Broadcast:** An address (`FF:FF:FF:FF:FF:FF`) used to send data to all devices in a network segment.

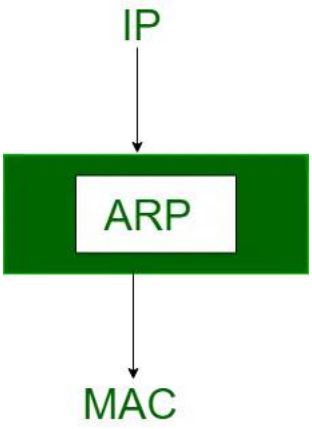
Functions

- **Frame Delivery:** MAC addresses are used to deliver frames within a local network.
- **Communication:** They ensure devices can communicate within the same local area network (LAN).

Structure

- **Organizationally Unique Identifier (OUI):** The first 24 bits, identifying the manufacturer.
- **Network Interface Controller (NIC) Specific:** The last 24 bits, uniquely identifying the device.

4.5.2 Address Resolution Protocol (ARP)



ARP is a protocol used to map IP addresses to MAC addresses, enabling proper data packet delivery within a LAN.

Purpose

- **IP to MAC Mapping:** ARP translates 32-bit IPv4 addresses to 48-bit MAC addresses, facilitating communication between devices on the same network.

ARP Process

- **ARP Request:**
  - A device broadcasts an ARP request packet to all devices on the network.
  - The packet contains the IP address of the destination device whose MAC address is being requested.
- **ARP Reply:**
  - The device with the matching IP address sends an ARP reply packet, including its MAC address.
  - This reply is sent directly to the requesting device.

Types of ARP

- **Gratuitous ARP:** A device broadcasts an ARP request for its own IP address to update other devices' ARP tables or to check for IP conflicts.
- **Proxy ARP:** One device answers ARP requests on behalf of another, used for routing purposes or in special network configurations.

Caching

- **ARP Cache:** Devices maintain a table of IP-to-MAC address mappings to reduce the frequency of ARP requests.
- **Stale Entries:** ARP entries have a limited lifetime and must be refreshed periodically to ensure accuracy.

Security Concerns

- **ARP Spoofing/Poisoning:** Malicious actors can send forged ARP messages to associate their MAC address with the IP address of another device, leading to man-in-the-middle attacks or denial of service (DoS).

4.5.3 Summary

- **Link Layer Addressing:** Utilizes MAC addresses to uniquely identify devices on a network, ensuring proper delivery of data frames within a LAN.
- **ARP:** Bridges the gap between the IP layer and the link layer by mapping IP addresses to MAC addresses, crucial for local network communication.

4.6 Ethernet

Ethernet is the most commonly used technology for Local Area Networks (LANs), governed by IEEE standards 802.3. It's favored for its simplicity, cost-effectiveness, and flexibility in network design. Ethernet operates across two layers of the OSI model: the **physical layer**, which deals with hardware connections, and the **data link layer**, responsible for frame transmission. It primarily uses a bus topology and employs the **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** protocol to manage data collisions.

Although wireless technologies like Wi-Fi have gained popularity, Ethernet remains prevalent in wired networks due to its reliability and security. While Wi-Fi offers wireless convenience, Ethernet ensures higher data transfer speeds and lower susceptibility to interference.

4.6.1 History of Ethernet

Ethernet revolutionized computer networking when Robert Metcalfe invented it in 1973. Initially supporting speeds of 10 Mbps, Ethernet's adoption soared after standardization by IEEE in 1983. Over time, its speeds increased to 100 Gbps, becoming the standard for wired connections worldwide.

4.6.2 Key Features of Ethernet

- **Speed**: Ethernet supports high-speed data transfer, with modern standards reaching up to 100 Gbps.
- **Flexibility**: It's adaptable to various devices and operating systems and easily scalable.
- **Reliability**: Utilizes error-correction techniques to ensure accurate data transmission.
- **Cost-effectiveness**: Provides a cost-efficient solution for network implementation and maintenance.
- **Security**: Offers built-in security features like encryption and authentication.

- **Manageability**: Networks are easily monitored and controlled by administrators.
- **Compatibility**: Works seamlessly with other networking technologies.
- **Scalability**: Can accommodate the addition of new devices and users without sacrificing performance.

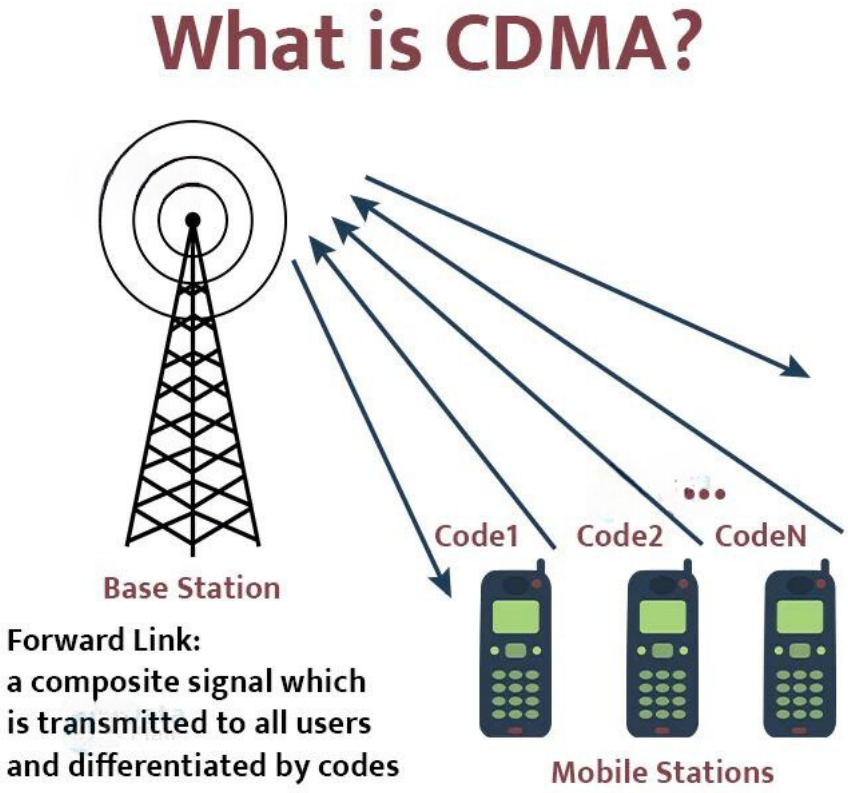
4.6.3 Advantages of Ethernet

- **Speed**: Offers significantly higher speeds compared to wireless connections.
- **Efficiency**: Consumes less energy, making it more energy-efficient.
- **Data transfer quality**: Maintains high-quality data transfer due to noise resistance.

4.6.4 Disadvantages of Ethernet

- **Distance limitations**: Maximum cable length restricts network size.
- **Bandwidth sharing**: Shared bandwidth may reduce network speeds with multiple devices.
- **Security vulnerabilities**: Despite built-in security, susceptible to breaches.
- **Complexity**: Requires specialized knowledge for setup and maintenance.
- **Compatibility issues**: May face compatibility challenges with older systems.
- **Cable installation**: Installation of physical cables can be time-consuming and costly.
- **Physical limitations**: Wired connections restrict mobility and flexibility.

4.7 CDMA (Code Division Multiple Access)



CDMA, or Code Division Multiple Access, is a wireless technology allowing multiple users to share the same frequency band simultaneously. Unlike other technologies dividing the spectrum

into separate channels, CDMA spreads data across the entire spectrum using unique codes. This enables multiple users to transmit and receive data concurrently without interference.

4.7.1 Key Features of CDMA

- **Spread Spectrum Technology**: Spreads data across a wider frequency band, enhancing resistance to interference.
- **Multiple Access**: Allows simultaneous transmission by assigning unique codes to users.
- **Soft Handoff**: Supports seamless transition between base stations for uninterrupted connectivity.
- **Capacity**: Accommodates a high number of simultaneous users efficiently.

4.8 Wi-Fi

Wi-Fi, short for Wireless Fidelity, facilitates wireless local area networking based on IEEE 802.11 standards. It enables devices to connect to the internet wirelessly via WLAN networks and access points (APs).

4.8.1 Wi-Fi Architecture

Wi-Fi architecture includes two services:

- **BSS (Basic Service Set)**: Consists of wireless mobile stations and optional central base stations (APs).
- **ESS (Extended Service Set)**: Comprises multiple BSSs with APs connected to a distribution system, typically Ethernet.

4.8.2 Features of Wi-Fi

- **Wireless Connectivity**: Provides mobility and flexibility by eliminating physical cables.
- **High Speed**: Offers fast internet access for data-intensive tasks.
- **Easy Setup**: Simple configuration requiring minimal technical expertise.
- **Multiple Device Connectivity**: Supports simultaneous connections for multiple users.
- **Security**: Ensures data protection through encryption and authentication measures.
- **Range**: Covers a wide area, depending on router capabilities and environmental factors.
- **Compatibility**: Works with various devices, including smartphones, laptops, and smart home devices.
- **Interference**: Susceptible to signal disruptions from other wireless devices and obstacles.
- **Reliability**: May experience signal loss or dropouts in congested or interfered environments.