

Chapter 1

Introduction to Computer Network

Prepared By R.G.B

Visit For Notes: <http://sites.google.com/site/rohitgbal>

Email: rohitgbal@gmail.com

Introduction

Network is the interconnection of a set of devices capable of communication.

There may be 2 kinds of devices in the network

1. Host:- also called end system. (desktop, laptop, cell phone)
2. Connecting Devices:- connects to other devices(modem, router, switch)

Network Criteria

1. Performance(evaluated by throughput and delay)
2. Reliability(evaluated by frequency of failure)
3. Scalability(Adding processing capacity)
4. Security(protecting data from unauthorized access)

Introduction

Application of Computer Networks

1. Business Application

- a) Resource Sharing
- b) High Reliability
- c) Saving Money

2. Home Application

- a) Access to Remote Information(WWW)
- b) Person to Person communication
- c) Interactive Entertainment(Live TV, Games)

Merits

- Allows File Sharing/ Resource Sharing
- Inexpensive System
- Flexible to be Used
- Increase in Storage Capacity of the Software

Demerits

- **Security Difficulties(Hacking)**
- **Presence of Computer Viruses and Other Malwares**

Network Models

- There are several classification for networks
- Classification based on Scale(size)
- Classification based on Topology
- Classification based on Architecture

Network Models : Based on Scale

- According to the scale(size) of the networks is classified into following
 1. PAN (Personal Area Network)
 2. LAN (Local Area Network)
 3. CAN (Campus Area Network)
 4. MAN (Metropolitan Area Network)
 5. DAN (Desert Area Network)
 6. CAN* (Country Area Network)
 7. WAN (Wide Area Network)
 8. GAN (Global Area Network)

Personal Area Network(PAN)

- Used for data transmission among devices such as computers, mobile phones, PDA etc.
- Within few meters like 10 meters only
- Medium : Bluetooth, Infrared
- Only very few connections will be available

Local Area Network(LAN)

- It is a computer network that spans a relatively small area
- Most LANs are confined to a single building or group of buildings
- One LAN can be connected to other LANs over any distance via telephone lines and radio waves (WAN)
- Medium: optical fibers, coaxial cables, twisted pair, wireless.
- Low latency (except in high traffic periods).
- High speed networks (0.2 Mb/sec to 1Gb/sec).
- Speeds adequate for most distributed systems

Campus Area Network(CAN)

- Computer network that links the buildings and consists of two or more local area networks (LANs) within the limited geographical area
- It can be the college campus, enterprise campus, office buildings, military base, industrial complex
- CAN is one of the type of MAN (Metropolitan Area Network) on the area smaller than MAN
- The Campus networks usually use the LAN technologies, such as Ethernet, Token Ring, Fibber Distributed Data Interface (FDDI), Fast Ethernet, Gigabit Ethernet, Asynchronous Transfer Mode (ATM)

Metropolitan Area Network(MAN)

- Metropolitan Area Network, are data networks designed for a town In terms of geographic breadth
- MANs are larger than local area networks (LANs), but smaller than wide-area networks s)
- MANs are usually characterized by very high-speed connections using fiber optical cable or other digital media

Features:

- Generally covers towns and cities (50 kms)
- Medium: optical fibers, cables.
- Data rates adequate for distributed computing applications.

Metropolitan Area Network

- MAN is usually **not** privately **owned** by an organization (Like banks, MNC)
- Access to a MAN is usually through a network provider who sells the service to the users
- MAN often acts as a **high speed network** to allow sharing of regional resources
- It is also frequently used to provide a shared connection to other networks using a link to a WAN

Country Area Network(CAN*)

- It's wide area network which is limited to country
- It consist of more than one MAN
- It may be extended up to thousands kms
- It is more public network owned by some public organization or governments
- Example: In Nepal NTC have CAN*
-

Wide Area Network(WAN)

- A computer network that spans a relatively large geographical area
- WAN consists of two or more local-area networks (LANs).
- Computers connected to a wide-area network are often connected through public networks, such as the telephone system
- They can also be connected through leased lines or satellites
- The largest WAN in existence is the **Internet**

Global Area Network(GAN)

- A global area network (GAN) refers to a network composed of different interconnected networks that cover an unlimited geographical area.
- The term is loosely synonymous with Internet, which is considered a global area network.

Topology

Topology :- Physical inter connection between different node

Node:- End device in computer network(Laptop, mobile, desktop, PDA, tablet etc.)

Various Topologies are:-

- Bus
- Ring
- Star
- Mesh
- Tree
- Hybrid

Bus

- In this system there are 8 nodes connected to network using common connection also called bus
- All communication is done with help of bus.

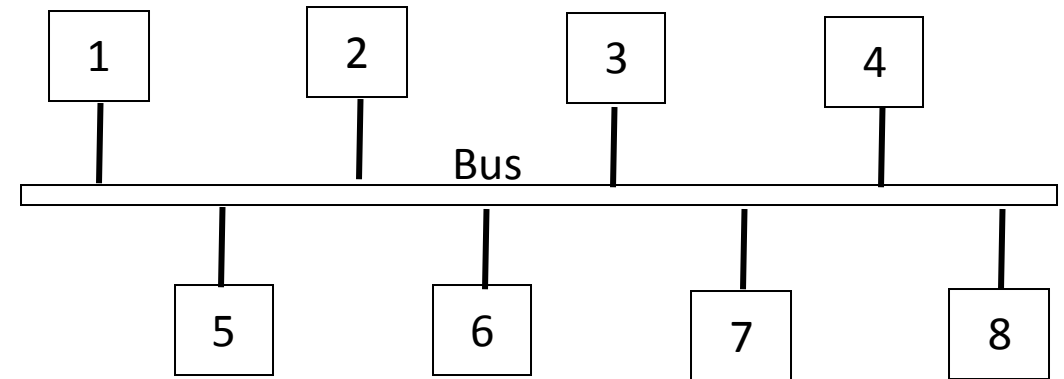
Advantage:

Less expensive

Disadvantage

Only one connection at a time

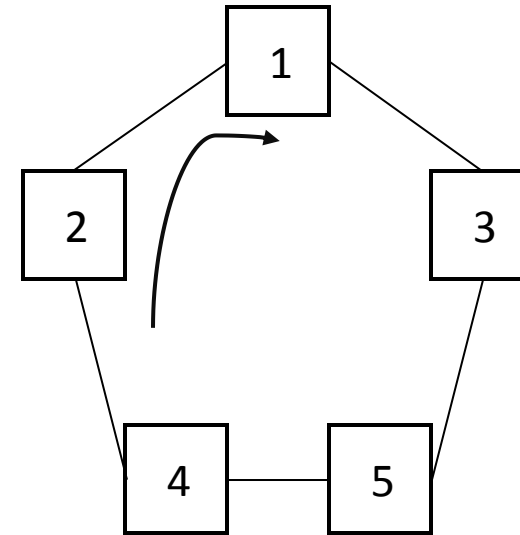
Figure : Bus Topology



Consider if node 1 is communicating with 5 other node have to wait for data transfer till 1-5 finished the communication is completed

Ring

- Data travels in circular fashion from one computer to another on the network.
- Typically FDDI, SONET or Token Ring technology are used to implement a ring network
- Data access based on token
- Only one way data transfer
- Data passed through intermediate nodes to destination



Consider if data transfer from node 1 to 2, It will pass through 3,5,4 and reaches 2

Ring

Advantages

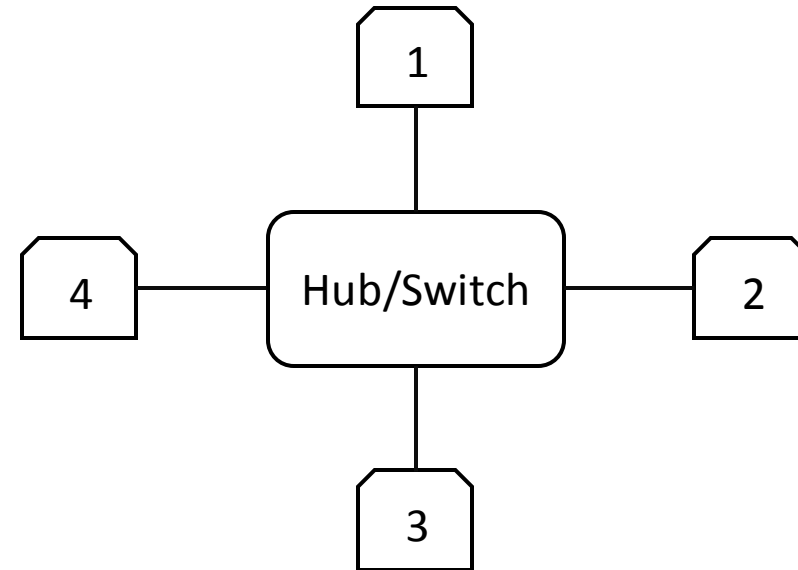
- A central server is not required for the management
- Traffic is unidirectional and the data transmission is high-speed.
- Comparison to a bus, a ring is better at handling load.
- Easier configuration and fault detection
- Less expensive than a star topology.

Disadvantage

- Failure of a single node in the network can cause the entire network to fail.
- Less secured because of intermediate nodes
- Lower speed because of intermediate nodes

Star

- All computers/devices connect to a central device called hub or switch.
- Each device requires a single cable
- Point-to-point connection between the device and hub.
- Most widely implemented
- Hub/Switch is the single point of failure



Star

Advantages

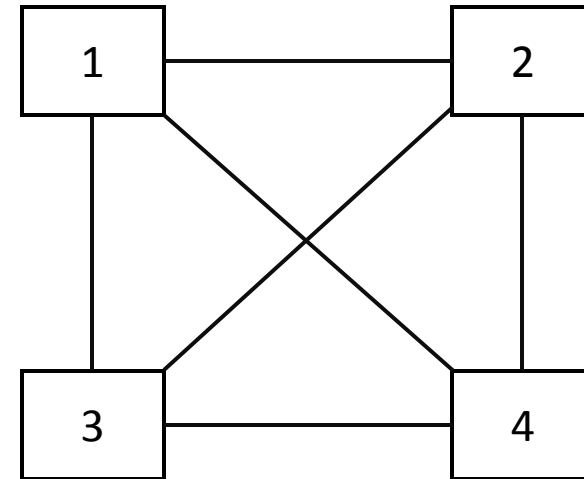
- Due to its centralized nature, the topology offers **simplicity of operation**
- **Isolation** of each device in the network
- Adding or removing network nodes is easy, and can be done without affecting the entire network
- Due to the centralized nature, it is easy to detect faults in the network devices
- As the analysis of traffic is easy, the topology poses lesser security risk

Disadvantage

- Network operation depends on the functioning of the central hub. Hence, central hub failure leads to failure of the entire network
- Also, the number of nodes that can be added, depends on the capacity of the central hub
- The setup cost is quite high.

Mesh

- Each computer connects to every other.
- High level of redundancy.
- Rarely used
- Wiring is very complicate
- Cabling cost is high
- Troubleshooting a failed cable is tricky



Mesh

Advantages

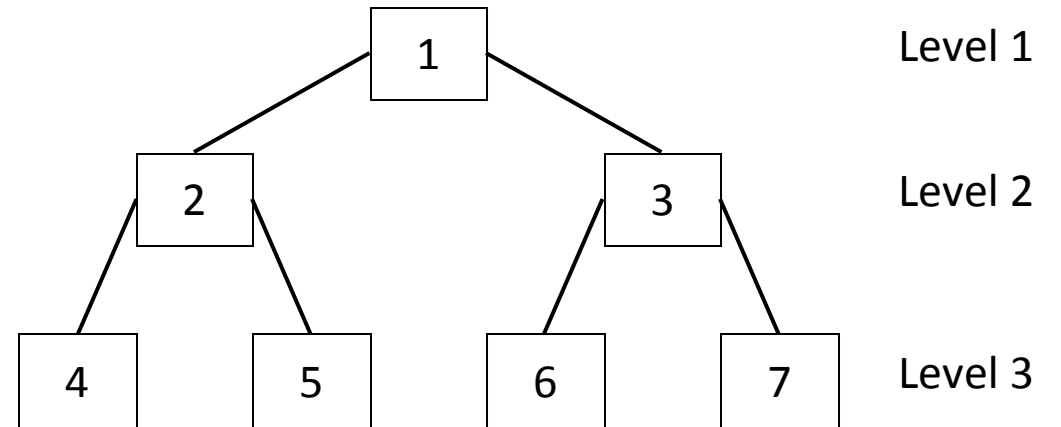
- Possible to transmit data from one node to many other nodes at the same time
- Failure of a single node does not cause the entire network to fail as there are **alternate paths** for data transmission
- It can handle heavy traffic, as there are dedicated paths between any two network nodes
- Point-to-point contact between every pair of nodes, makes it **easy to identify faults**

Disadvantages

- Many connections serve **no major purpose**
- Lot of cabling is required
- Costs incurred in setup and maintenance are **high**
- **Administration** of a mesh network is **difficult**

Tree

- Hierarchical structure like inverted tree
- Top node (node 1) is the root node
- It should at least have 3 levels
- Ideal for nodes that are grouped for some specific job



Tree

Advantages

- Expansion of nodes is possible and easy
- Easily managed and maintained
- Error detection is easily done

Disadvantages

- Heavily cabled
- Costly
- If more nodes are added maintenance is difficult
- If one node fails all nodes under it will be out of the network

Hybrid

- Two or more different types of topologies which is a mixture of two or more topologies
- For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

Advantages

- Effective
- Scalable
- Flexible

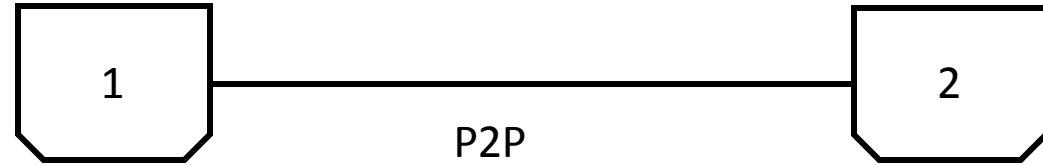
Disadvantages

- Complex in design
- Costly.

Network Models : Based on Architecture

- Network architecture refers to how computers are organized in a network and how tasks are allocated between these computers
- Two of the most widely used types of network architecture are
 1. **Peer-to-Peer(P2P)**
 2. **Client/Server**

Peer to Peer(P2P)



- Tasks are allocated among all the members of the network
- No hierarchy(importance) -- All considered equal
- Does not use a central computer server that controls network activity
- All computer on the network has a special software running that allows for communications between all the computers
- One – One(1:1) relationship
- Peer-to-peer is mostly used for file sharing
- One of the earliest peer-to-peer file sharing networks was Napster
- Now **torrent** uses this way to share files

Peer to Peer(P2P)

Advantage

1. Easy to install and configure
2. All the resources and contents are shared by all the peers
3. P2P is more reliable as central dependency is eliminated
4. No need for full-time System Administrator(No central Admin)
5. Cost comparatively very less

Peer to Peer(P2P)

Disadvantage

1. One person (user / administrator)cannot determine the whole accessibility setting of whole network
2. Security in this system is very less viruses, spywares,trojans, etc malwares can easily transmitted over this P-2-P architecture
3. Data recovery or backup is very difficult. Each computer should have its own back-up system
4. Lot of movies, music and other copyrighted files are transferred using this type of file transfer. P2P is the technology used in torrents

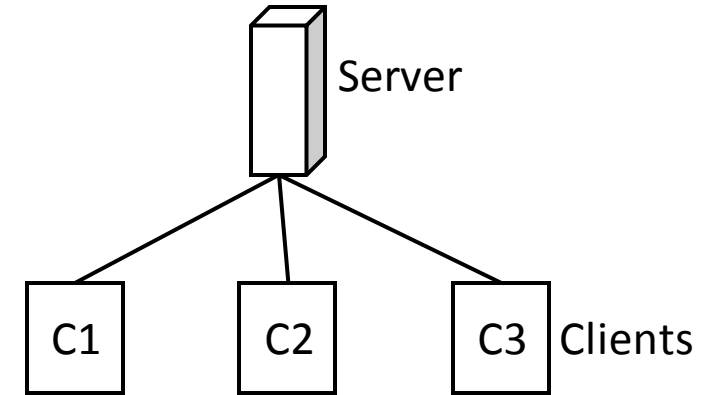
Client/Server(Tiered)

- Computing system in which one powerful workstation serves the requests of other systems
- Server :- Provides services to clients
- Client :- Accept services from server
- Server is central device for managing files , and other resources.
- If server is down all communication among the clients will be down
- **Features of Servers :-**
 1. They have large storage capacity.
 2. They are able to provide information to many computers simultaneously, therefore have large RAM
 3. Its processor speed is high, as it may have to execute multi-tasking too

Client/Server

Advantages

1. Centralization
2. Proper Management
3. Back-up and Recovery possible
4. Upgradation and Scalability in Client-server set-up
5. Accessibility
6. Security



Client/Server

Disadvantages

1. Congestion in Network(Too many requests at same time)
2. Cost : It is very expensive to install and manage this type of computing
3. Client-Server architecture is not as robust as a P2P and if the server fails, the whole network goes down.
4. You need professional IT people to maintain the servers and other technical details of network.

Active Networks(ANTS)

- Allows packets flowing through a telecommunications network to dynamically modify the operation of the network
- Dynamic modification is mainly for improving the performance of the system
- Real time /Rapid changes in network is allowed
- Usually network packets consist of data only but in ANTS packets consist of code and data
- Application customized code to be executed in network

Internet, Intranet & Extranet

- **Internet:-** Connections between different network/LAN. There will be outside connection. It is public network
- **Intranet:-** Connection inside a network/LAN. No outside connection
- **Extranet:-** Connects 2 or more intranet but not private. It is used to connect between 2 branches of company or connection between company and client.

Chapter 2

Reference Model

Prepared By R.G.B

Visit For Notes: <http://sites.google.com/site/rohitgbal>

Email: rohitgbal@gmail.com

Reference Model

- 2 important reference models **OSI reference model & TCP/IP reference model**
- Also called Protocol Architecture or Layered Architecture
- Mainly define the protocols of communication in layered architecture

Protocol ???

- Protocol means rule
- In computer networking Protocol means rules for establishing communication between 2 devices
- Consists of a set of rules that govern data communications
- determines what is communicated, how it is communicated and when it is communicated
- **Key Elements**
 1. Syntax
 2. Semantics
 3. Timing

Syntax, Semantics and Timing

Syntax

- Structure or format of the data
- Indicates how to read the bits - field delineation
- Syntax should be same in sender and receiver for to communicate

Semantics

- Interprets the meaning of the bits
- Knows which fields define what action
- Interpretation of the syntax should be same

Timing

- When data should be sent and what
- Speed at which data should be sent or speed at which it is being received

ISO/OSI Reference Model

- ISO- International Organisations for Standard
- OSI- Opens System Interconnections
- Stats developing in late 1970s
- Approved by 1984
- The term “Open” in Open System Interconnections denotes **“to communicate with any 2 systems”**
- There are 7 layers in OSI Reference model
- It is also called OSI layered architecture /OSI Protocol architecture

ISO/OSI Reference Model

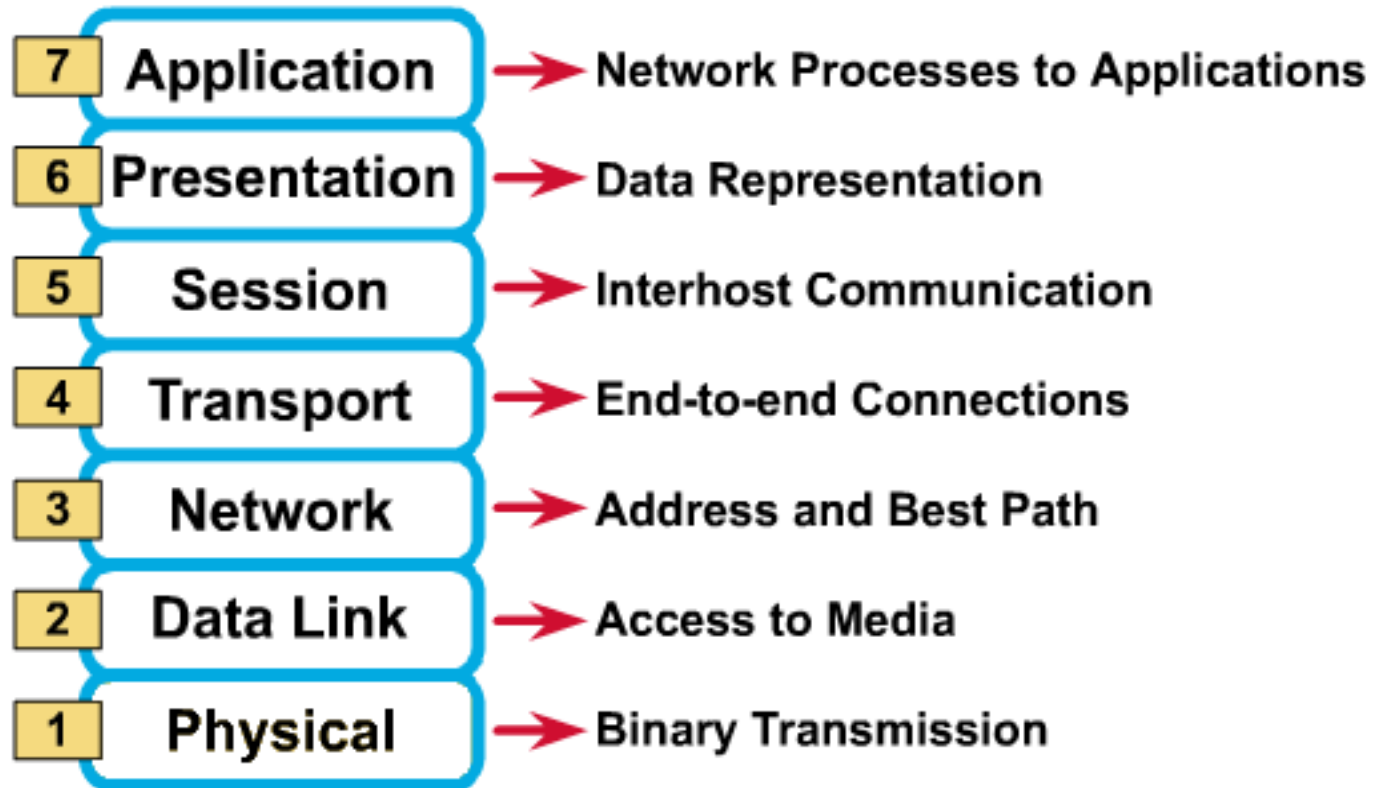
- The process of breaking up the functions or tasks of networking into layers reduces complexity.
- Each layer provides a service to the layer above it in the protocol specification.
- Each layer communicates with the same layer's software or hardware on other computers.
- The lower 4 layers are concerned with the flow of data from end to end through the network
- The upper Three layers of the OSI model are orientated more toward services to the applications

ISO/OSI Reference Model- 7 Layers

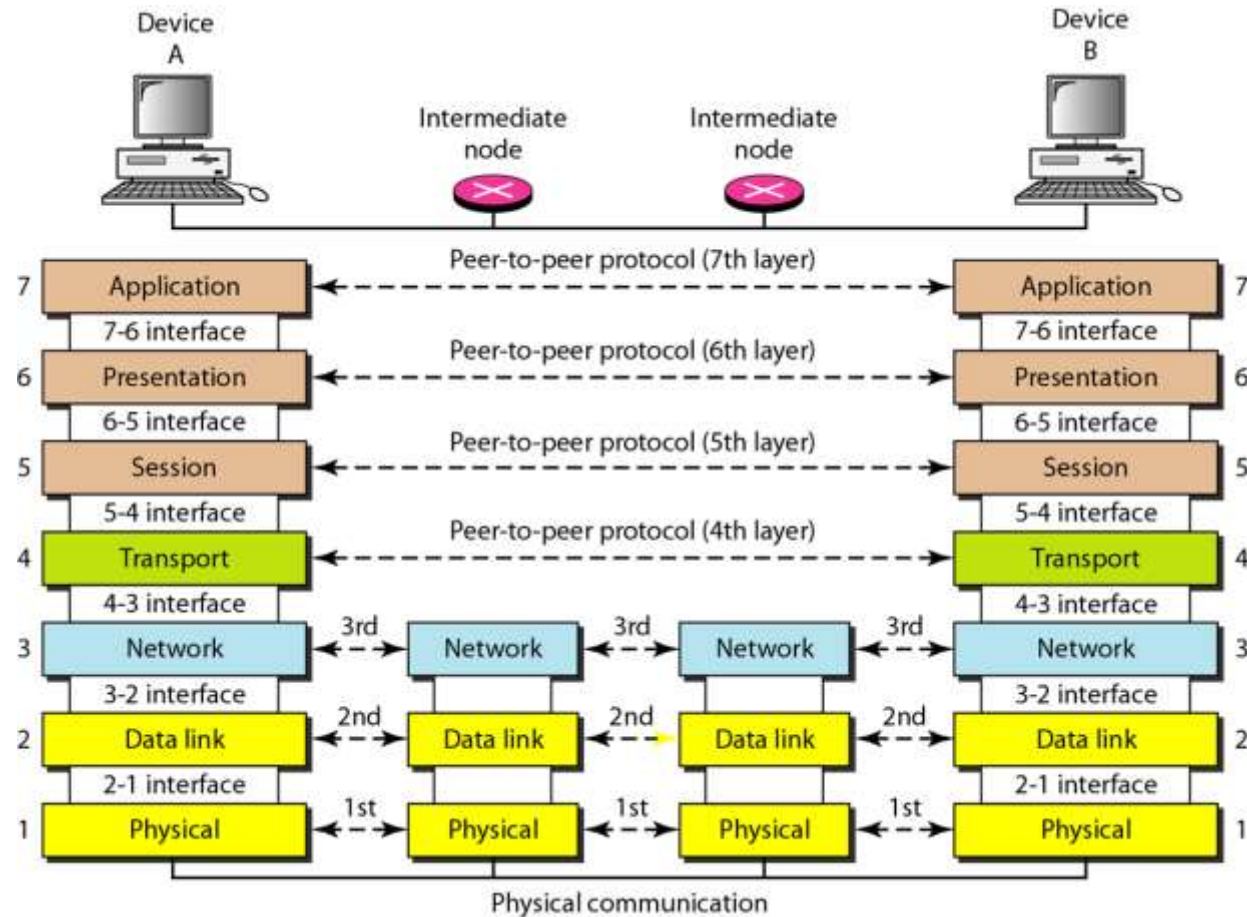
- Layer 7 –Application Layer
- Layer 6 –Presentation Layer
- Layer 5 –Session Layer
- Layer 4 –Transport Layer
- Layer 3 –Network Layer
- Layer 2 –Data Link Layer
- Layer 1 –Physical Layer

OSI Consider a receiver system hence Layer 1 at bottom

ISO/OSI Reference Model- 7 Layers



ISO/OSI Reference Model- 7 Layers



Application Layer (Layer 7)

- The application layer is responsible for providing services to the user
- The layer relates to the services that directly support user applications, such as software for file transfers, database access, and e-mail, web browsers
- A message to be sent across the network enters and exits the OSI reference model's at this layer.
- Protocols works in this layer are HTTP,FTP,DNS..
- HTTP(HyperText Transfer Protocol)
- FTP(File Transfer Protocol)
- DNS(Domain Name System)

Presentation Layer (Layer 6)

- Defines the format used to exchange data among networked computers
- Acts like translator (interpreter)
- When computers from dissimilar systems—such as IBM, Apple, and Sun—need to communicate, a certain amount of translation and byte reordering must be done
- Within the sending computer, the presentation layer translates data from the format sent down from the application layer into a commonly recognized, intermediary format

Presentation Layer (Layer 6)

- At the receiving computer, this layer translates the intermediary format into a format that can be useful to that computer's application layer
- The presentation layer is responsible for converting protocols, **translating the data, encrypting the data**, changing or converting the character set, and expanding graphics commands.
- The presentation layer also manages **data compression** to reduce the number of bits that need to be transmitted.

Session Layer (Layer 5)

- Session is a logical connection between 2 systems
- Layer is responsible creating managing and termination of session
- Also responsible for dialogue management
- 3 Types of Dialogue
 1. Simplex : 1 Way Communication(Radio)
 2. Half Duplex : 2 Way Communication, But One at a time (Walkie-Talkie)
 3. Full Duplex: 2 Way Simultaneous Communication (Telephone)
- Also Provide Security and Check points in data

Transport Layer (Layer 4)

- Provide a reliable mechanism for the exchange of data between two processes in different computers.
- Data from above layer is converted into smaller Data Units called segments
- Segments consist of Port number , Acknowledge number, Sequence number

Transport Layer (Layer 4)

- Ensures that the data units are delivered error free, delivered in sequence, there is no loss or duplication of data units.
- Provides connectionless(UDP) or connection oriented service(TCP).
- Provides for the connection management.
- Multiplex multiple connection over a single channel.

Transport Layer (Layer 4) TCP vs UDP

TCP(Transmission Control Protocol)

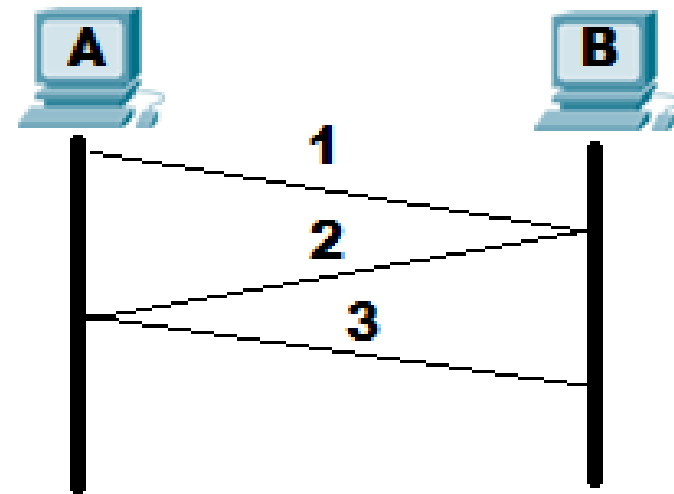
- Connection Oriented
- Reliable
- Have Acknowledgement
- Have Retransmission
- Have Sequence Delivery
- Have Handshaking

UDP (User Datagram Protocol)

- Connectionless
- Unreliable
- No Acknowledgement
- No Retransmission
- No Sequence delivery
- No Handshake signal

Transport Layer (Layer 4) - 2 Way Handshaking

- 3 way handshaking signal establish logical connection between 2 computers before data transfer
- Steps involved are:-
 1. TCP Connection Request(Syn A to B)
 2. TCP Connection Reply(Ack B to A)
 3. Data Transfer (A to B)



Network Layer (Layer 3)

- Data units from the Transport layer is converted into packets(IP Packets)
- Each packet consist of IP Header
- IP header consist of Source IP, Destination IP and several other details regarding Packet
- IP(Internet Protocol) address helps packet to navigate from source to destination between **different network**(internetwork)
- Implements routing of packets through the network

Network Layer (Layer 3)

- Defines the most optimum path the packet should take from the source to the destination
- Handles congestion in the network.
- Facilitates interconnection between heterogeneous networks (Internetworking).
- The network layer also defines how to fragment a packet into smaller packets to accommodate different media
- Protocol in this layer is IP(Internet Protocol)

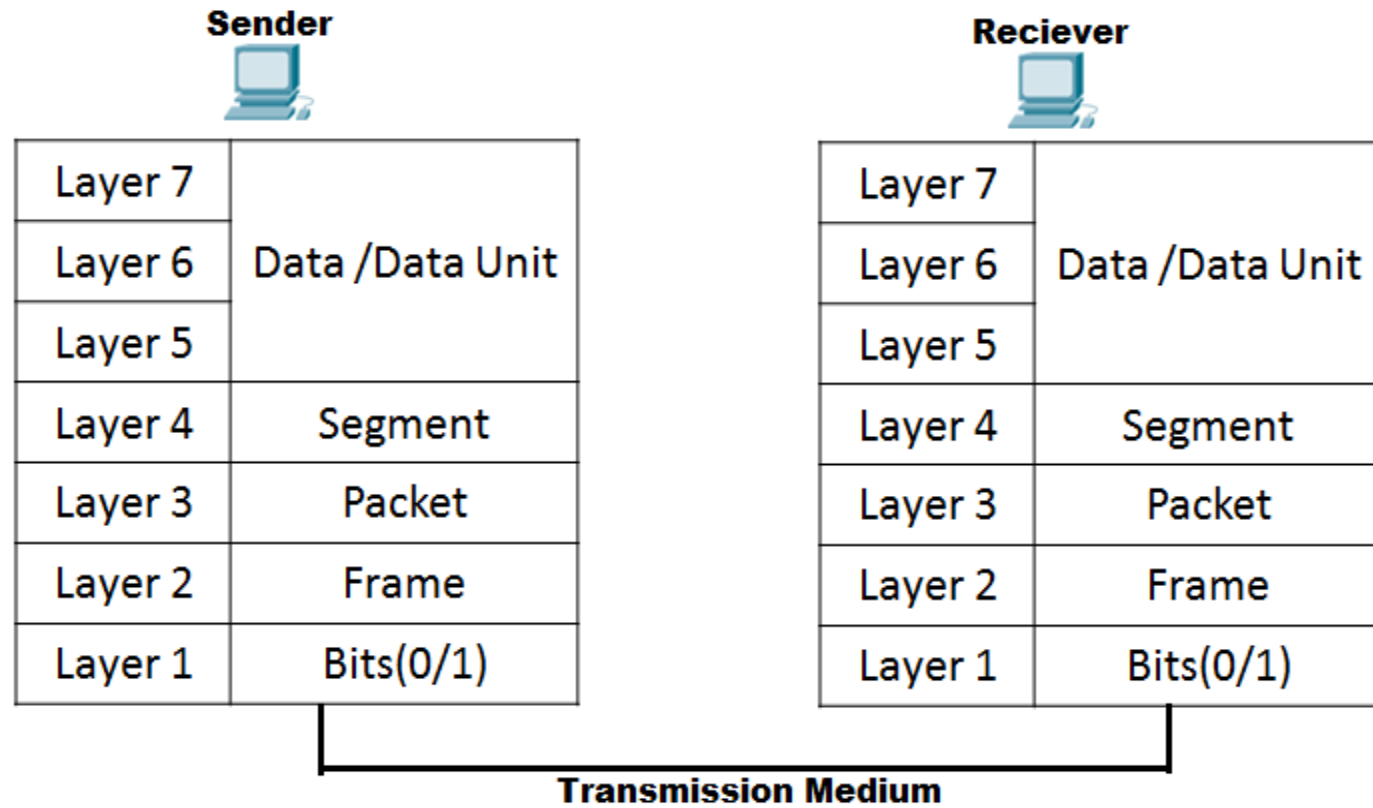
Data Link Layer (Layer 2)

- Packet from network layer is converted to Frames
- Frame consist of frame header
- Frame header consist of source and destination MAC(Media Access Control) Address
- Data link layer attempts to provide reliable communication over the physical layer interface
- Create and detect frame boundaries
- Implement flow control, Error control(Parity, Hamming Code)
- Supports points-to-point(unicasting) as well as broadcast communication
- Supports simplex, half-duplex or full-duplex communication

Physical Layer (Layer 1)

- Convert the frames into bits (0/1) and transmit through medium
- Provides physical interface for transmission of information
- Defines rules by which bits are passed from one system to another
- Covers all - mechanical, electrical, functional and procedural - aspects for physical communication.
- Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.

OSI Layer Working



TCP/IP Reference Model

- Also called Internet Reference model
- Consist of 4 layered Architecture
 1. Application Layer
 2. Transport Layer
 3. Internetwork Layer(Internet Layer)
 4. Network Access Layer (Network Interface Layer)

TCP Layer

Application Layer

- Similar to Application Presentation and Session layer in OSI
- Application programs using the network

Transport Layer (TCP/UDP)

- Similar to Transport Layer in OSI
- Only TCP protocol works
- Management of end-to-end message transmission,
- error detection and error correction

TCP Layer

Internetwork Layer (IP)

- Similar to Network layer in OSI
- IP Address
- Handling of packets : routing and congestion

Network Access Layer

- Similar to Datalink and physical layer in OSI
- Management of cost effective and reliable data delivery,
- access to physical networks
- Physical Media

TCP/IP vs OSI

Application	Data	Application	Data
Presentation			
Session			
Transport	Segment	Transport	Segment
Network	Packet	Internetwork	Packet
Data Link	Frames	Network Access	Frames & Bits
Physical	Bits		
OSI		TCP/IP	

TCP/IP Vs OSI

OSI

- 7 Layered architecture
- Designed for General Network
- Supports TC and UDP
- Designed both Functionalities of layer and protocol
- Defines functionalities of all layer
- Protocols are hidden in OSI model and are easily replaced as the technology changes.

TCP/IP

- 4 Layered architecture
- Internet only
- Supports only TCP
- More based on protocols than functions
- Only protocol
- Difficult to change the protocol in future

Networking Devices

- NIC
- HUB
- REPEATER
- SWITCH
- ROUTER
- BRIDGE

NIC

- NIC(Network Interface Card) also called Network Adapter
- It is a part of computer which provide communication
- The network adapter provides one or more ports for the network cable to connect to, and it transmits and receives data onto the network cable
- NIC may be wired or wireless
- Every networked computer must also have a network adapter driver, which controls the network adapter.
- Each network adapter driver is configured to run with a certain type of network adapter

NIC

Functions of NIC:-

1. Data encapsulation
2. Signal encoding and decoding
3. Transmission and reception
4. Data buffering
5. Serial/parallel conversion
6. Media access control
7. Network protocols

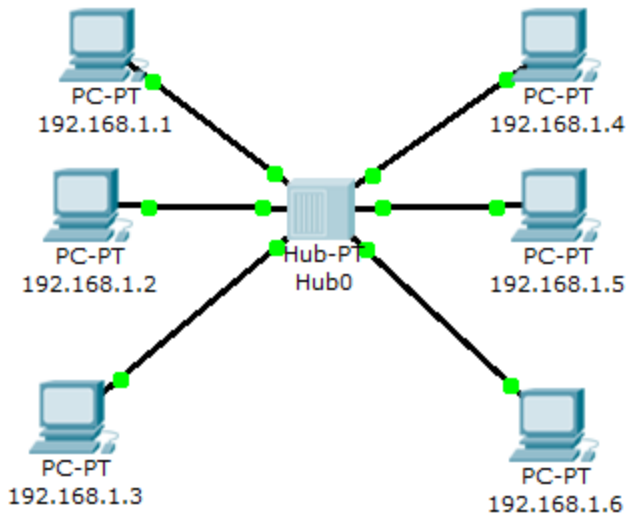


HUB

- Works in physical layer
- Device used to connect different computers to a network(LAN), Only same range of IP is allowed
- Supports simplex and Half duplex data transmission, Only station can transmit at a time
- Hub is based on broadcasting
- Hub will forward the data to all other port, only the receiver will receive and other nodes will drop the data
- Because the hub is broadcasting the Chance of collision is high in HUB
- Easily scalable

LAN Connection With HUB

- *In figure all IP in switch are of same range (192.168.1.0 range)*



SWITCH

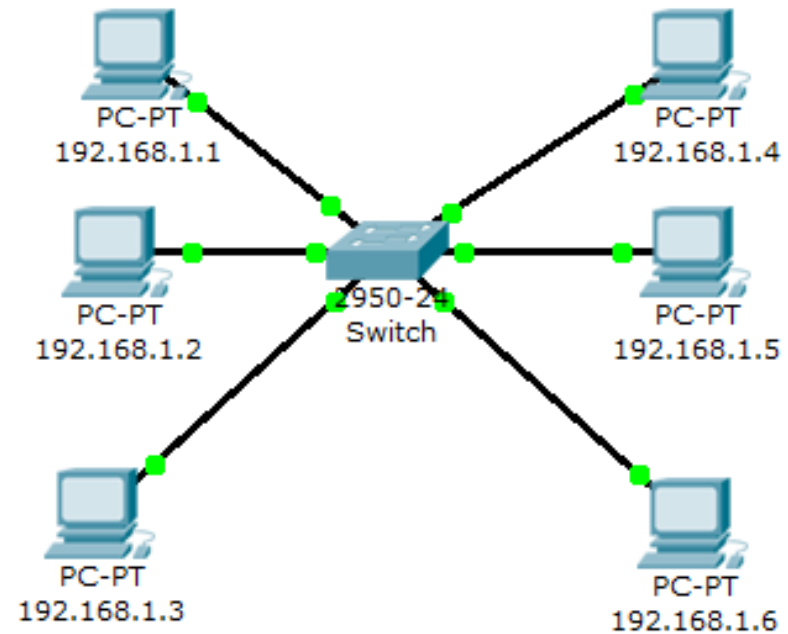
- Works on Layer 2
- Works based on MAC address
- Used to connect computers in Network (LAN), Only same range of IP
- Have MAC address table to store information about ports and MAC address of computer connected in port
- Broadcasting only done initially after that unicasting
- Broadcasting only before learning the mac address of the systems connected

SWITCH

- Switch automatically will learn the MAC Address of the system connected in the port and stores in MAC table
- After learning the address only unicasting is used for data transmission
- It can operate in simple, half duplex and full duplex mode
- Easily Scalable

SWITCH

- There are 4 forwarding methods:
 1. Store and forward
 2. Cut through
 3. Fragment free
 4. Adaptive
- *In figure all IP in switch are of same range (192.168.1.0)*



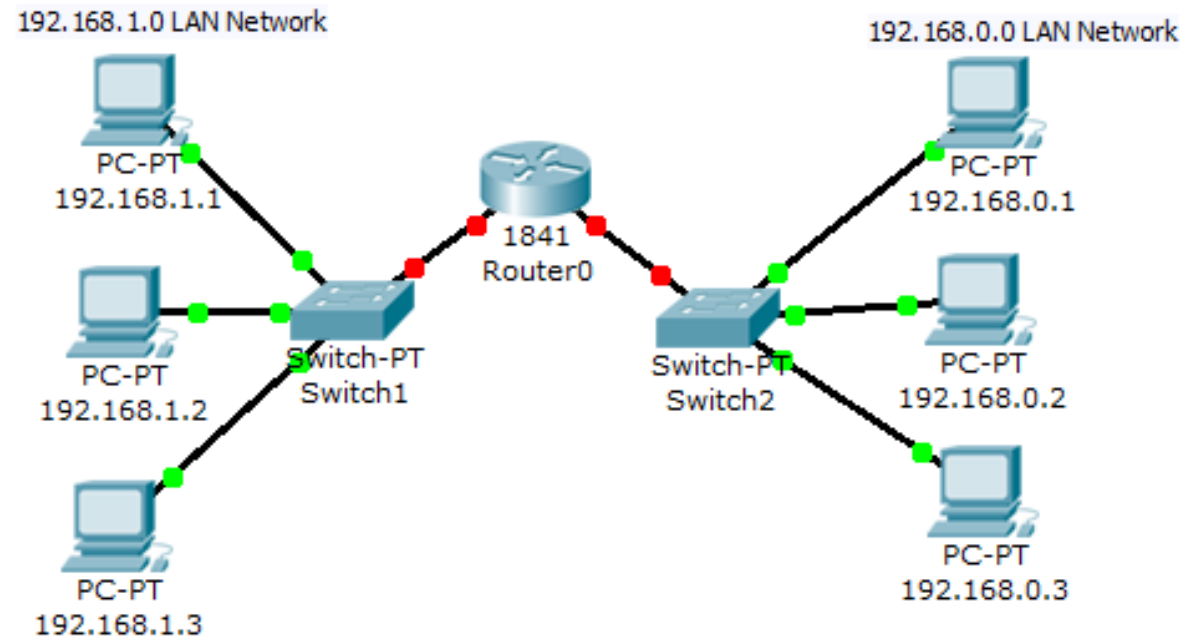
ROUTER

- Router works on Network layer
- It work based on IP address
- It helps in finding route ,best path in Networks
- A router is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network
- Routers are located at gateways, the places where two or more networks connect each other

ROUTER

- Router Have routing table which stores information about IP, interface , best route.
- Routing table will help in routing of the packets in network.
- Router also have some algorithm for finding route and shortest path first such as RIP,OSPF, EIGRP

Connecting 2 Network using Router

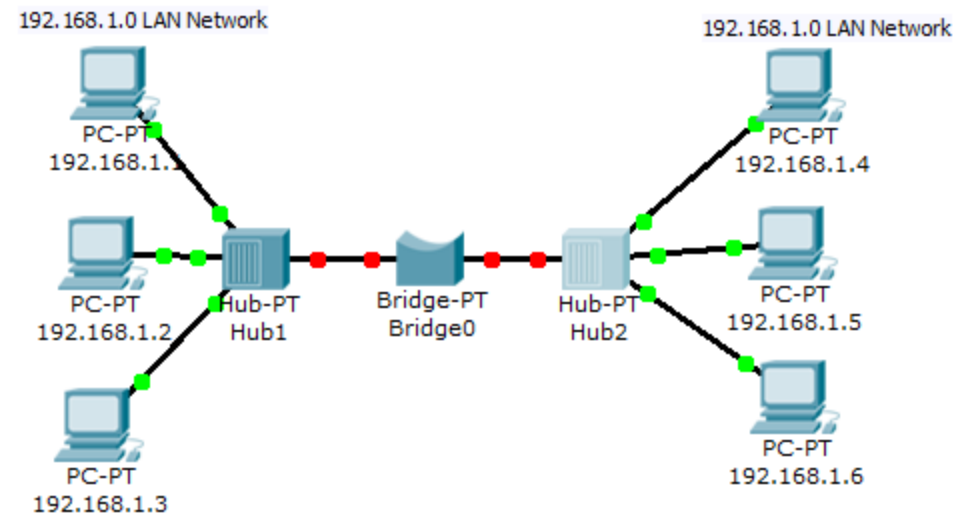


BRIDGE

- Bridge connect 2 segments of same network
- Bridge works on same principle of switch(Layer 2 , MAC table)
- Bridges are used when hub is used in LAN
- HUB have higher no of collision when more devices are the in network
- To avoid the no of collision in network connected using hub
- Network is divided into smaller segments connected using bridge

Connecting 2 segments of one network using Bridge

- 2 segments of same network(192.168.1.0)
- Segment One (LHS) 192.168.1.1-\ to 3
- Segment Two (RHS) 192.168.1.4-\ to 6



REPEATER

- Works on Layer One of OSI layer
- Device that receives a signal and retransmits it at a higher level or higher power
- In wireless communication, receives a signal and it also retransmits it onto the other side of an obstruction
- It helps signal to cover longer distances
- Also called signal booster

Chapter 3

Physical Layer

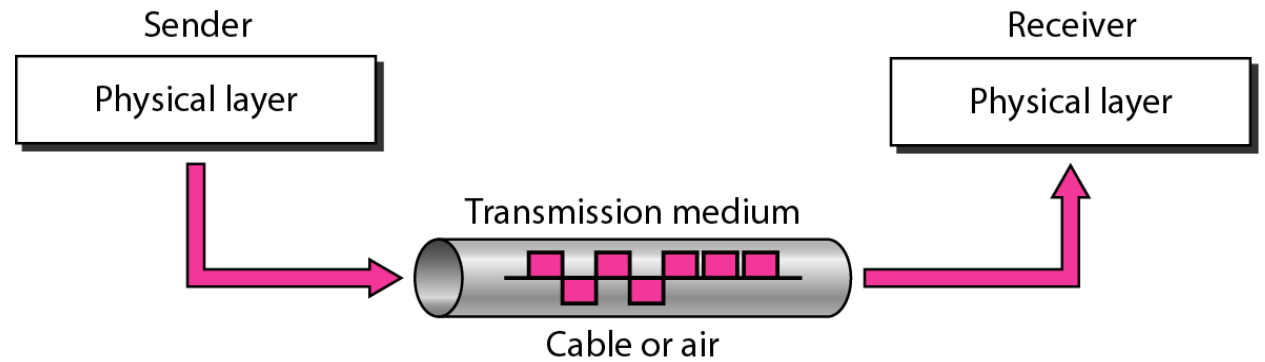
Prepared By R.G.B

Visit For Notes: <http://sites.google.com/site/rohitgbal>

Email: rohitgbal@gmail.com

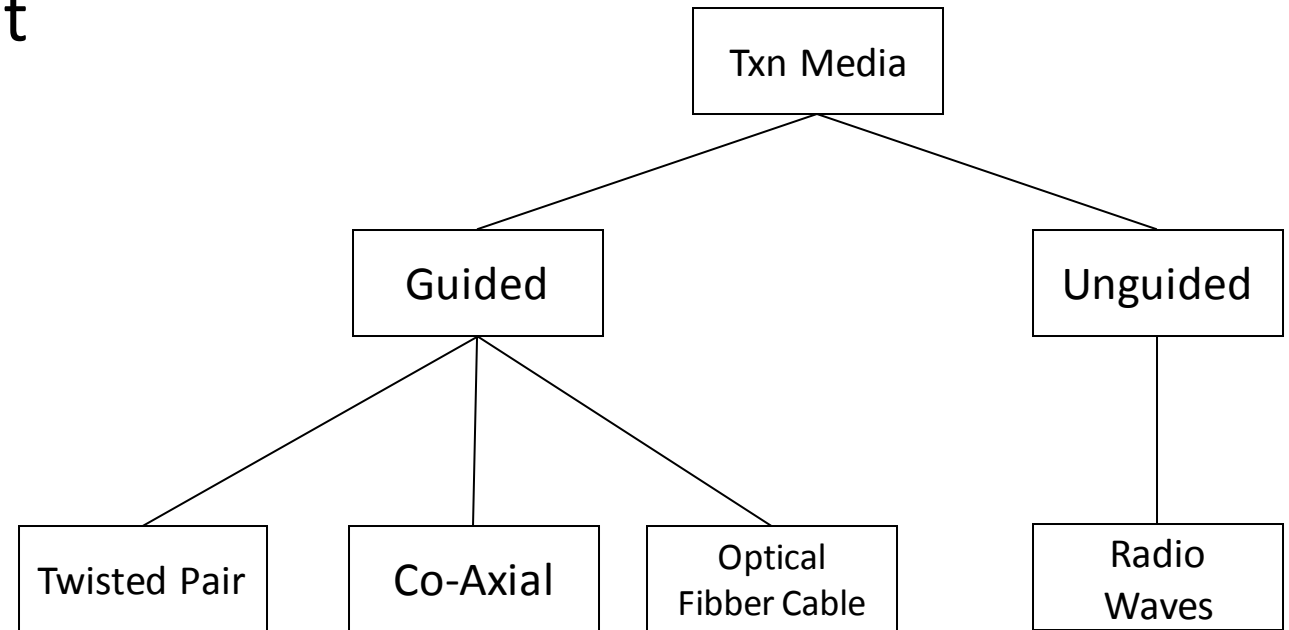
Topics Covered

1. Transmission media
 1. Guided media
 2. Unguided media
2. Switching methods
 1. Circuit Switching
 2. Packet Switching
 3. Message Switching
3. ISDN
 1. ISDN Architecture
 2. ISDN Channels
 3. ISDN Access Interface
4. Network Performance



Transmission Media

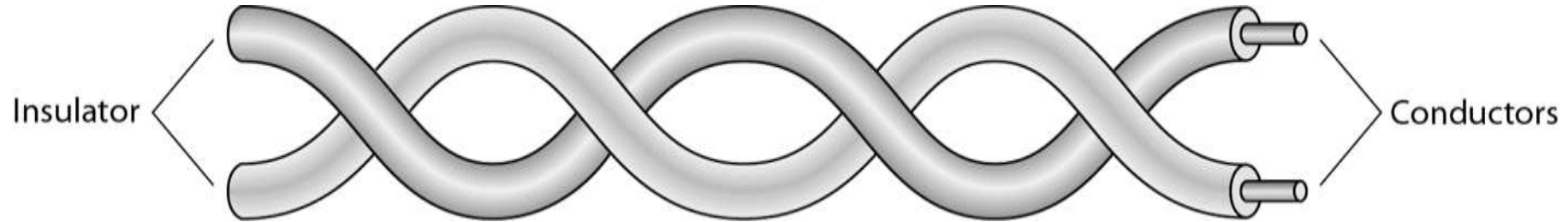
- A transmission medium can be broadly defined as anything that can **carry information** from a **source** to **destination**
- Transmission medium is usually **free space, metallic cable, or fibber-optic cable**
- Information :- Signal that is the result of a conversion of data from another form



Guided Media

- Also called Bounded media/ Wired Media
- Guided media, which are those that provide a conduit from one device to another
 1. Twisted-pair cable
 2. Coaxial cable
 3. Fiber-optic cable
- A signal traveling along any of these media is directed and contained by the **physical limits of the medium**
- Twisted-pair and coaxial cable -- Metallic (copper) conductors -- **signals in the form of electric current**
- Optical fiber -- **transports signals in the form of light**

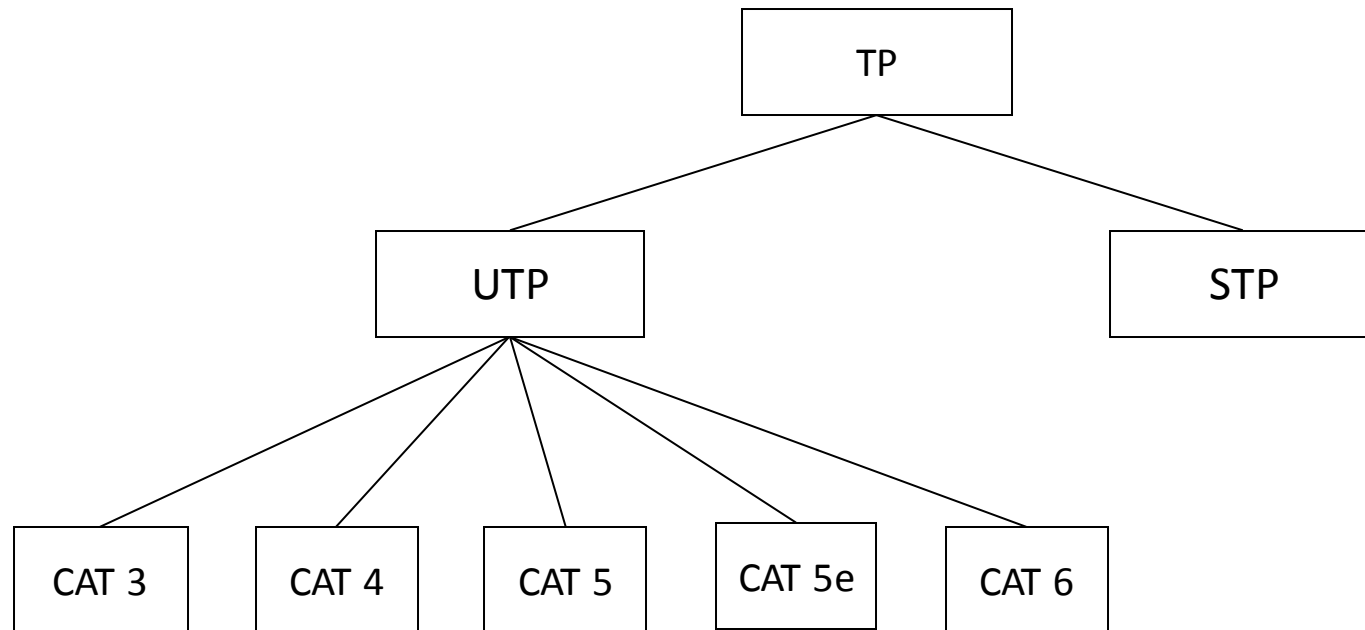
Twisted Pair



- The wires are twisted together in a helical form.
- A twisted pair consists of two insulated copper wires twisted together in a regular spiral pattern
- Twisting tends to decrease crosstalk
- Crosstalk is the interference due to the magnetic field of 2 wires nearby
- Used to transmit both analog and digital transmission

Twisted pair

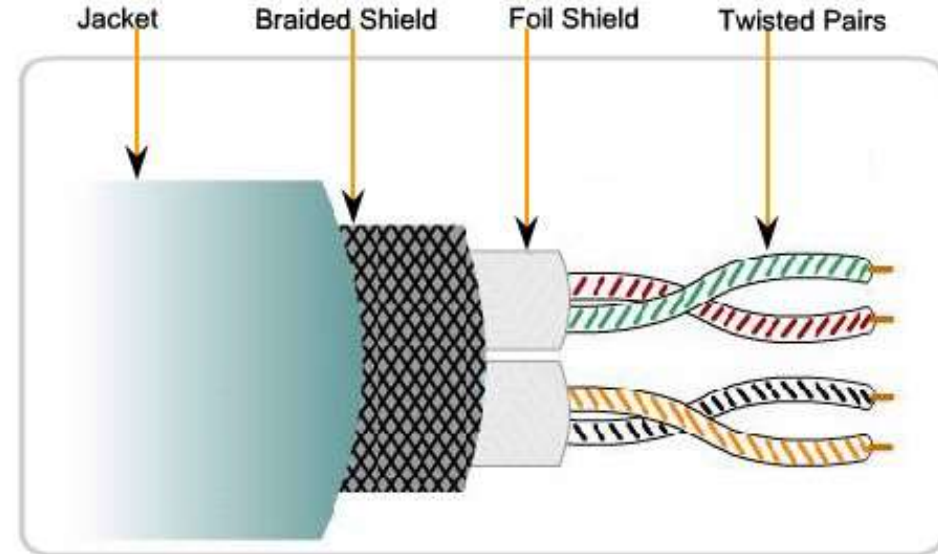
- Twisted pair is limited in distance, bandwidth, and data rate.
- The attenuation for twisted pair is a very strong function of frequency



Shielded Twisted Pair(STP)

- STP uses two or more pairs of wires that are wrapped in an overall metallic braid or foil.
- Shields the entire bundle of wires within the cable as well as the individual wire pairs
- Provides better noise protection
- Higher price

Figure STP Cable



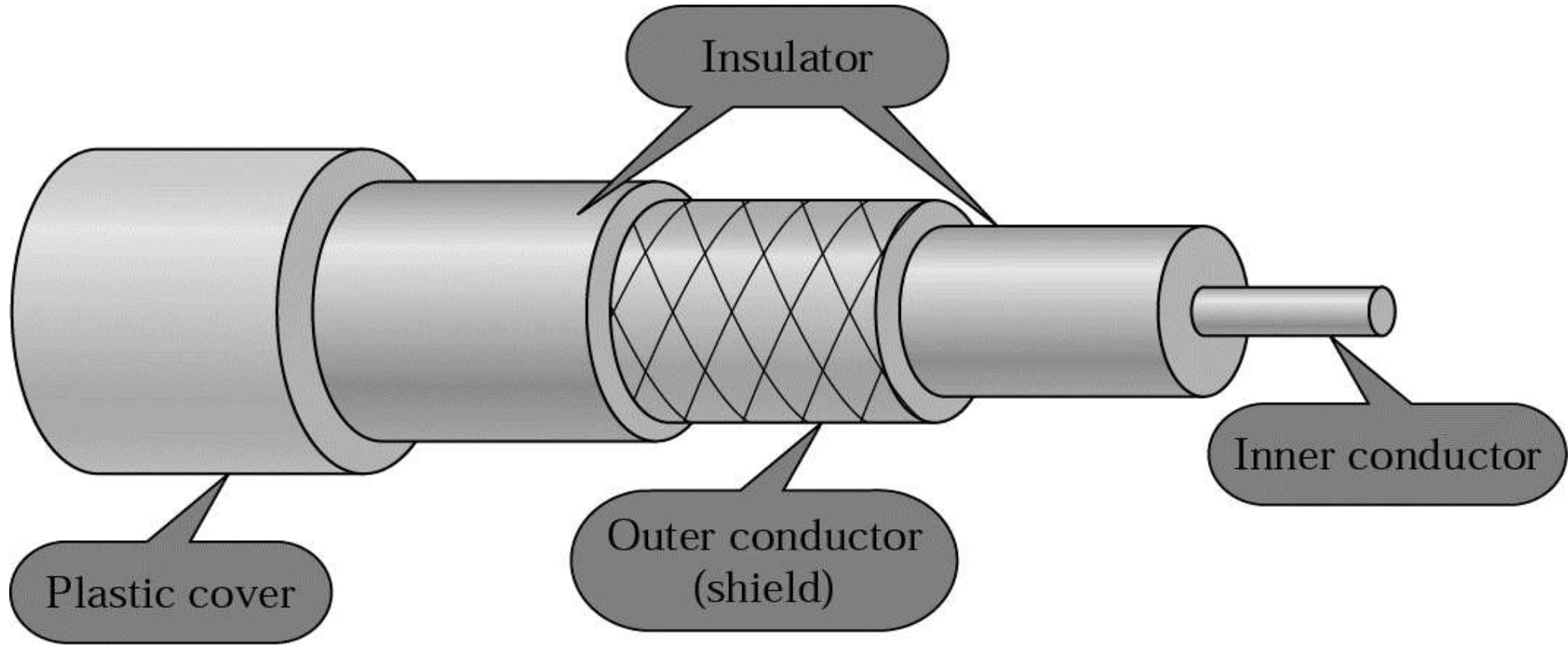
Shielded Twisted Pair(STP)

- More expensive
- Easiest to install
- Harder to handle (thick, heavy)
- Data Rate : 10- 100 Mbps
- Max Cable Length – 100M

Unshielded Twisted Pair(UTP)

- Flexible and cheap cable.
- Category rating based on number of twists per inch and the material used
- CAT 3, CAT 4, CAT 5, Enhanced CAT 5 and now CAT 6.

Co-axil Cable

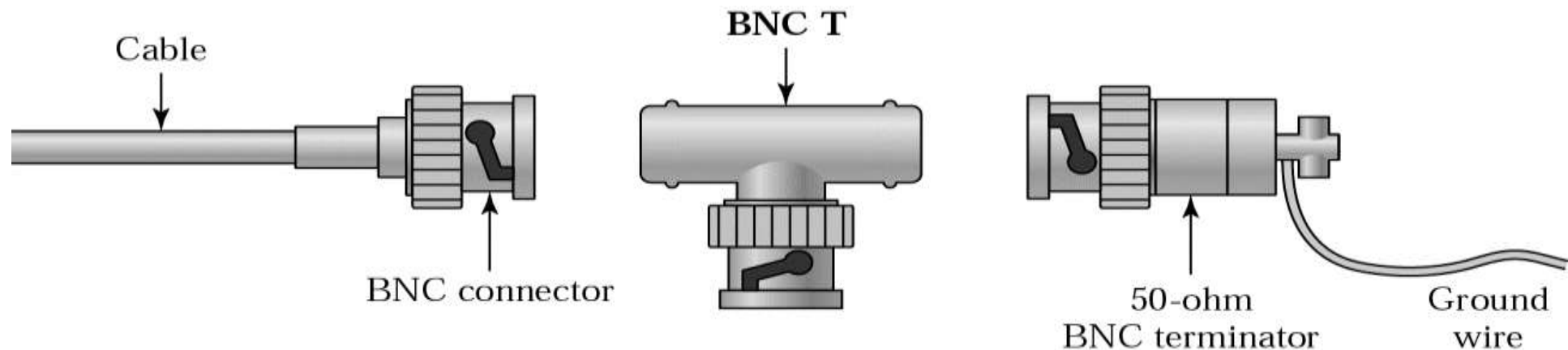


Co-axil Cable

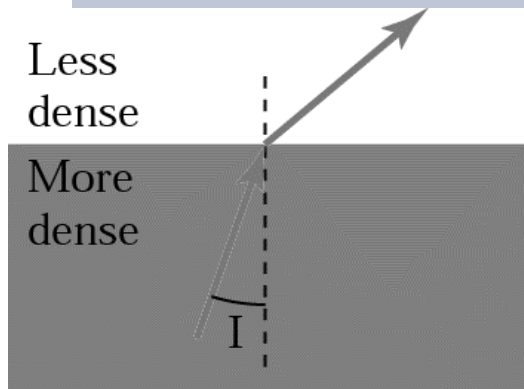
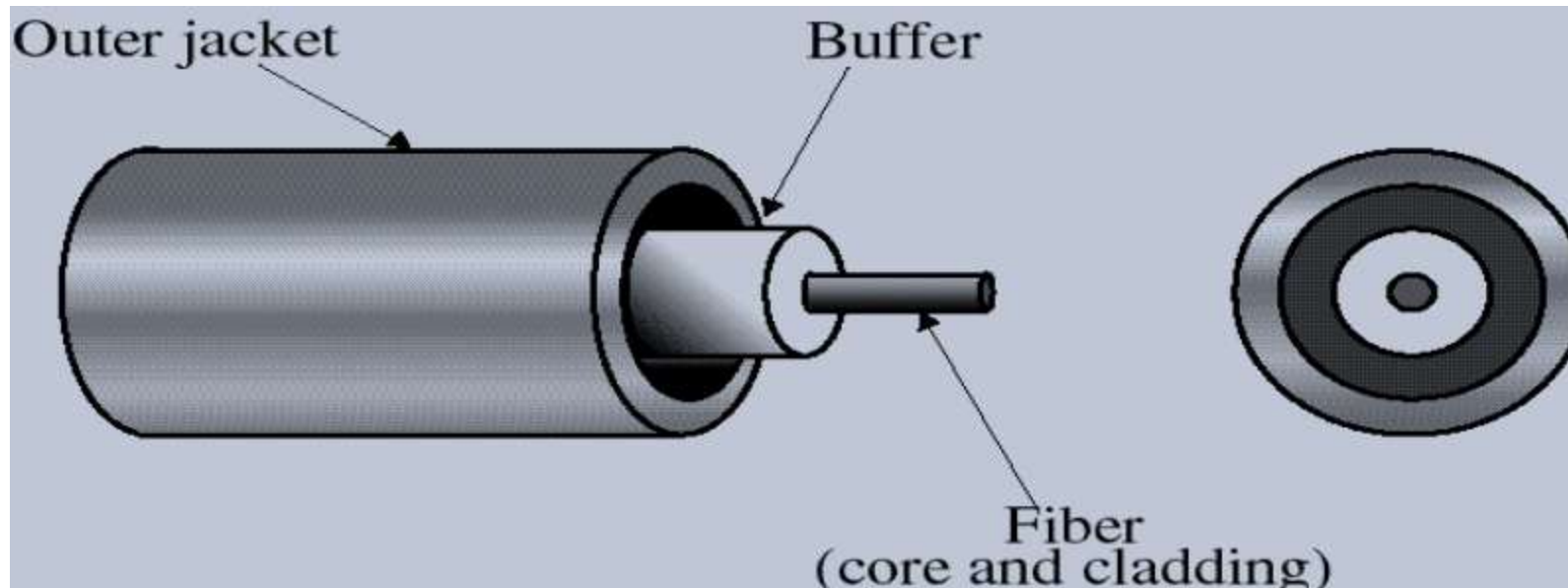
- Both conductors share a common center axial, hence the term “co-axial”
- Coaxial cable consist the followings layers in its construction
 - Copper conductor
 - Insulation layer of plastic foam
 - Second conductor or shield of wire mesh tube or metallic foil
 - Outer jacket of tough plastic
- Coaxial cable can be used over longer distances and support more stations on a shared line than twisted pair
- Coaxial cable is a versatile transmission medium, used in a wide variety of applications, including:
 - Television distribution - aerial to TV systems

Co-axil Cable

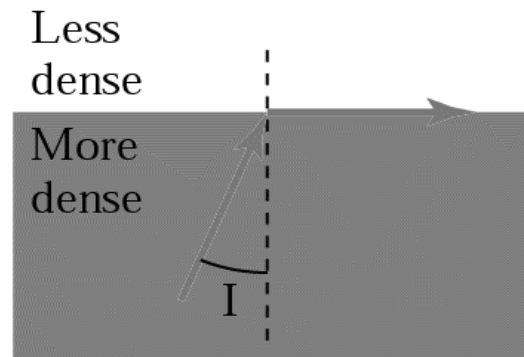
- Characteristics
 - It is comparatively inexpensive
 - Its installation us comparatively simple
 - It must be grounded properly in a network connection
 - Its bandwidth capacity is around 10 Mbps
 - It suffers from data attenuation
- BNC Connectors are used for connecting to co-axial cables



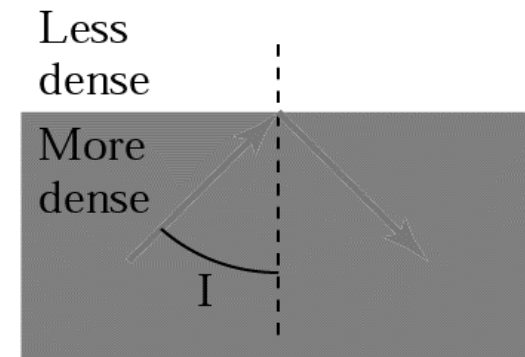
Fibber Optics (Optical Fibber Cable)



$I < \text{critical angle}$,
refraction



$I = \text{critical angle}$,
refraction



$I > \text{critical angle}$,
reflection

Fibber Optics

- Most sophisticated cables used in long distance network connections
- Through this cable data transmission is done through **Light ray signal transmission**
- It has inner core of glass that conducts light
- This inner core is surrounded by cladding
- Cladding is nothing but layer of glass material that reflects light back into the core
- Each fiber is then surrounded by plastic sheath

Optical Fiber - Transmission Characteristics

- Uses total internal reflection to transmit light
 - effectively acts as wave guide for 10^{14} to 10^{15} Hz
- Can use several different light sources
 - Light Emitting Diode (LED)
 - Cheaper, wider operating temp range, lasts longer
 - Injection Laser Diode (ILD)
 - More efficient, has greater data rate
- Relation of wavelength, type & data rate

Optical Fiber Cable

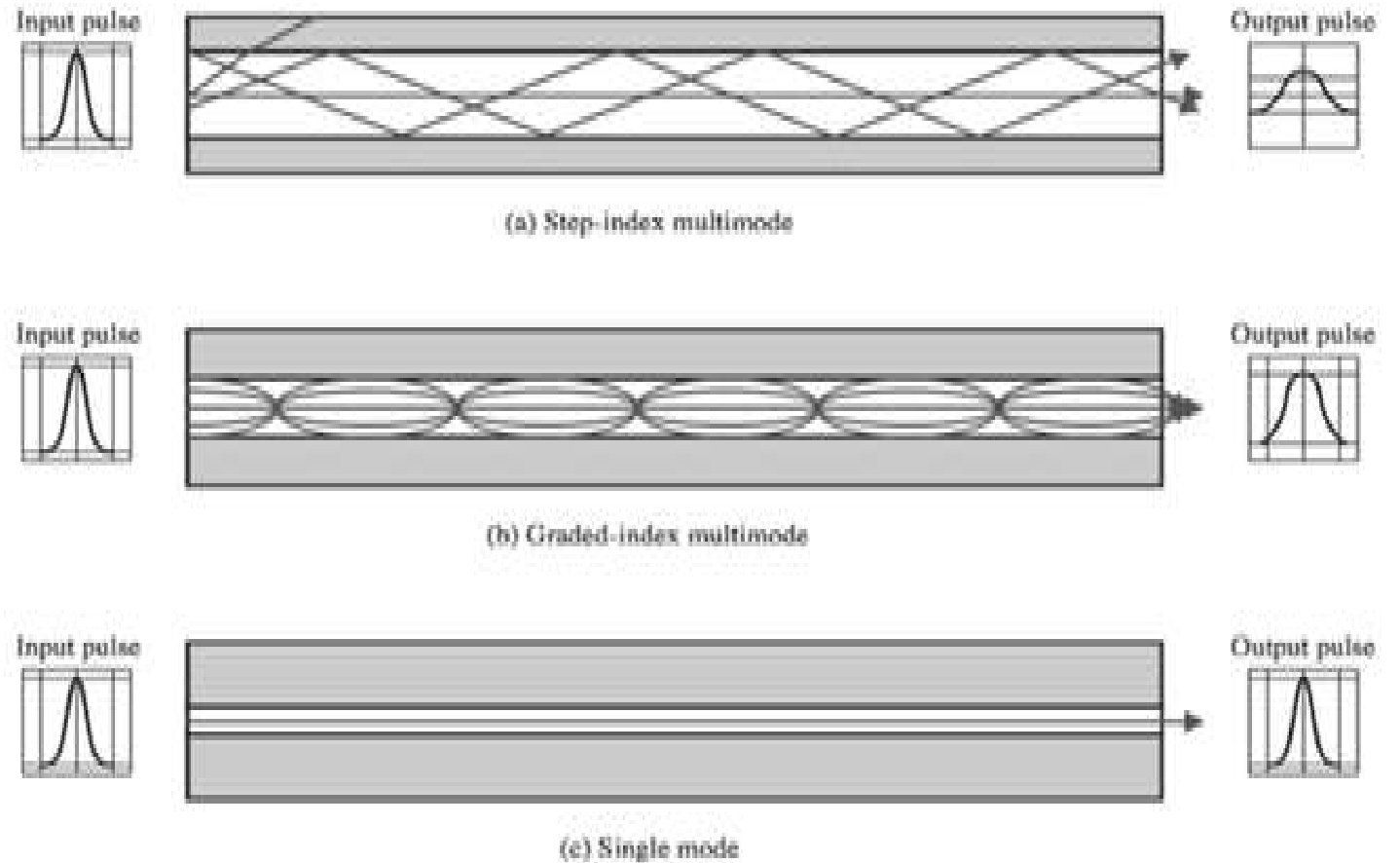
- The bandwidth of the signal produced by the transmitting antenna is more important than the medium in determining transmission characteristics.
1. Optical Fiber – Benefits
 2. greater capacity
 3. data rates of hundreds of Gbps
 4. smaller size & weight
 5. lower attenuation
 6. electromagnetic isolation
 7. greater repeater spacing
 8. 10s of km at least

Optical Fiber Cable Advantages

- **Greater capacity:** Data rates of hundreds of Gbps
- **Smaller size and lighter weight**
- **Electromagnetic isolation**
- **Greater repeater spacing**
- **Lower attenuation**

Optical Fiber Cable Types

- Single Mode
- Multi Mode
 1. Step Index
 2. Graded Index



Unbounded Media(Wireless Media)

- Very useful in difficult terrain where cable laying is not possible
- Provides mobility to communication nodes
- Right of way and cable laying costs can be reduced
- Antenna radiates electromagnetic energy into the medium(air)
- Antenna picks up electromagnetic waves from the surrounding medium

Disadvantages

- Susceptible to rain, atmospheric variations
- Objects in transmission path will reduce the signal strength

Advantages

- **Greater Bandwidth**
- **Low Power Loss**
- **Less Interference**
- **Scalable Size**
- **Safety**
- **Security**
- **Flexibility**

Frequency Bands

Band	Range	Propagation	Application
VLF	3–30 KHz	Ground	Long-range radio navigation
LF	30–300 KHz	Ground	Radio beacons and navigational locators
MF	300 KHz–3 MHz	Sky	AM radio
HF	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF	3–30 GHz	Line-of-sight	Satellite communication
EHF	30–300 GHz	Line-of-sight	Long-range radio navigation

Wireless Technology

Table 6-2 Wireless technologies

wireless technology	transmission distance
Bluetooth	33 feet (10 meters)
WLAN 802.11b	375 feet (112 meters)
WLAN 802.11a	300 feet (90 meters)
WLAN 802.11g	375 feet (112 meters)
Satellite	Worldwide
Fixed broadband	35 miles (56 kilometers)
WAP (cell phones)	Nationwide

Transmission

- Radio Waves 3 KHz to 1 GHz
- Micro Waves 1 GHz to 300 GHz
- Infrared 300 GHz to 400 THz

Infra Red

- Infrared signals have frequencies between 300 GHz to 400 THz.
- They are used for short-range communication.
- Infrared signals have high frequencies and cannot penetrate walls.
- Line of Sight is needed.
- Infrared is used in devices such as the mouse, wireless keyboard and printers.
- Due to its short-range communication system, the use of an infrared communication system in ONE ROOM will not be affected by the use of another system in the next room.

Radio Waves

- Radio waves are normally omnidirectional.
- When an antenna transmits radio waves, they are propagated in all directions
- Sending and receiving antennas do not have to be aligned.
- The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers.
- Our AM and FM radio stations, cordless phones and televisions are examples of multicasting.
- Bluetooth ,Wi-Fi, GSM, CDMA

Bluetooth

- Bluetooth is a wireless technology standard for exchanging data over short distances
- Using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz
- Used from fixed and mobile devices, and building personal area networks (PANs)
- It can connect several devices, overcoming problems of synchronization
- Physical range :Typically less than 10 m, upto 100 m

Wi-Fi (Wireless LAN)

- Wi – Fi (Wireless Fidelity) is a standard that certifies that wireless devices (Wireless LAN) can work together.
- Supports IEEE802.11b or IEEE802.11g or IEEE802.11b/g standard
- Wi - Fi high-speed wireless Internet technology is commonly used in the world.
- Uses radio signals to transmit high speed data over the wireless network with the installation of the Access Point to connect to the device, Such as mobile phones, PDAs and notebook
- Range appx 100M
- Mainly uses 2.4GHz radio waves

GSM

- GSM (Global System for Mobile Communications, originally **G**roupe **S**pécial **M**obile)
- Standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks
- GSM networks operate in a number of different carrier frequency ranges (separated into GSM frequency ranges for 2G and UMTS frequency bands for 3G),
- Most 2G GSM networks operating in the 900 MHz or 1800 MHz bands

Micro Waves

- Electronic waves with frequencies between 1 GHz to 300 GHz are normally called microwaves.
- Microwaves are unidirectional, in which the sending and receiving antennas need to be aligned.
- Microwaves propagation is line-of-sight therefore towers with mounted antennas need to be in direct sight of each other.
- Due to the unidirectional property of microwaves, a pair of antennas can be placed aligned together without interfering with another pair of antennas using the same frequency.
- High-frequency microwaves cannot penetrate walls. This is why receiving antennas cannot be placed inside buildings.

Satellite Communication

- Because **microwave** restrictions on the landscape that affect obscure wave, satellite is introduced
- A communication satellite is, In fact, Satellite is a microwave station.
- It is used to link two or more ground-based microwave transmitter /receivers, known as earth stations, or ground stations
- Implementing such satellite to orbit above the Earth's surface, only three satellites, it can be cover to communicate to all the world
- The satellite receives transmissions on one frequency band (uplink), amplifies or repeats the signal, and transmits it on another frequency (downlink)

Switching Technologies

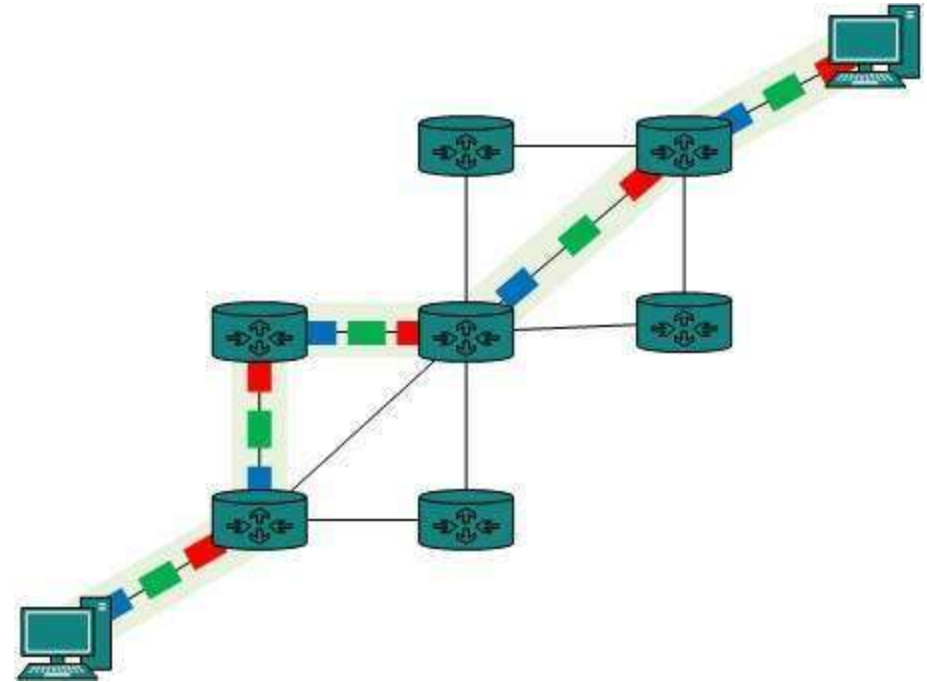
- Switching is process to forward packets coming in from one node to a another leading towards the destination
- Communication system may include number of switches and nodes.
- At broad level, switching can be divided into two major categories:
 1. **Connection Oriented:** Pre-establish circuit along the path between both endpoints
 2. **Connectionless:** No previous handshaking is required and acknowledgements are optional.
- There are 3 main technologies used in Computer Networks
 1. Circuit switching
 2. Message switching
 3. Packet switching

Circuit Switching

- When two nodes communicate with each other over a dedicated communication path, it is called circuit switching (Eg: Telephone Network)
 - Need of pre-specified route from which data will travel and no other data is permitted.
 - In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place
 - Circuits can be permanent or temporary.
 - Applications which use circuit switching may have to go through three phases:
 1. Establish a circuit
 2. Transfer the data
 3. Disconnect the circuit
- ❖ Main disadvantage is Path is blocked for 2 nodes only

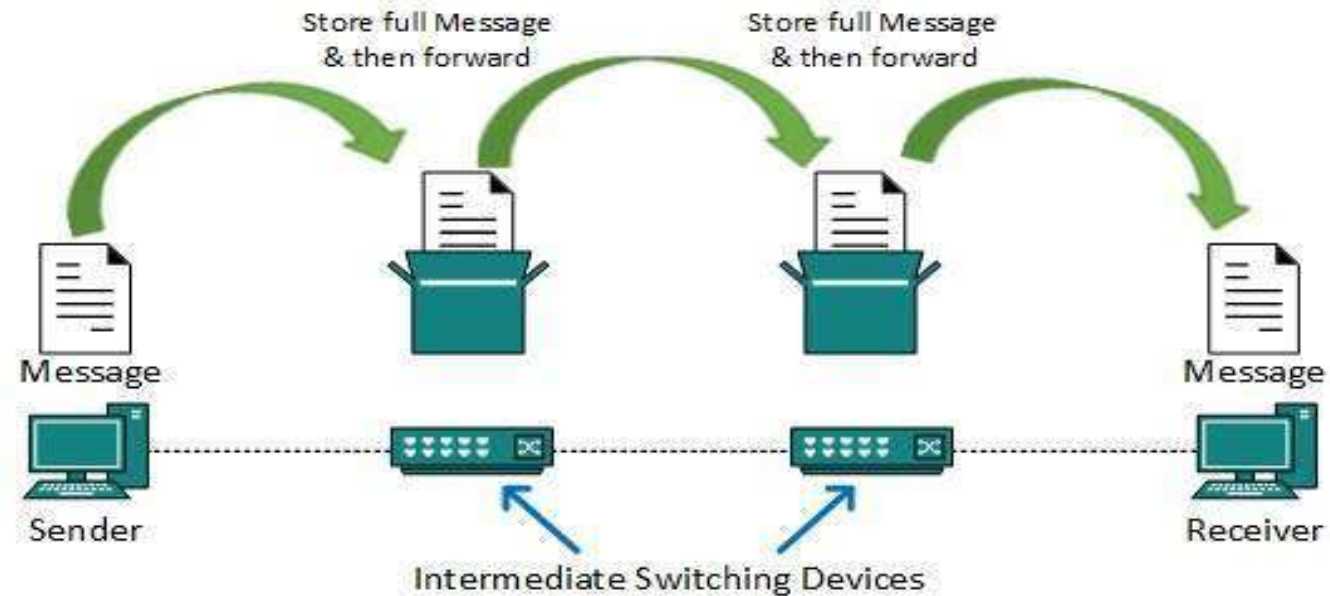
Circuit Switching

- Circuit switching was designed for voice applications.
- Telephone is the best suitable example of circuit switching.
- Before a user can make a call, a virtual path between caller and callee is established over the network.
- In the figure data always passes through same circuit.



Message Switching

- In message switching, the **whole message is treated as a data unit** and is switching / transferred in its entirety.
- This technique was introduced in between circuit switching and packet switch



Message Switching

- A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop.
- If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.

Message Switching

Advantages

1. Channel efficiency can be greater compared to circuit-switched systems, because more devices are sharing the channel.
2. Traffic congestion can be reduced, because messages may be temporarily stored in route.
3. Message priorities can be established due to store-and-forward technique.

Message Switching

Drawbacks:

1. Every switch in transit path needs enough storage to accommodate entire message
2. Because of store-and-forward technique and waits included until resources are available, message switching is very slow
3. Message switching was not a solution for streaming media and real-time applications

Packet Switching

- Shortcomings of message switching gave birth to an idea of packet switching
- Entire message is broken down into smaller chunks called **packets**
- Switching information is added in the **header(source and destination address)** of each packet and transmitted independently
- It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches
- Packet switching can be seen as a solution that tries to combine the **advantages of message and circuit switching and to minimize the disadvantages of both.**

Packet Switching

- Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier
- Internet uses packet switching technique
- Packet switching enables the user to differentiate data streams based on priorities
- Packets are stored and forwarded according to their priority to provide quality of service
- There are two types of packet switching methods:
 1. Virtual circuit
 2. Datagram

Packet Switching - Virtual Circuit

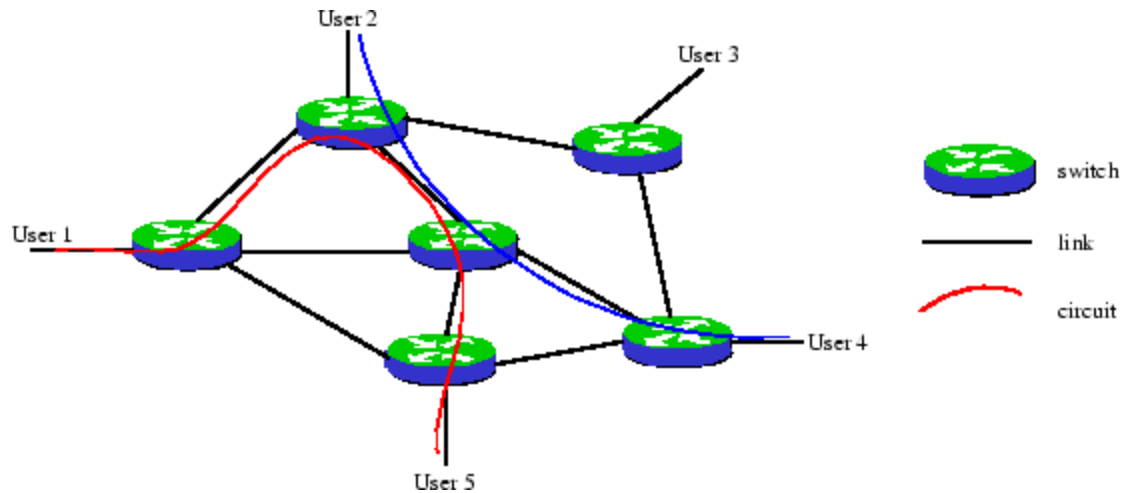
- Virtual circuit switching is a packet switching methodology whereby a logical path is established between the source and destination
- All the packets will go through same path which is called a virtual circuit
- To the user, the connection appears to be a dedicated physical circuit
- Other communications may also be sharing the parts of the same path
- It is connection oriented

Packet Switching - Virtual Circuit

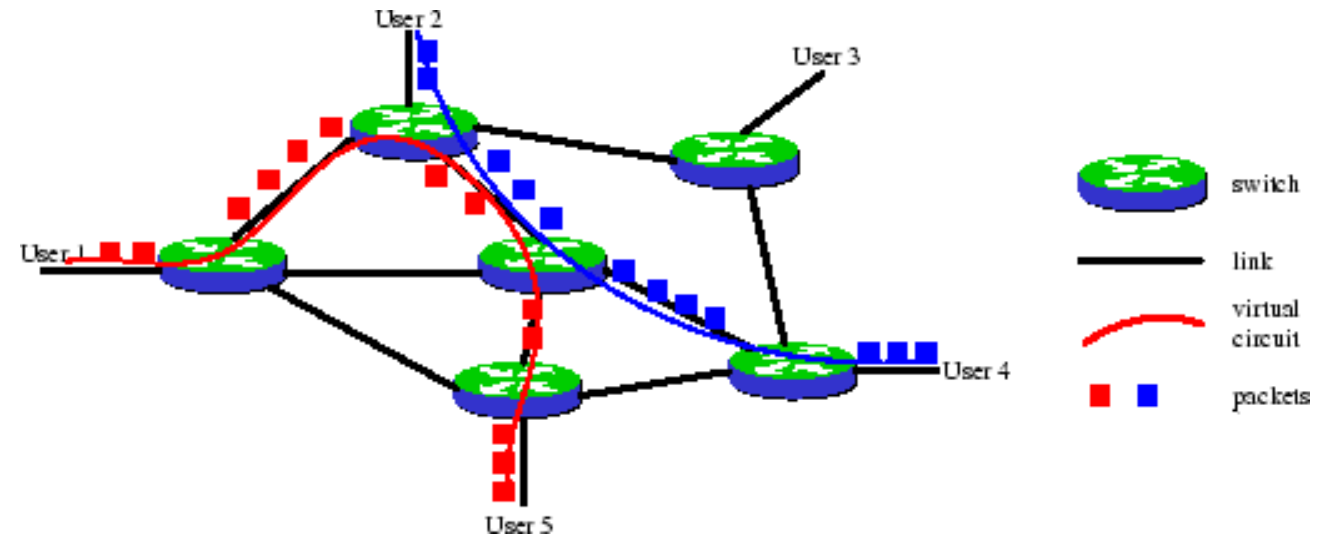
- Before the data transfer begins, the source and destination identify a suitable path for the virtual circuit.
- All intermediate nodes between the two points put an entry of the routing in their routing table for the call
- Additional parameters, such as the maximum packet size, are also exchanged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

Packet Switching - Virtual Circuit

- Virtual Circuit Establishment



- Data Transfer



Packet Switching - Virtual Circuit

Advantages

- Packets are delivered in order, since they all take the same route;
- The overhead in the packets is smaller
- The connection is more reliable

Disadvantages

- The switching equipment needs to be more powerful
- Resilience to the loss of a trunk is more difficult, since if there is a failure all the calls must be dynamically re-established over a different route.

Packet Switching - Datagram

- Datagram packet-switching is a packet switching technology by which each packet, now called a datagram, is treated as a separate entity
- Each packet is routed independently through the network
- Therefore packets contain a header with the full information about the destination
- The intermediate nodes examine the header of a packet and select an appropriate link to another node which is nearer to the destination
- Packets do not follow a pre-established route, and the intermediate nodes do not require prior knowledge of the routes that will be used

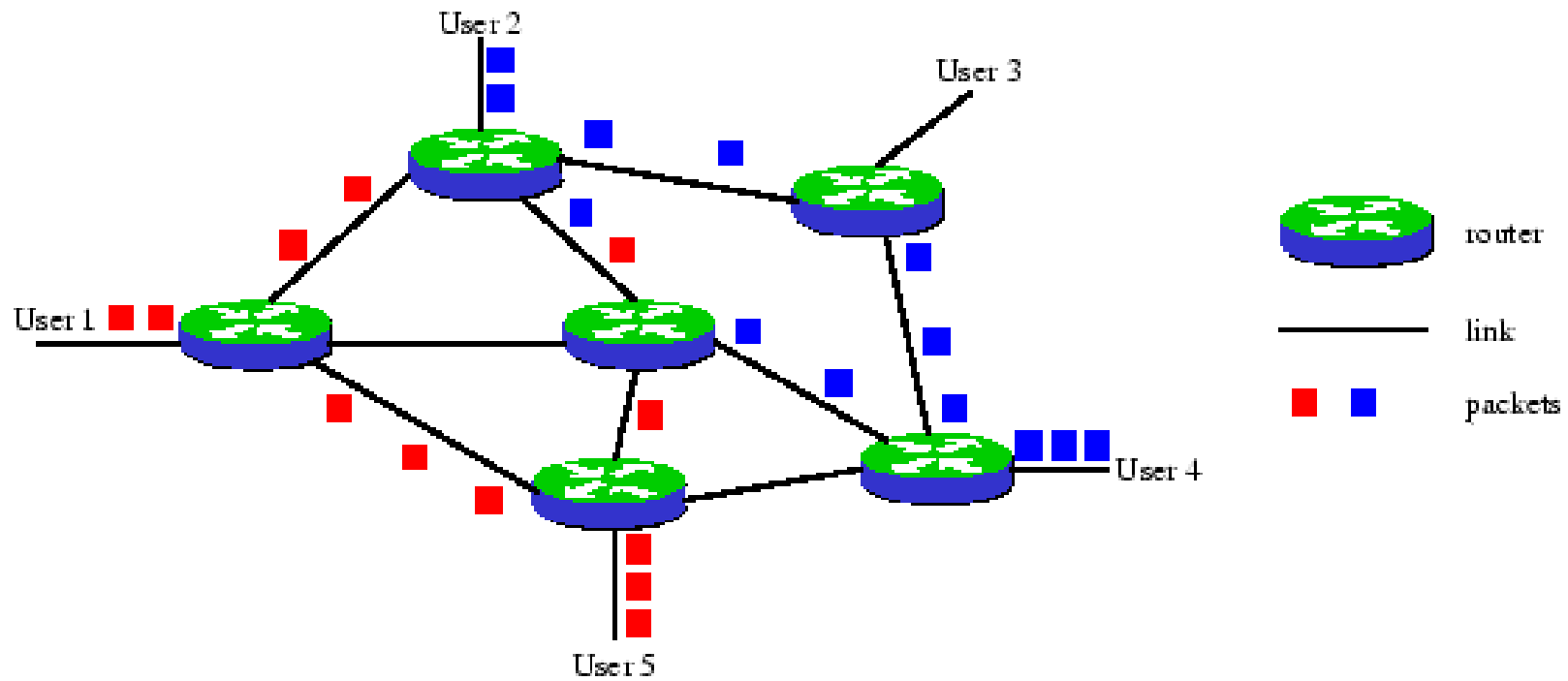
Packet Switching - Datagram

- The individual packets which form a data stream may follow different paths between the source and the destination
- Packets may arrive at the destination out of order
- When this occurs, the packets will have to be reassembled to form the original message.
- Because each packet is switched independently, there is no need for connection setup and no need to dedicate bandwidth in the form of a circuit(Connection less)
- Datagram packet switches use a variety of techniques to forward traffic; they are differentiated by how long it takes the packet to pass through the switch and their ability to filter out corrupted packets.

Packet Switching - Datagram

- A datagram network is a best effort network
- Delivery is not guaranteed
- Reliable delivery must be provided by the end systems (i.e. user's computers) using additional protocols.

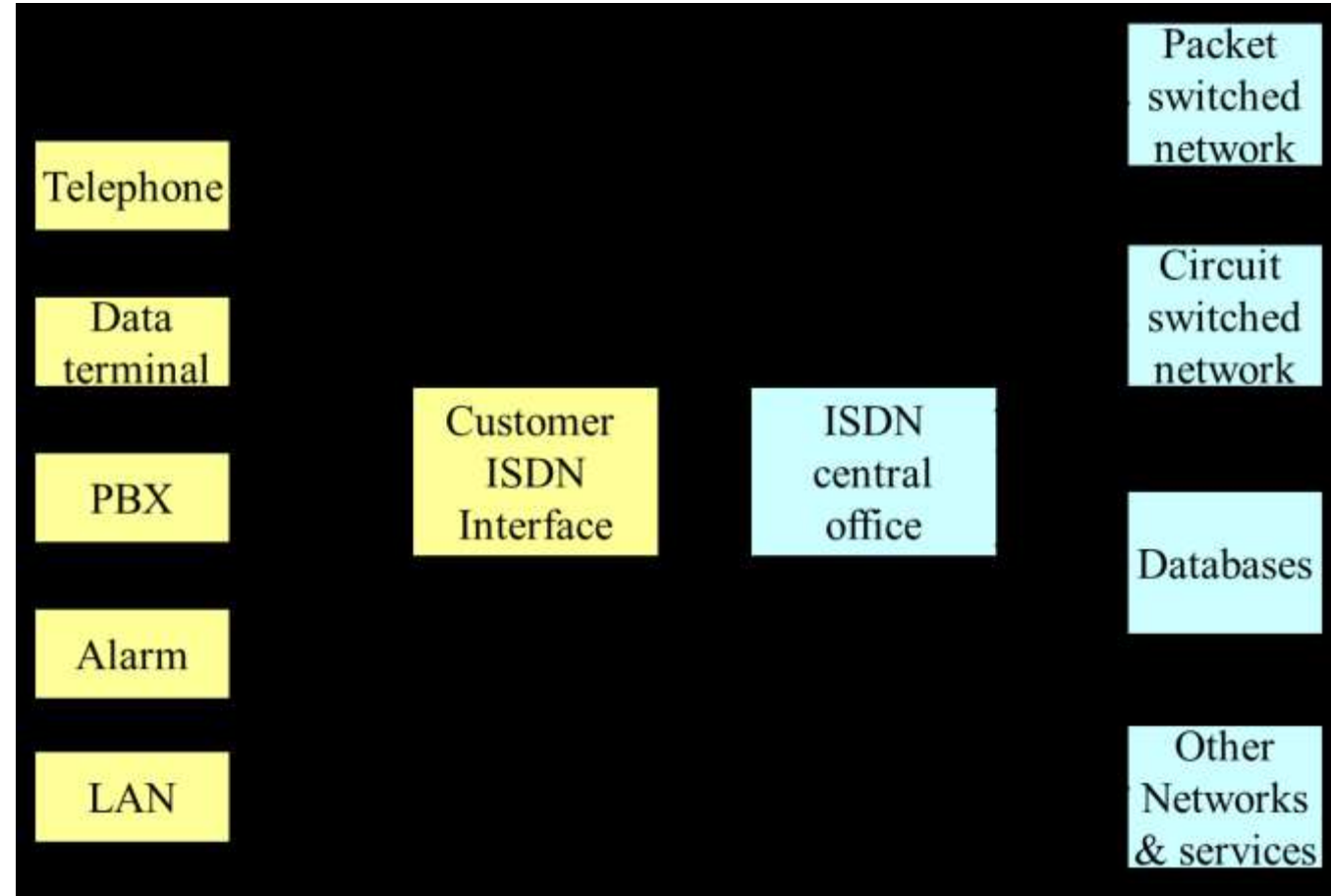
Packet Switching - Datagram



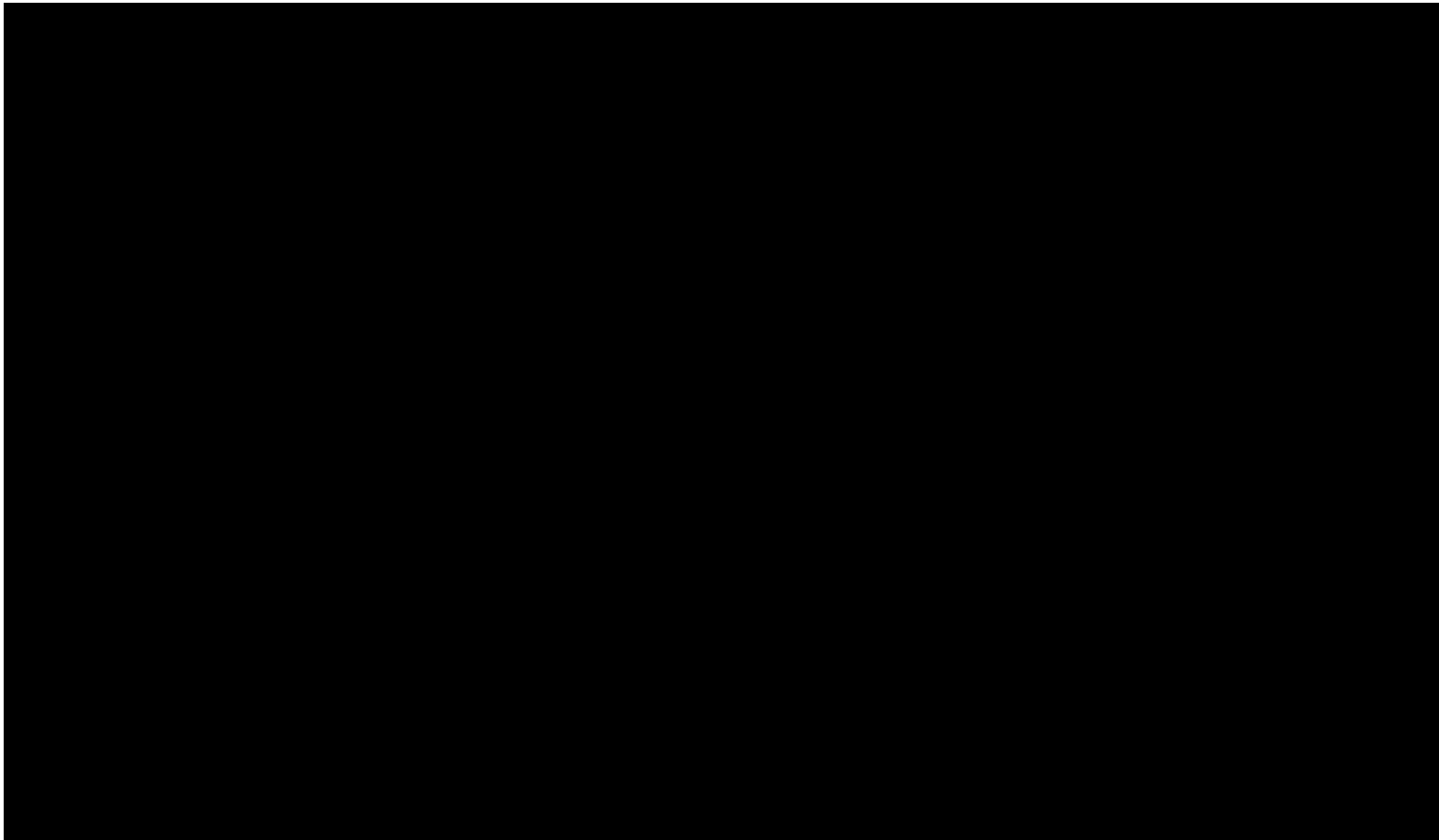
ISDN (Integrated Services Digital Network)

- The Public Switched Telephone network(PSTN) is still analogue from
- The need has arisen to extend the digital network out to subscribers and to provide a single standardised interface to all different users of public networks
- Integrated -> Both transmission and Switching
- Telephone services -> Telecommunication services
- Used for voice, image and data
- In Practice there are multiple networks providing the service nationally , user however sees a single network

ISDN



ISDN Architecture



ISDN Channels

- The Digital pipe is made up of channels - one of three types
 1. B channel
 2. D channel
 3. H channel
- Channels are grouped and offered as a package(Interfaces) to users

B (Basic) Channel

- B channel-64 kbps
- B is basic user channel
 - can carry digital data
 - PCM-encoded voice
 - Mixture of lower rate traffic
- Four kinds of connection possible
 - Circuit-switched
 - Packet-switched (X.25)
 - Frame mode - frame relay (LAPF)
 - Semi permanent - equivalent to a leased line

D Channel

- D Channel - 16 or 64 kbps
- Carries signalling information to control circuit-switched calls on B channels
- Can also be used for packet switching or low-speed telemetry

H Channel

- Carry user information at higher bit rates 384kbps or 1536kbps or 1920kbps
- Can be used as a high-speed trunk
- Can also be subdivided as per user's own TDM scheme
- Uses include high speed data, fast facsimile, video, high-quality audio

ISDN Channel Grouping

- Channels are grouped into 2 accessing modes or interface
 1. Basic Access (Basic Rate Interface)
 2. Primary Access (Primary Rate Interface)

Basic Service / BRI (Basic Rate Interface)

- Management rate: 192 kbps
- Standard throughput: 144 kbps
- Composition: B + B + D channels, Synch & framing
- 2 B Channel -> Information: Voice, Data
- D Channel -> Signaling: Overhead or telemetry, etc.

Primary Service / PRI (Primary Rate Interface)

- Intended for users with greater capacity requirements
- Rate: 1.544/2.048 Mbps
- Composition:
 1. European Standard 2.048 Mbps: 30 B at 64 kbps each & 2 D at 64 kbps
 2. American Standard 1.544 Mbps: 23 B at 64 kbps each & 1 D at 64 kbps
- B Channels -> PCM voice channels
- D Channel -> Signaling

Network Performance (Parameters)

- Bandwidth
- Throughput
- Latency
- Bandwidth- Delay Product
- Jitter

Bandwidth

- Bandwidth is defined as the amount of data that can be transmitted in a fixed amount of time.
- Bandwidth is also defined as a range within a band of frequencies or wavelengths
- For digital devices, the bandwidth is usually expressed in bits per second(bps) or bytes per second
- For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz).

Throughput

- Amount of data transferred from one place to another
- Amount Processed in a specified amount of time
- Data transfer rates for disk drives and networks are measured in terms of throughput.
- Typically, throughputs are measured in kbps, Mbps and Gbps.

Latency

- In networking, the amount of time it takes a packet to travel from source to destination.
- Together, latency and bandwidth define the speed and capacity of a network.

Bandwidth*Delay Product

- The Bandwidth*Delay Product, or BDP for short determines the amount of data that can be in transit in the network.
- It is the product of the available bandwidth and the latency, or RTT.
- BDP is a very important concept in a Window based protocol such as TCP. It plays an especially important role in high-speed / high-latency networks, such as most broadband internet connections.
- It is one of the most important factors of tweaking TCP in order to tune systems to the type of network used.
- $\text{BDP (bits)} = \text{total_available_bandwidth (bits/sec)} \times \text{round_trip_time (sec)}$

Jitter

- Any distortion of a signal or image caused by poor synchronization
- Deviation/Error in normal signal
- In the context of computer networks, jitter is the variation in latency as measured in the variability over time of the packet latency across a network.
- A network with constant latency has no variation (or jitter).
- Packet jitter is expressed as an average of the deviation from the network mean latency. However, for this use
- The standards-based term is "packet delay variation" (PDV).
- PDV is an important quality of service factor in assessment of network performance.

Chapter 4

Data Link Layer

Prepared By R.G.B

Visit For Notes: <http://sites.google.com/site/rohitgbal>

Email: rohitgbal@gmail.com

Contents

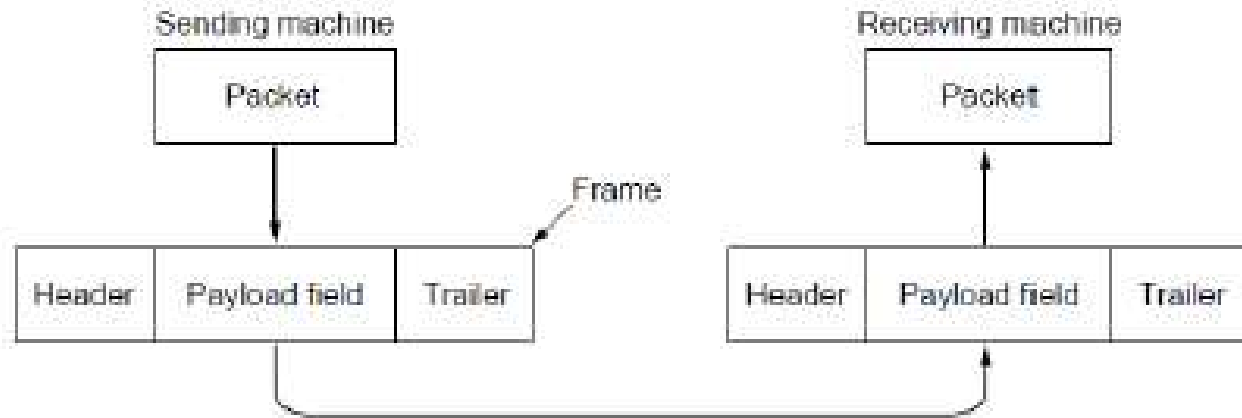
- Sub Layers
 1. LLC
 2. MAC
- MAC Address
- Framing
- Flow Control
 1. Stop and Wait ARQ
 2. Go Back N ARQ
 3. Selective Repeat ARQ
- Error Control Mechanisms
 1. Error Detection
 2. Error Correction
- Channel (Multiple) Access
 1. ALOHA
 2. CSMA
- IEEE 802 Standards
- Virtual Circuit Switching
 1. Frame Relay
 2. ATM
 3. X.25

1.Data Link Layer

- Functions of the data link layer include:
- Providing a well-defined service interface to the network layer (framing)
- Dealing with transmission errors (error control)
- Regulating the flow of data so that slow receivers are not swamped by fast senders (flow control)

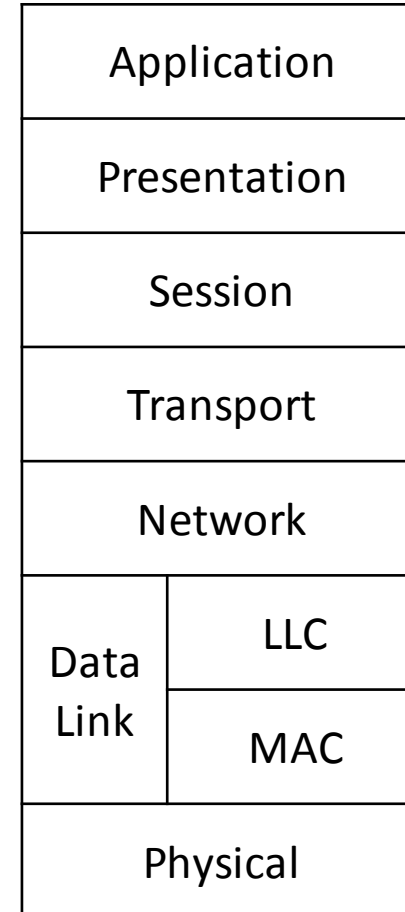
1. Data Link Layer

- To accomplish these goals, packets from the network layers are encapsulated into frames (See Figure Given Below):



1.1 Data Link Sub Layers

- Data link layer is divided into 2 sublayers
 1. MAC (Media Access Control)
 2. LLC (Logical Link Control)



1.1 Link Sub Layers

1. MAC

- MAC sub layer directly interact with lower layer i.e. Physical layer
- Framing is done in MAC sub layer
- Framing done with help of MAC address

2. LLC

- LLC sub layer directly interact with upper layer i.e. network layer
- Error Control and Flow control is done in LLC sublayer

2 MAC Address

- **Media Access Control (MAC address)**, also called **physical address**, is a unique identifier assigned to network interfaces for communications on the physical network segment
- It is used in data link layer communication
- If devices are in same network (LAN) MAC address is used for communication
- MAC address is 48 bit in length i.e. 6 Bytes(Octets)
- It represented using Hexa-decimal Values (6 groups)
- Example : F1-23-45-67-89-AB

2 MAC Address

- First 3 bytes is assigned to specific Organization

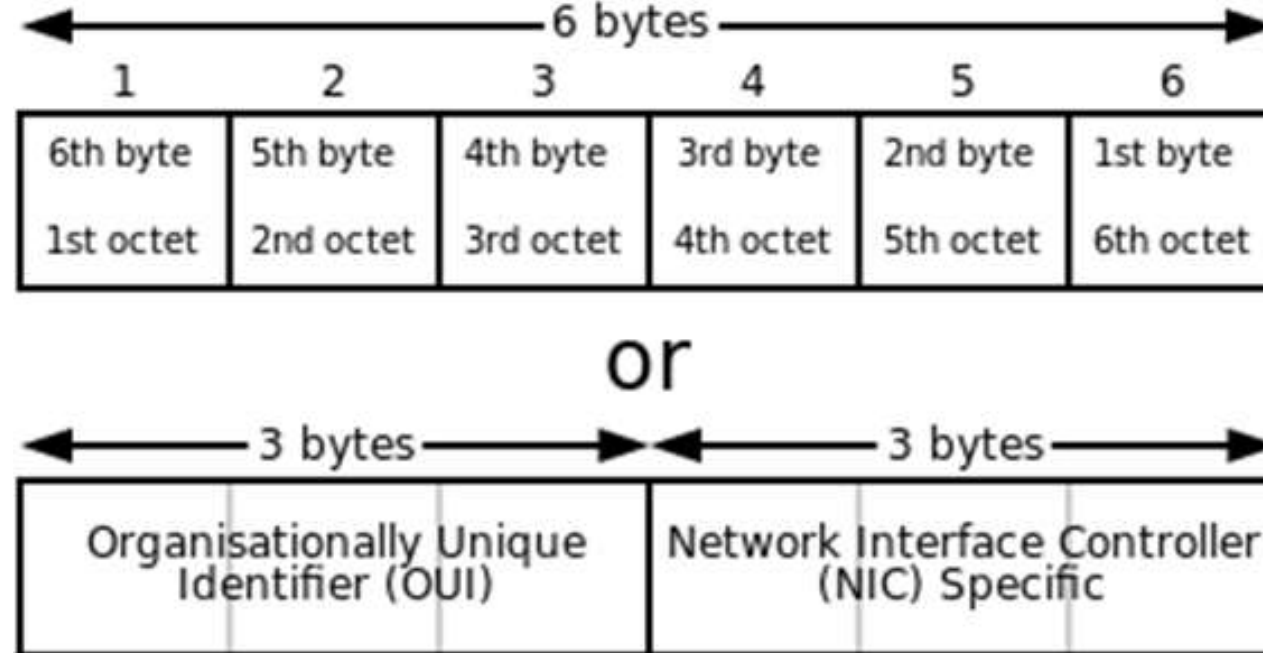


Figure : MAC Address Format

3 Framing

- Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination
- The physical layer provides bit synchronization to ensure that the sender and receiver use the same bit durations and timing
- The data link layer, on the other hand, **needs to pack bits into frames**, so that **each frame is distinguishable from another**
- Framing in the data link layer **separates a message from one source to a destination, or from other messages to other destinations**, by adding a sender address and a destination address

3 Framing

- The **destination address** defines **where the packet is to go**; the **sender address** helps the **recipient acknowledge the receipt**
- **Frames are of 2 types**
 1. **Fixed Size**
 2. **Variable**

3.1 Fixed size frame

- Fixed size frames all frames a have same size
- No need for defining frame boundary
- Size itself can be used as a delimiter
- Fixed type of framing is used ATM network
- ATM frame size is 53 bytes (48 for payload +5 for header)

3.2 Variable frame size

- Size of each frames will be different sizes
- In variable-size framing, **Start of frame and end of frame** (i.e. frame boundary) has to be defined
- Two approaches were used for this purpose defining frame boundary:
 1. Character(Byte) -oriented approach
 2. Bit-oriented approach

Header	Payload	Trailer	Header	Payload	Trailer
Frame 1			Frame 2		

Figure : Frame Format in Variable Size frame

3.2.1 Character (Byte)- Oriented

- Data to be carried are 8-bit characters from a coding system such as ASCII



Figure : Frame in Character Oriented Protocol

- In character oriented protocols, a frame starts with synchronization characters (one or more)
- SYN- Synchronization Idle Character (Usually coded as 0x16)
- SOH- Start of Header(means Start of frame information)

3.2.1 Character (Byte)- Oriented

- STX - Start of Text(Means start of data)
- ETX - End of Text
- ETB - End of Transmission Block
 - If Multiple Frames are send ETB is used in intermediate frames and ETX at the last frame
- BCC – Binary Check Character (for error detection)
- DLE – Data Link Escape(Escape Character/ Flag/ Delimiter)
 - If the DLE character appears in the data field it must be replaced by the sequence DLE DLE (Known as **Character stuffing**)

NB :Character Stuffing Section is explained in next slide

3.2.1.1 Character(Byte) Stuffing

- If the DLE(Escape) character appears in the data field it must be replaced by the sequence DLE DLE This Known as **Character stuffing or Byte Stuffing**
- This creates another problem. What happens if the text contains one or more escape characters followed by a flag?
- The receiver removes the escape character, but keeps the flag, which is incorrectly interpreted as the end of the frame
- To solve this problem, the escape characters that are part of the text must also be marked by another escape character.

- In other words, if the escape character is part of the text, an extra Escape Character is added to show that the second one is part of the text

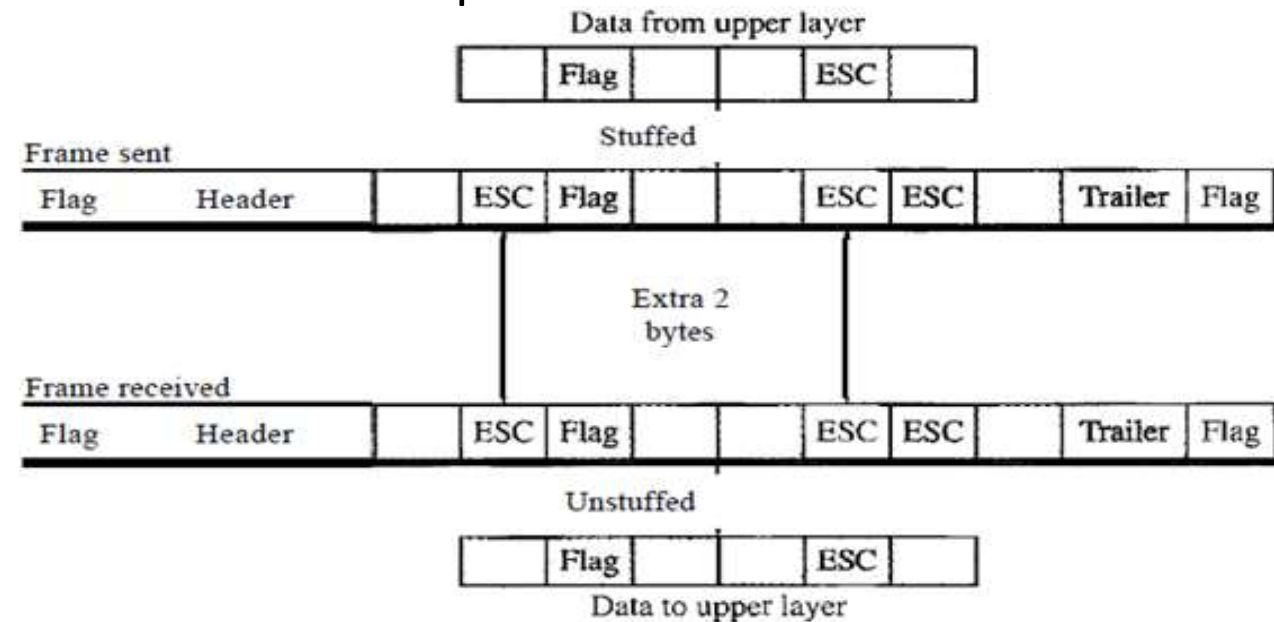


Figure : Byte Stuffing (Sender) and Un-stuffing (Receiver)

3.2.2 Bit Oriented Protocol

- Frame is a collection of bit
- In a bit-oriented protocol, the data section of a frame is a sequence of bits to be interpreted by upper layer data(Text, video, audio, etc..)
- Each frame have **Address, control, data, FCS and Delimiter(Flag)**

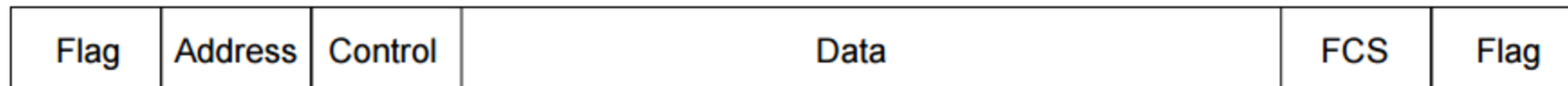


Figure 3 : Frame in Bit Oriented Protocol

- Flag (Delimiter)
 - Used to mark start and end of frame(usually 8 bit pattern flag 01111110)
 - One flag is used to separate end and start of next frame if they are contiguous

3.2.2 Bit Oriented Protocol

- **Address** field indicates source and destination address
- **Control** field indicates type or length of frame
- **FCS (Frame Check Sequence)** : For error detection
- **Bit Stuffing**: is the process of adding one extra 0 whenever there is 5 consecutive 1's in frame , so that the receiver does not mistake the pattern 0111110 for a flag.

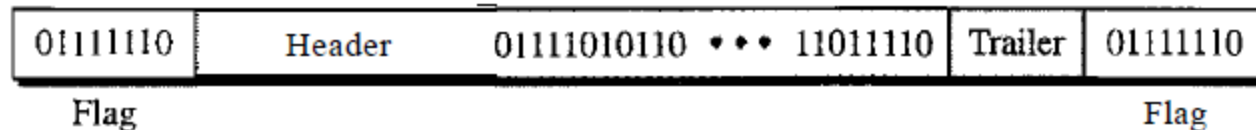


Figure 5 : Bit Oriented Frame with data field having 01111110 pattern flag

3.2.2.1 Bit stuffing

- Each frame begins and ends with a special bit pattern called a flag byte [01111110]
- Whenever sender data link layer encounters *five consecutive 1's* in the data stream, it automatically stuffs a 0 bit into the outgoing stream
- When the receiver sees *five consecutive incoming 1's followed by a 0 bit*, it automatically destuffs the 0 bit before sending the data to the network layer

3.2.2.1 Bit stuffing

0110111111001111011111111100000

Figure : Original Data in sender

0110111110110011110011111011111000000

Stuffed bits

Figure: Data sent to receiver after stuffing

0110111111001111011111111100000

Figure: Data un stuffed after receiving

3.3 Frame format

Preamble(7)	SFD(1)	Destination Address(6)	Source Address(6)	Type/ Length (2)	Data And Padding	CRC (4)
-------------	--------	------------------------	-------------------	------------------	------------------	---------

Figure : Frame format (Numbers in each field indicates size in bytes)

- Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium
- Acknowledgments must be implemented at the higher layers
- The Ethernet frame contains seven fields as shown in figure

NB : Explanation of Each field is given in next page

3.3.1 Frame format- Preamble

- The first field of frame contains 7 bytes (56 bits)
- Alternating 0's and 1's that alerts the receiving system to the coming frame and enables it to synchronize its input timing

01

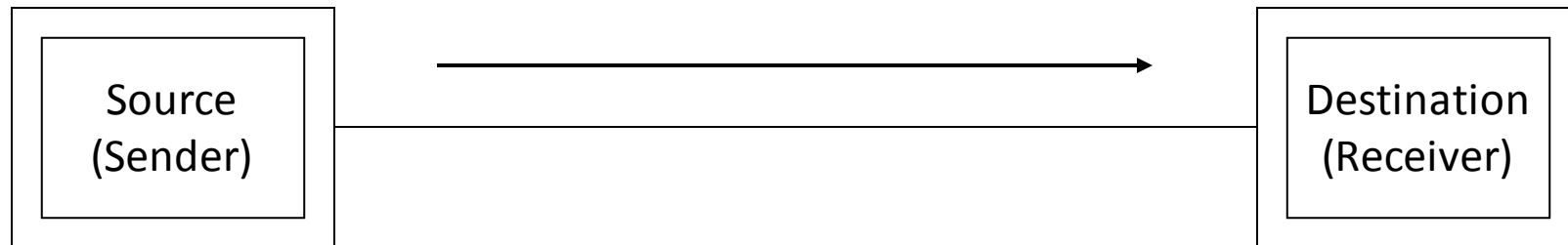
- The pattern provides only an alert and a timing pulse
- The 56-bit pattern allows the stations to miss some bits at the beginning of the frame
- The preamble is actually added at the physical layer and is not (formally) part of the frame.

3.3.2 Frame format- SFD

- The second field is Start Frame Delimiter(SFD) is of 1 byte
- 10101011 (8 bits)
- signals the beginning of the frame
- The SFD warns the station or stations that this is the last chance for synchronization
- The last 2 bits alerts the receiver that the next field is the destination address

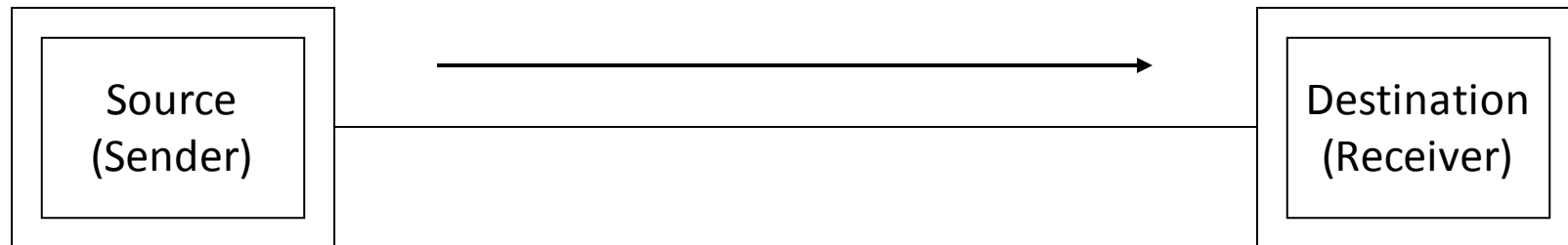
3.3.3 Frame format- Destination Address

- The DA field is 6 bytes
- It contains the physical address(MAC) of the destination station or stations to receive the packet



3.3.4 Frame format- Source Address

- The SA field is 6 bytes
- It contains the physical address(MAC) of the source station or stations to receive the packet

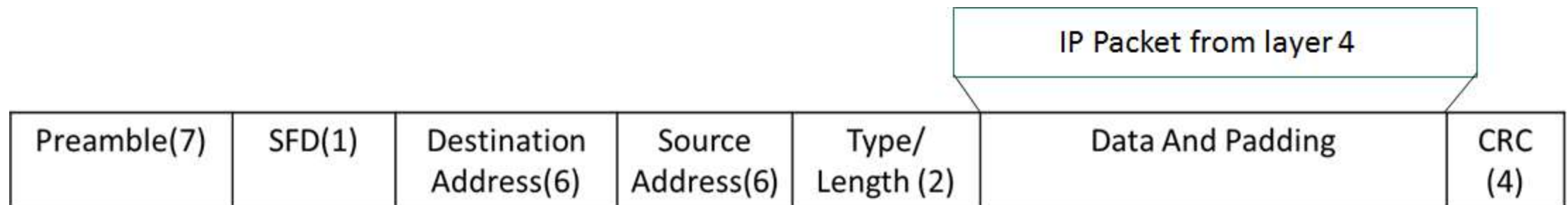


3.3.5 Frame format- Type/Length

- This field is defined as a type field or length field.
- The original Ethernet used this field as the **type field to define the upper-layer protocol using the MAC frame.**
- The IEEE standard used it as the **length field to define the number of bytes in the data field**

3.3.6 Frame format- Data and Padding

- This field carries data encapsulated from the upper-layer protocols.
- It is a minimum of 46 and a maximum of 1500 bytes, as we will see later
- If upper layer data is less than 46 byte add 0's
- used to insure data is minimum 46 bytes.



3.3.7 Frame format- CRC

- CRC- Cyclic Redundancy Checking
- For Error control
- It is 4 bytes

4 Error Control

- Error is corruption (change) in bit / bits due to noise, signal distortion or attenuation in the media
- If errors do occur, then some of the bits will either change from 0 to 1 or from 1 to 0
- There are 2 types of error
 1. **Bit error** : Only one bit is corrupted in data
 2. **Burst error**: More than one bits are corrupted in data
- Error Control allows the **receiver to inform the sender** of any frames lost or damaged in transmission and coordinates the **retransmission** of those frames by the sender

4 Error Control

2 ways of error control

1. FEC(Forward Error Correction)
2. ARQ(Automatic Repeat reQuest)

1. FEC

- FEC is accomplished by adding redundancy to the transmitted information using a predetermined algorithm
- Each redundant bit is invariably a complex function of many original information bits

4 Error Control

1. ARQ

- Receiver detects transmission errors in a message and automatically requests a retransmission from the transmitter
- When the transmitter receives the ARQ, the transmitter retransmits the message until it is either correctly received or the error persists beyond a predetermined number of retransmissions (*usually 15*)
- A few types of ARQ protocols are Stop-and-wait ARQ, Go-Back-N ARQ and Selective Repeat ARQ (*We will discuss in Flow control*)

4 Error Control

- Error control is divided into 2 categories
 1. **Error detection**
 2. **Error correction**
- **Error Detection:** It allows a receiver to check whether received data has been corrupted during transmission. If corrupted it can check for retransmission (*Example: Parity Checking and CRC*)
- **Error Correction:** It allows a receiver check for error and to reconstruct the original information when it has been corrupted during transmission (*Example : Hamming code*)

4.1 Error Detection

- It allows a receiver to check whether received data has been corrupted during transmission
- If corrupted it can check for retransmission
- Here ARQ is used for Error correction
- *Error Detection Mechanism*
 1. *Parity Checking (Bit error checking)*
 2. *CRC(Burst error checking)*
 3. *Checksum (Burst error checking)*

4.1.1 Parity Checking

- The simplest error-detection scheme is to append a parity bit to the end of a block of data
- Value of parity bit is selected so that the character has an even number of 1s (even parity) or an odd number of 1s (odd parity)

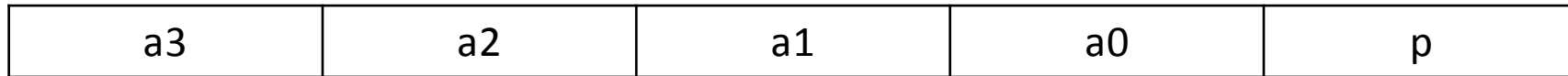
Data Bits (n)	Parity bit(1)
Message to be Sent = Data + Parity (total n+1 bits)	

Figure : Parity Message format

- Parity can detect odd numbers of errors only.

4.1.1 Parity Checking

- Consider parity encoding scheme with 4 bit data and bit parity
- Code word = data + parity (5 bit)



- Parity bit is calculate with the help modulo 2 arithmetic

$p = a_3 \text{ XOR } a_2 \text{ XOR } a_1 \text{ XOR } a_0 \text{ (modulo 2 method)}$
--

- Here even parity is used
- If data bits have odd number of 1's then parity bit will be 1
- If data bits have even number of 1's then parity bit will be 0

4.1.1 Parity Checking

Example Scenario

- Consider message 1010 (4 bit)
- Parity bit p is calculating using **XORing** (modulo 2 method)
- Transmitter will append parity bit (0 because of even number of 0's)
- Code word 10100 is send through medium to receiver(message + parity bit , total 5 bits)
- Receiver will check received data and do **XORing** (modulo 2 arithmetic) and compare the result with parity bit
- If parity bit in code word and **XORing** in receiver matches **NO ERROR**

4.1.2 CRC

- CRC (Cyclic Redundancy Checking)
- CRC is based on polynomial
- Sender and receiver have to choose a common polynomial for checking error
- Instead of one parity bit here **R parity bits** are used for error checking
- The **value of R** is determined by the degree of polynomial selected
- Data word(N bits) + parity word(R bits) = code word (K bits)

4.1.2 CRC

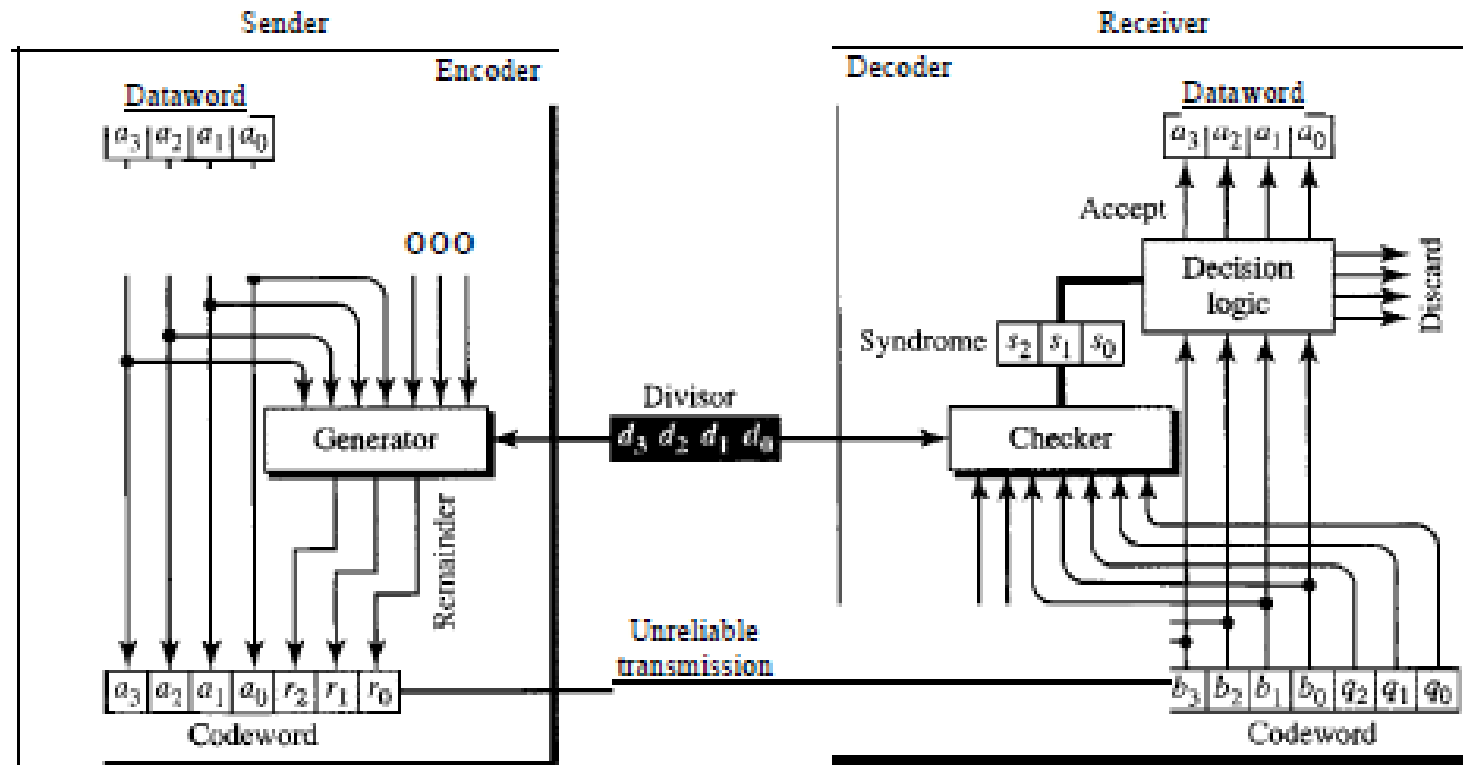


Figure : CRC Encoder/Decoder

4.1.2.1 CRC – Encoder (Sender)

- Consider
- Data word(message) =1001 (4 bit)
- Polynomial = x^3+x+1 (i.e. in binary representation 1011)
- The above polynomial is of degree 3 (so 3 parity bit is used)
- Code word (k)= 7 bit in total
- Code word is generated with help of data bit and polynomial

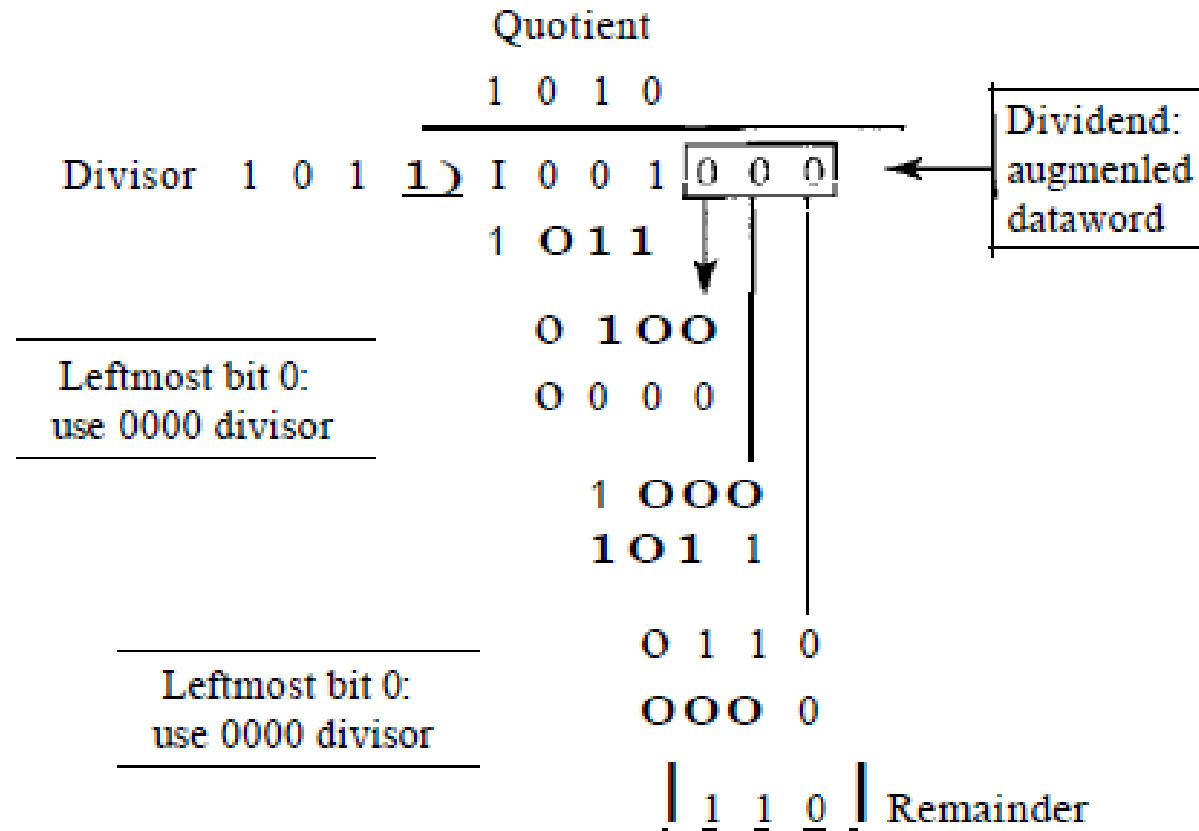
4.1.2.1 CRC – Encoder (Sender)

Steps in encoder

1. First add R bits of 0's in the with the data word
2. 1001 is data word and 3 0's augmented(added) so 1001000 is generated
3. 1001000 is called augmented data word
4. 1001000 is divided with the polynomial bits i.e. 1011(divisor)
5. 110 is obtained as reminder and quotient is discarded
6. 110 is augmented with data bits i.e. 1001 to create code word i.e. 1001110
7. Code word is sent through the transmission media

NB: Division is shown in next page

4.1.2.1 CRC – Encoder (Sender)



4.1.2.1 CRC – Decoder (Receiver)

- Received Code word(message + parity) =1001110 (7 bit)
- Have same Polynomial = x^3+x+1 (i.e. in binary representation 1011)
- The above polynomial is of degree 3 (so 3 parity bit is used)
- Receiver will check for error by doing division with the code word received and polynomial as divisor
- If the remainder is 000 then there is no error in transmission else there is error in transmission.

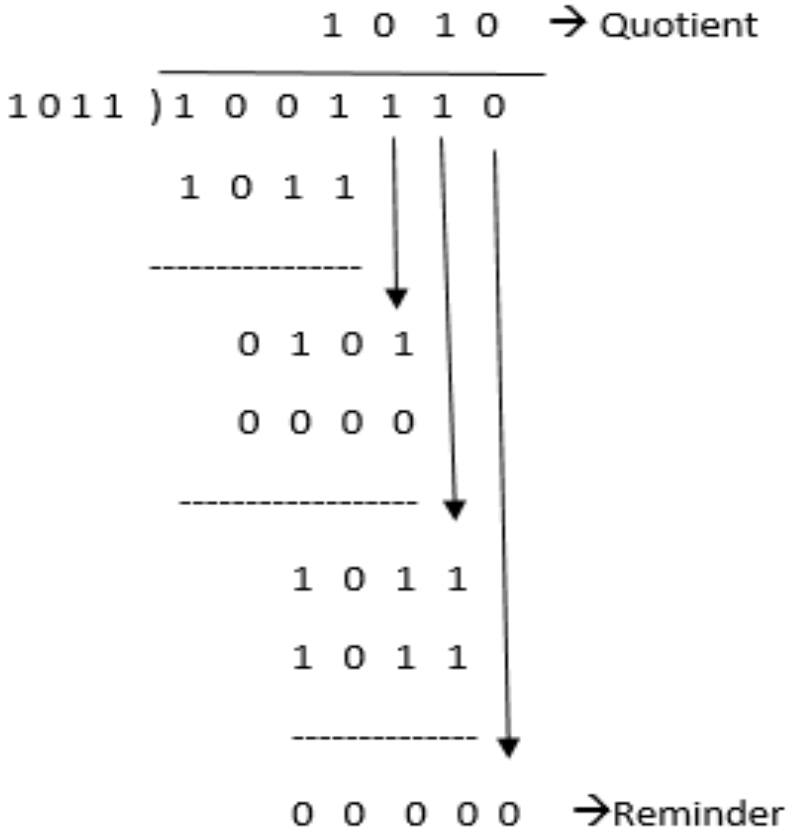
4.1.2.1 CRC – Decoder (Receiver)

Steps in Decoder.

1. Code word (1001110) is received through the transmission media
2. First divide (binary modulo 2 division) the code word the polynomial bits i.e. 1011(divisor)
3. After division discard the quotient and take remainder only
4. If remainder is 000 then there is no error in transmission

NB : Division is shown in next page

4.1.2.1 CRC – Decoder (Receiver)



4.2. Error Correction Codes

- It allows a receiver check for error and to reconstruct the original information when it has been corrupted during transmission
- It is also called FEC (Forward Error Correction)
- Hamming Code is Error correction code
- Error correction done with help of Hamming Distance

4.2.1. Hamming Distance

- Given any two code words that may be transmitted or received—say, 10001001 and 10110001 respectively
- To determine how many bits differ(error), just XOR the two code words and count the number of 1 bits in the result

1 0 0 0 1 0 0 1 XOR

1 0 1 1 0 0 0 1

0 0 1 1 1 0 0 0 → Here 3 bits One So 3 error bits(Hamming Distance = 3)

4.2.2. Minimum Hamming Distance

- The minimum Hamming distance is the smallest Hamming distance between all possible pairs in a set of words
- First find all distances and find the minimum distance
- For 2 bit word all possible combinations are (00,01,10,11)

$$d(00,01)=1 \quad d(00,10)=1 \quad d(00,11)=2$$

$$d(01,10)=2 \quad d(01,11)=1 \quad d(10,11)=1$$

Here minimum distance for 2 bit word is 1

4.2.3. Hamming Code

- Hamming code can be used to check and correct errors
- Hamming code works based on minimum hamming distance(d_{min})
- Consider Hamming code(n,k)
 - n- no of code bits
 - k- no of data bits
 - r- no of redundant bit(Bits added with data For Error detection and correction)
 - $n = k+r$
- *With the help of below equation we can calculate the number of redundant bit for given data bit*

$$2^r \geq k + r + 1$$

4.2.4. Hamming Code(7,4)

- Consider example hamming code(7,4)
- No of data bits (k)=4
- Calculating redundant bits with help of formula $2^r \geq k + r + 1$
 - Consider $r=1 \rightarrow 2 \geq 4 + 1 + 1$ (*Not Feasible*)
 - Consider $r=2 \rightarrow 4 \geq 4 + 2 + 1$ (*Not Feasible*)
 - Consider $r=3 \rightarrow 8 \geq 4 + 3 + 1$ (*Feasible*)
- For data (k) bits =4 we need 3 redundant (r) bits
- So total number bits in code word (n)=4+3 (k+r)=7
- In this example Minimum hamming distance is $d_{min} = 3$

4.2.4.1. Hamming Code(7,4) Encoder

- Consider 4 data bits as (d_0, d_1, d_2, d_3) and 3 redundant bits (r_0, r_1, r_2)
- Calculation of redundant bits (Modulo 2 addition / XOR)
- $r_0 = d_3 + d_2 + d_1$
- $r_1 = d_3 + d_2 + d_0$
- $r_2 = d_3 + d_1 + d_0$

4.2.4.1. Hamming Code(7,4) Encoder

Consider message 0011 sent using hamming bit(order is d_3, d_2, d_1, d_0)

Find the redundant bits with help of formula given in previous page

- $r_0 = d_2 + d_1 + d_0 = 0 + 1 + 1 = 0$
- $r_1 = d_3 + d_2 + d_1 = 0 + 0 + 1 = 1$
- $r_2 = d_3 + d_1 + d_0 = 0 + 1 + 1 = 0$

- Code word=0011010($d_3 d_2 d_1 d_0 r_2 r_1 r_0$)
- This code word is transmitted to receiver

d_0	d_1	d_2	d_3
1	1	0	0
Data bits			

r_0	r_1	r_2
0	1	0
Redundant Bits		

4.2.4.2. Hamming Code Decoder

- Here 7 bit code word is received and receiver has to do error checking and correction
- Syndrome bit is used for error correction
- First step receiver will find the number of syndrome bits
- Here number of code word position in which error might occur is 7 and other condition is no error in code word (total 8 conditions)
- So we can consider 3 syndrome bits which will produce 8 combinations (000 to 111)

4.2.4.2. Hamming Code Decoder

- Calculation of syndrome bits
- (Modulo 2 addition / XOR)
- $s_0 = r_0 + d_3 + d_2 + d_1$
- $s_1 = r_1 + d_3 + d_2 + d_0$
- $s_2 = r_2 + d_3 + d_1 + d_0$

If there is error in transmission syndrome matrix will help to find which bit the error is located and corrected by receiver

s_2	s_1	s_0	Error Bit	Remark
0	0	0	No Error	
0	0	1	r_0	r_0 only in s_0
0	1	0	r_1	r_1 only in s_1
0	1	1	d_2	d_2 in s_0, s_1
1	0	0	r_2	r_2 only in s_2
1	0	1	d_1	d_1 in s_0, s_2
1	1	0	d_0	d_0 in s_2, s_1
1	1	1	d_3	d_3 in s_0, s_1, s_2
Syndrome matrix in receiver				

4.2.4.2. Hamming Code Decoder (No Error Condition)

- Consider the message we encoded in the Encoder section i.e. $0011010(d_3 d_2 d_1 d_0 r_2 r_1 r_0)$ received same message
- Syndrome bit 0 means no error in that bit, 1 means error present



4.2.4.2. Hamming Code Decoder (Error Condition)

- First we have to find the syndrome bits
 - $s_0 = r_0 + d_3 + d_2 + d_1 = 1 + 0 + 0 + 1 = 0$
 - $s_1 = r_1 + d_3 + d_2 + d_0 = 1 + 0 + 0 + 1 = 0$
 - $s_2 = r_2 + d_3 + d_1 + d_0 = 0 + 0 + 1 + 1 = 0$
- Syndrome bit 000(s_2, s_1, s_0) means no error (From syndrome matrix) present in the received data

4.2.4.2. Hamming Code Decoder (Error Condition)

- Consider an error condition left most 3rd bit is changed in transmission
- 0011010($d_3 d_2 d_1 d_0 r_2 r_1 r_0$) send message
- 0001010($d_3 d_2 d_1 d_0 r_2 r_1 r_0$) received message



4.2.4.2. Hamming Code Decoder (Error Condition)

- First we have to find the syndrome bits
 - $s_0 = r_0 + d_3 + d_2 + d_1 = 1 + 0 + 0 + 0 = 1$
 - $s_1 = r_1 + d_3 + d_2 + d_0 = 1 + 0 + 0 + 1 = 0$
 - $s_2 = r_2 + d_3 + d_1 + d_0 = 0 + 0 + 0 + 1 = 1$
- Syndrome bits are 101(s_2, s_1, s_0)
- From the syndrome matrix error presents in bit which is present in s_2, s_0 and not present on s_1 , d_1 is commonly present in calculation of s_2 and s_0 not in s_1
- Negate the d_1 bit for correcting the error.

5. Flow Control

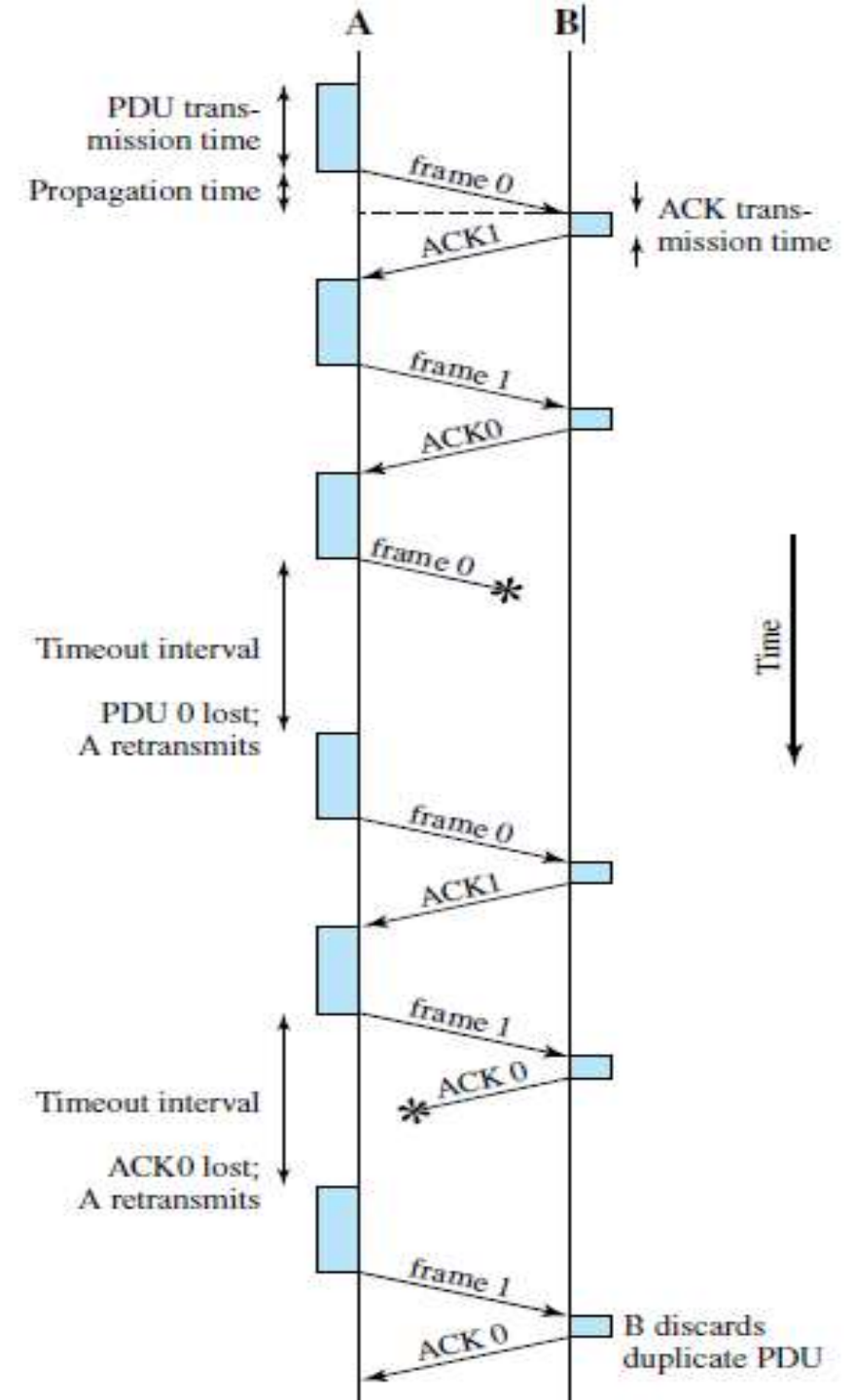
- There are 2 techniques of Error correction
 1. FEC (Forward Error correction) – Using Hamming codes
 2. ARQ (Automatic Repeat reQuest)– Resending of data
- In noisy Channel error control is achieved with help of ARQ which is a flow control mechanism
- Flow control is a technique for assuring that a transmitting entity does not overwhelm a receiving entity with data
- Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver

5.1 ARQ (Automatic Repeat reQuest)

- Any time an error is detected in an exchange, specified frames are retransmitted. This process is called ARQ
 - ARQ - Which basically means the retransmission of data
 - The ARQ techniques are:-
 1. Stop and Wait ARQ
 2. Go-Back-N ARQ
 3. Selective Repeat ARQ
- } Sliding Window Protocol

5.1.1 Stop and Wait ARQ

- Protocols in which the sender sends one frame and then waits for an acknowledgement before proceeding are called **stop-and-wait**
- No other data frames can be sent until the destination station's reply arrives at the source station
- Two sorts of errors could occur :
 1. Error in Data Frame
 2. Error in Acknowledgement



5.1.1 Stop and Wait ARQ

1. Error in Data Frame

- The frame that arrives at the destination could be damaged
- The receiver detects this by using the error-detection technique referred to earlier and simply discards the frame
- To account for this possibility, the source station is equipped with a timer
 - ❖ After a frame is transmitted, the source station waits for an acknowledgment
 - ❖ If no acknowledgment is received by the time that the timer expires, then the same frame is sent again

5.1.1 Stop and Wait ARQ

- To avoid this problem, frames are alternately labelled with 0 or 1 and positive acknowledgments are of the form ACK0 and ACK1
- ACK0 acknowledges receipt of a frame numbered 1 and indicates that the receiver is ready for a frame numbered 0
- All frame reaching for transmission is numbered 0 and 1 alternatively

2. Error in Acknowledgement

1. Station A sends a frame.
2. The frame is received correctly by station B, which responds with an acknowledgment (ACK).
3. The ACK is damaged in transit and is not recognizable by A, which will therefore time out and resend the same frame
4. This duplicate frame arrives and is accepted by B.
5. B has therefore accepted two copies of the same frame as if they were separate.

5.1.2 Go-Back-N ARQ

- Uses Sliding window Technique
- Station may send a series of frames sequentially numbered modulo some maximum value (Maximum size of window)
- Acknowledgement is send for the group of frame instead of single frame.
- Have positive and negative acknowledgement

Sequence Numbers

- Frames from a sending station are numbered sequentially However, because we need to include the sequence number of each frame in the header, we need to set a limit
- Range of sequence number varies from 0 to 2^m-1

5.1.2 Go-Back-N ARQ

- Consider $m=3$ so value is 0 to 7
- However, we can repeat the sequence. So the sequence numbers are

0,1,2,3,4,5,6, 7,0,1,2,3,4,5,6,7,0,1,...

Stop and wait single frame have single ack but in

- There is 2 types of Acknowledgement frames in this scenario
 1. RR(Receive Ready)
 2. REJ(Reject)

5.1.2 Go-Back-N ARQ

1. Receive Ready(RR)

It is like positive acknowledgement.

When all frames upto i^{th} frame is received receiver will send RR $i+1$ and after that sender will receive RR $i+1$ message then the sender will send $i+2$ th frame

1. REJECT(REJ)

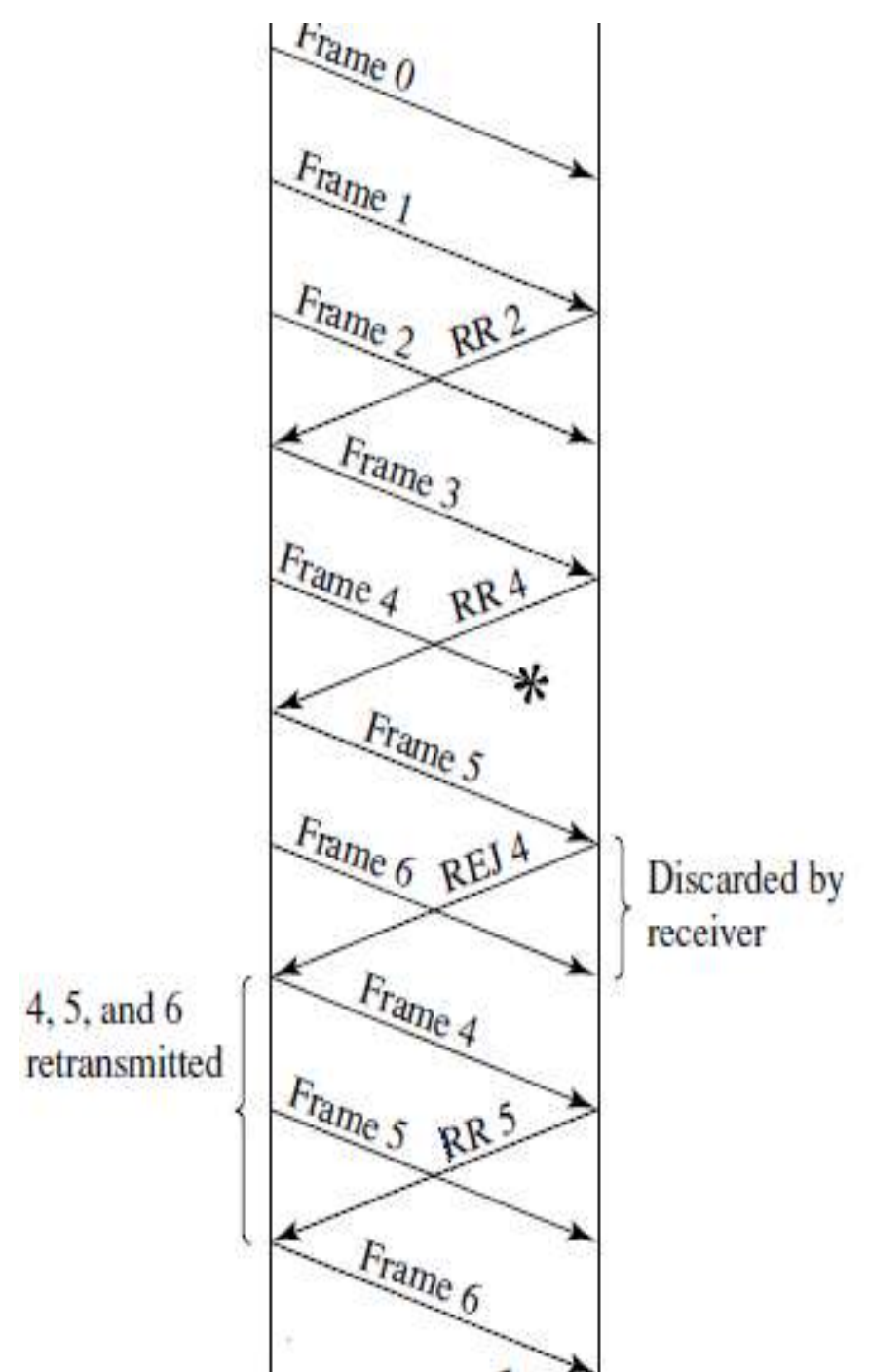
It is like negative acknowledgement.

When frame number i is not received

REJ i is send and sender will resend the frames starting from i

5.1.2 Go-Back-N ARQ

- In the figure First frame 0,1,2 is sent after Receiving Frame 1, RR2 is send by the receiver then frame 3 , 4 , 5 is sent and 4 is lost in middle of transmission and REJ 4 is sent after that frame 4,5 is sent again RR5 is sent after receiving frame 6,7 is sent

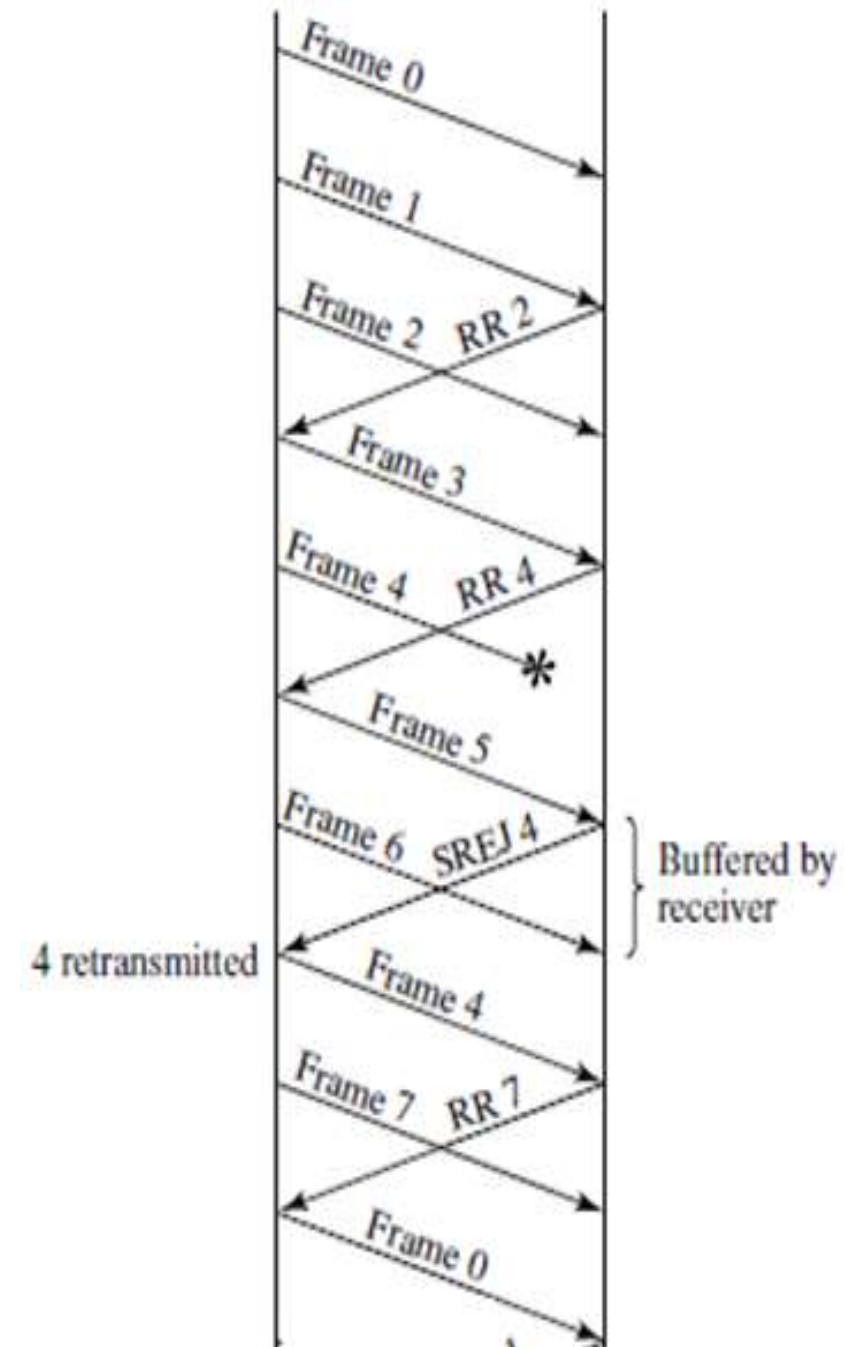


5.1.3 Selective Repeat ARQ

- RR is used similarly as in GO back N
- SREJ used as negative ACK
- With selective-reject ARQ, the only frames retransmitted are those that receive a negative acknowledgment, in this case called **SREJ**, or those that time out
- Selective reject would appear to be more efficient than go-back-N, because it minimizes the amount of retransmission
- On the other hand, the receiver must maintain a buffer large enough to save post-SREJ frames until the frame in error is retransmitted and must contain logic for reinserting that frame in the proper sequence

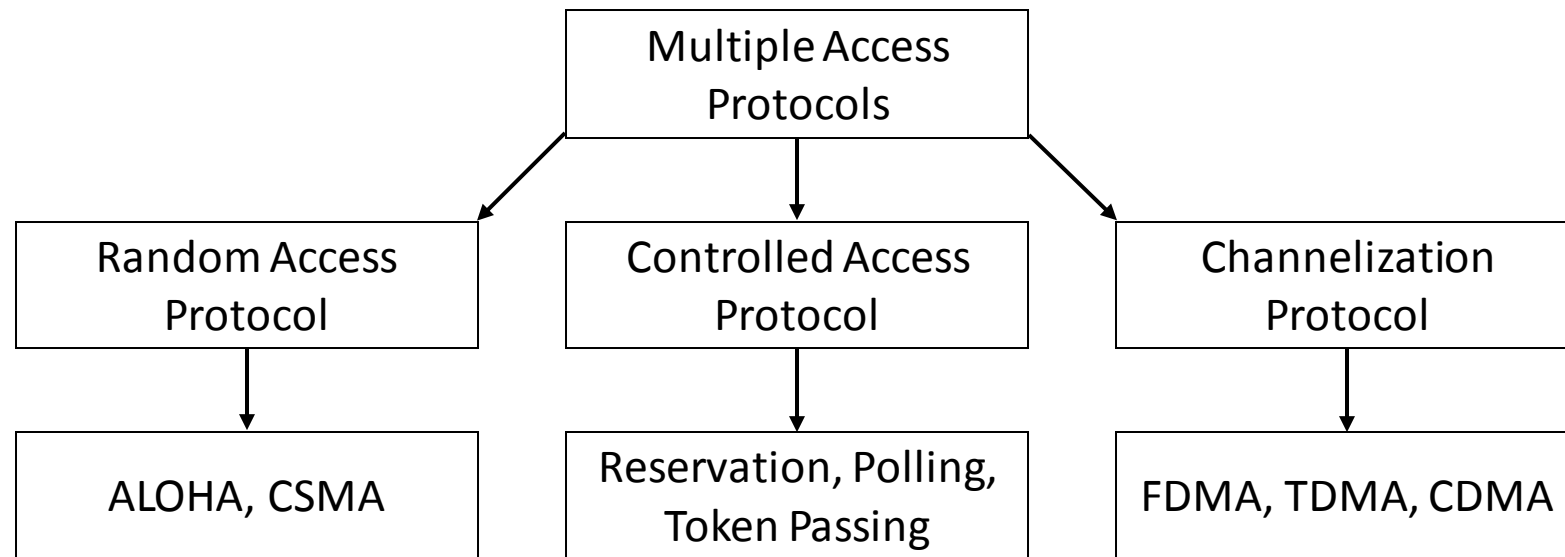
5.1.3 Selective Repeat ARQ

- The transmitter, too, requires more complex logic to be able to send a frame out of sequence
- Because of such complications, select-reject ARQ is much less widely used than go-back-N ARQ
- Selective reject is a useful choice for a satellite link because of the long propagation delay involved



6. Media Access(Multiple Access)

- In random access or contention methods, no station is superior to another station and none is assigned the control over another
- No station permits, or does not permit, another station to send(Randomly send if medium is free)



6. Media Access(Multiple Access)

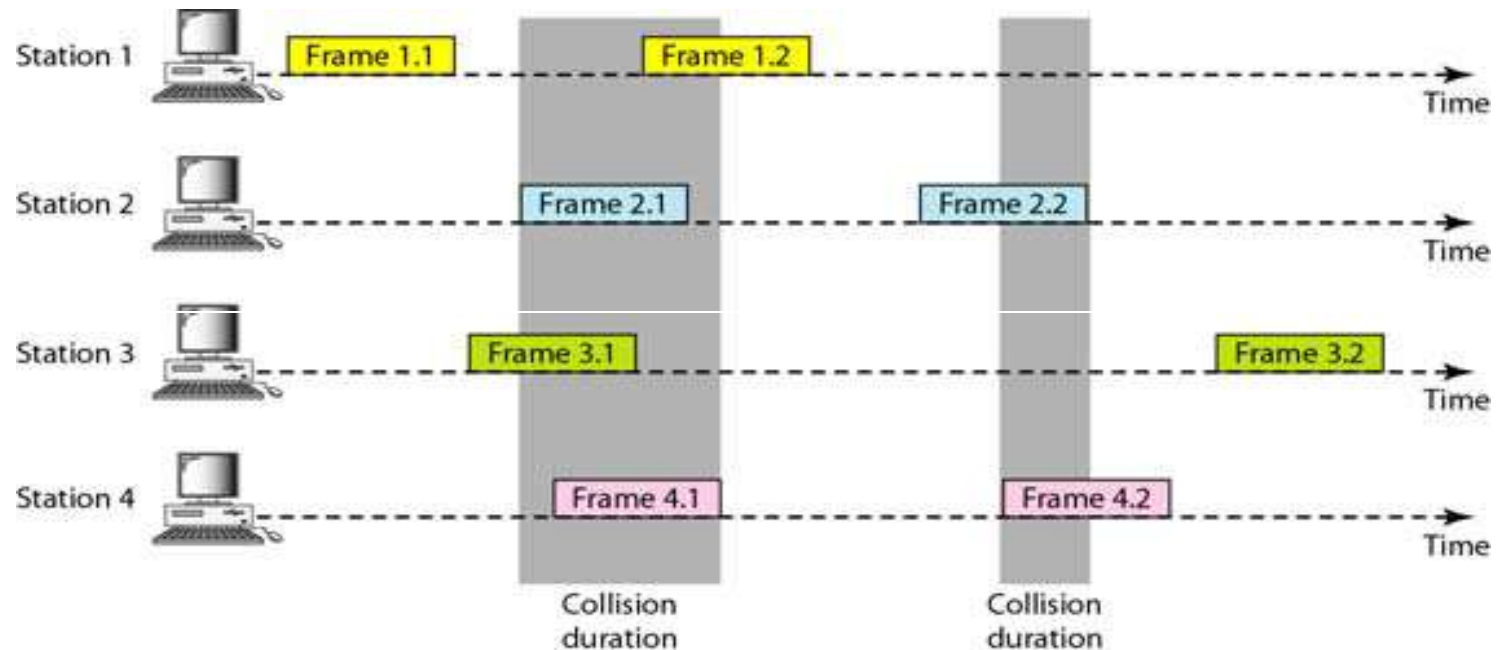
- Two features give random access method
 1. There is no scheduled time for a station to transmit. Transmission is random among the stations
 2. No rules specify which station should send next. Stations compete with one another to access the medium
- There are 2 methods
 1. ALOHA
 2. CSMA

6.1 ALOHA

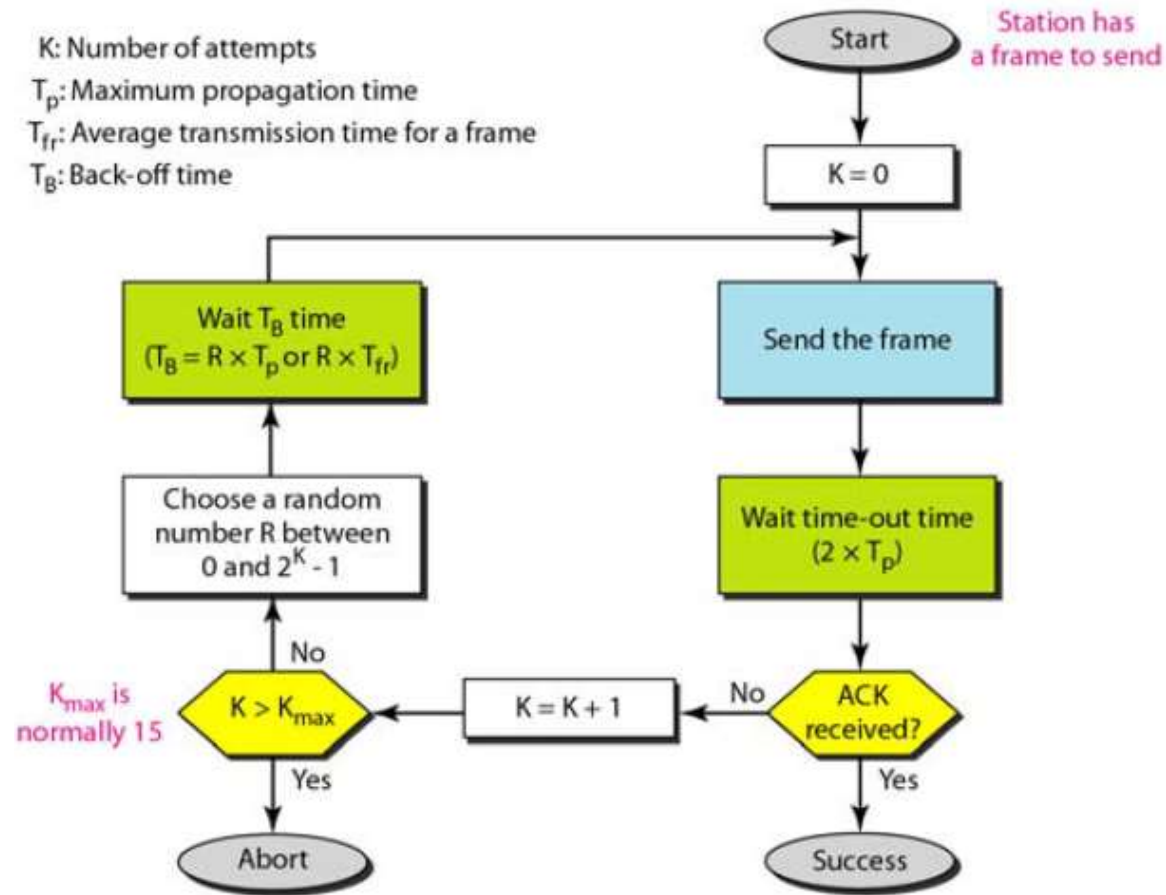
- Developed at the Univ. of Hawaii
- Random access method used for any type of shared medium(wireless and wired)
- ALOHA have 2 types
 1. Pure ALOHA
 2. Slotted ALOHA

6.1.1. pure ALOHA

- The node immediately transmits its frame completely. If the frame is collided it retransmits the frame again (after completely transmitting its collided frame) with the probability



6.1.1. pure ALOHA (Frame sending Procedure)



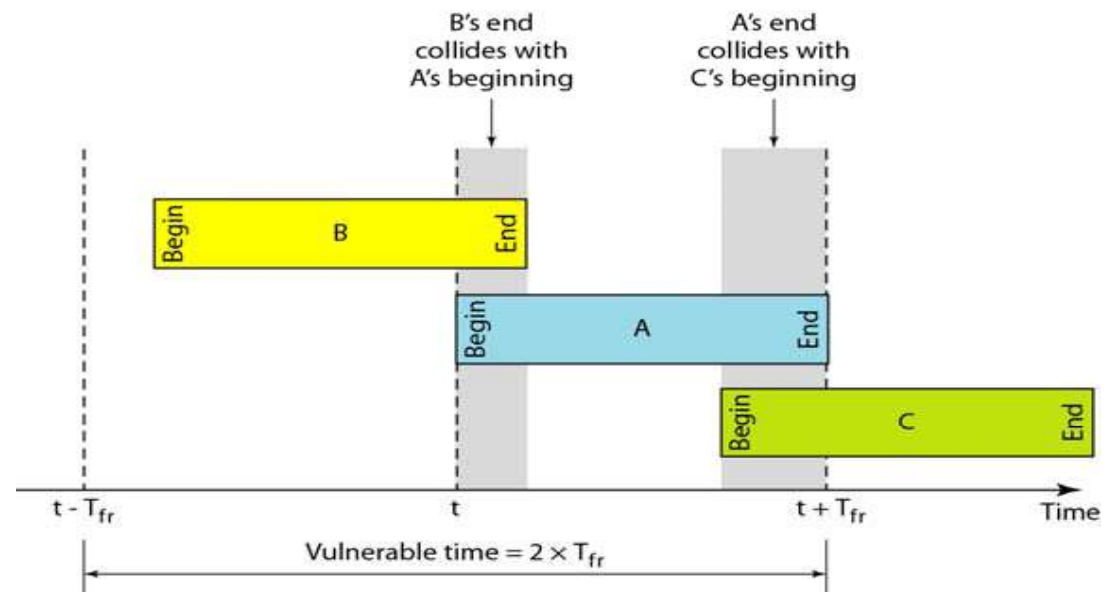
6.1.1. pure ALOHA (*Frame sending Procedure*)

- Procedure in pure ALOHA:
 1. Send frame
 2. Wait for a time out(time interval) and check if acknowledgement is received or not if received transmission is **SUCCESS** else go to step 3
 3. Increment the number of attempts (k)and check if it reaches maximum(15) if it reaches maximum attempt **ABORT** transmission else go to step 4
 4. Choose a random time interval (R) between 0 to $2^k - 1$ and calculate back off time(T_B) using random time interval time and propagation time/frame transmission time(T_p/T_{fr}) $\rightarrow T_B=R*T_p$ or $T_B=R*T_{fr}$
 5. Repeat from step 1 until success/ abort

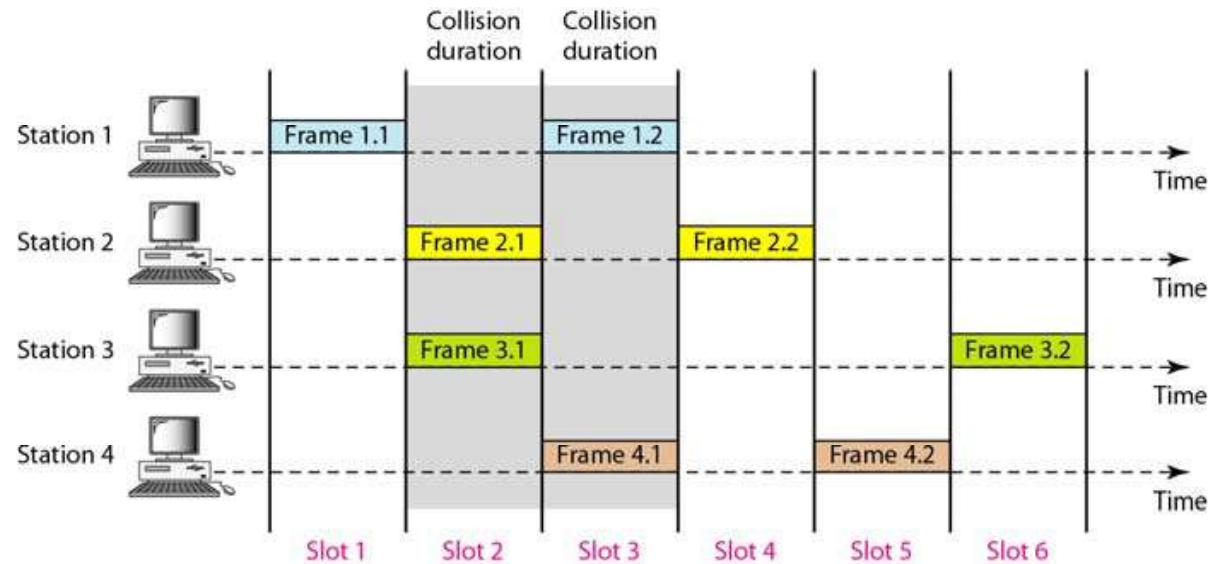
6.1.1. pure ALOHA (*Vulnerable Time*)

- Station A sends a frame at time t
- Now imagine station B has already sent a frame between $t - T_{fr}$ and t
- This leads to a collision between the frames from station A and station B
- The end of B's frame collides with the beginning of A's frame
- On the other hand, suppose that station C sends a frame between t and $t + T_{fr}$

- Here, there is a collision between frames from station A and station C. The beginning of C's frame collides with the end of A's frame
- Vulnerable time = $2 * T_{fr}$



6.1.2. slotted ALOHA



- Frames are of the same size time is divided into equal size slots, time to transmit 1 frame nodes start to transmit frames only at beginning of slots nodes are synchronized
- If a frame is ready for transmission after starting time of slot 1 it will be transmitted in slot 2
- If 2 or more nodes transmit in slot, all nodes detect collision

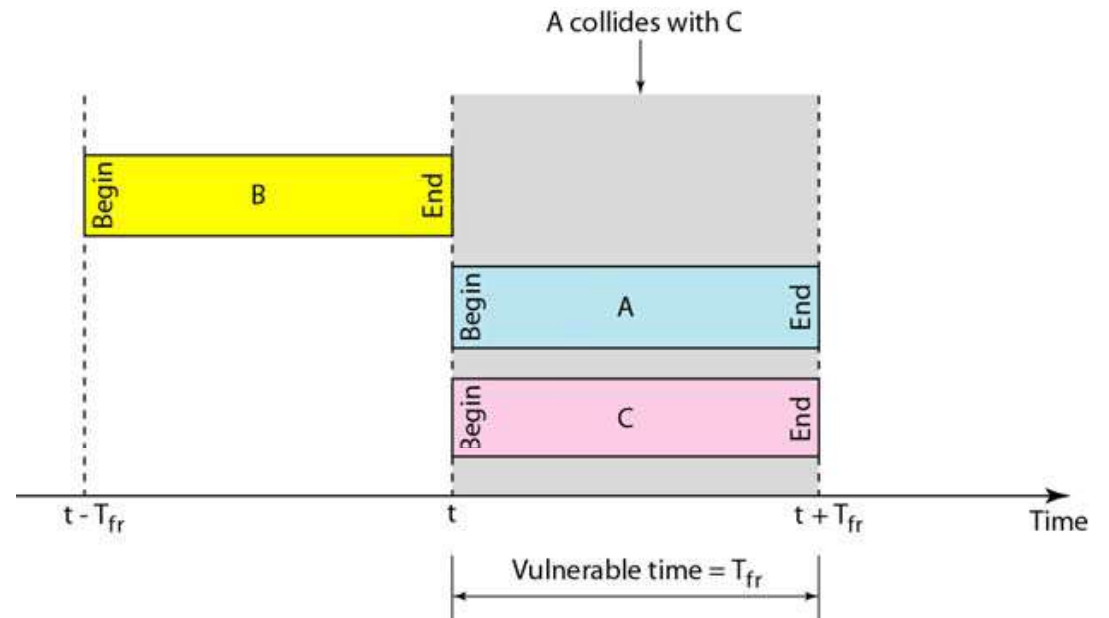
6.1.2. slotted ALOHA

- when node obtains fresh frame it transmits in next slot
- No collision, node can send new frame in next slot
- If collision, node retransmits frame in each subsequent slot with probability (p) until success
- Here Procedure of frame sending is similar to pure ALOHA but of frame will be sent only on starting of time slot

6.1.2. slotted ALOHA (*Vulnerable Time*)

- Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot
- This means that the station which started at the beginning of this slot has already finished sending its frame

- Vulnerable time = T_{fr}



6.2. CSMA (Carrier Sense Multiple Access)

- Invented to minimize collisions and increase the performance
- A station now “follows” the activity of other stations
- Simple rules for a polite human conversation
 1. Listen before talking
 2. If someone else begins talking at the same time as you, stop talking
- A node should not send if another node is already sending(Carrier Sensing)
- Vulnerable time is the propagation time which is the time needed for a signal to propagate from one end of the medium to the other

6.2.1 CSMA (Persistence Methods)

- Persistence methods :- Methods for Sensing the channel (busy/ idle)
- 3 Persistence methods are available:
 1. I-persistence
 2. Non-persistence
 3. P-persistence

6.2.1.1. I-Persistence Method

- **In** this method, after the station finds the line idle, it sends its frame immediately (with probability 1)
- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately

Figure : Behaviour I persistence

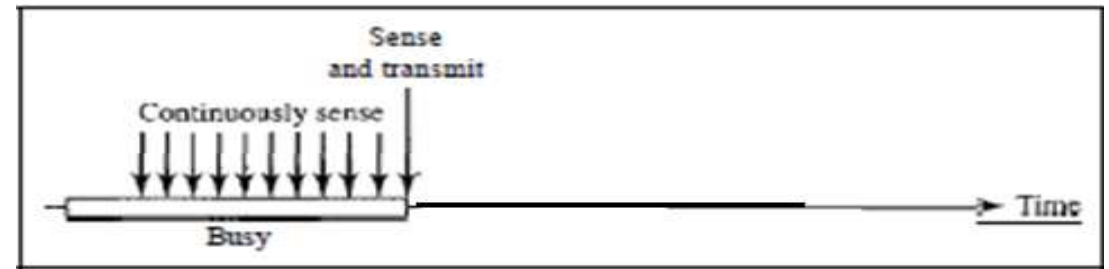
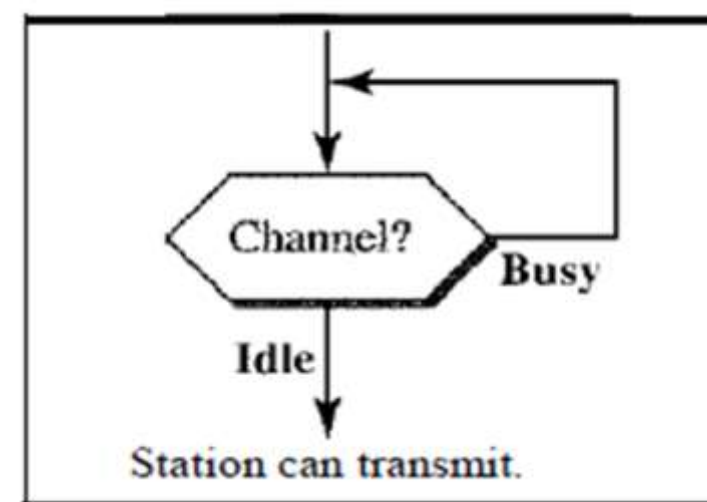


Figure : Flow diagram of I persistence



6.2.1.2. Non-Persistence Method

- In the Non-persistent method, a station that has a frame to send senses the line.
- If the line is idle, it sends immediately.
- If the line is not idle, it waits a random amount of time and then senses the line again.
- The Non-persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously
- This method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

Figure : Behaviour of Non persistence

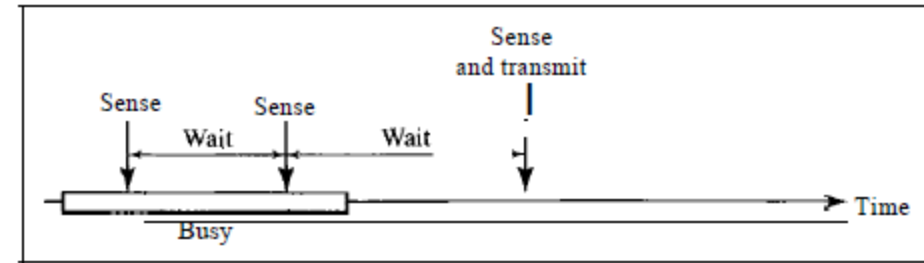
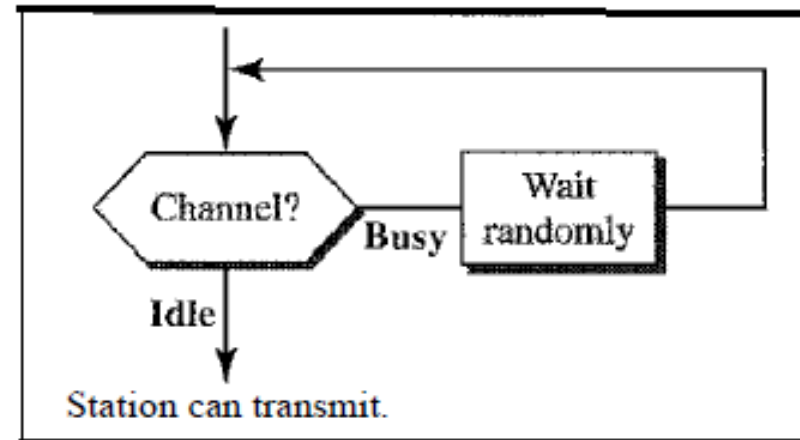


Figure : Flow diagram of Non persistence



6.2.1.3. P-Persistence Method

- **The p-persistent method** is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time
- The p-persistent approach combines the advantages of the other two strategies
- It reduces the chance of collision and improves efficiency.

Figure : Behaviour P persistence

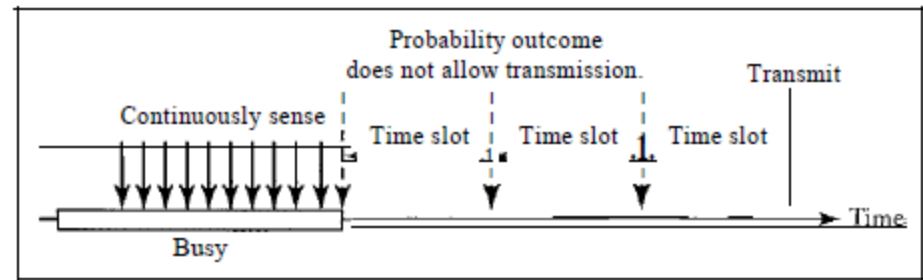
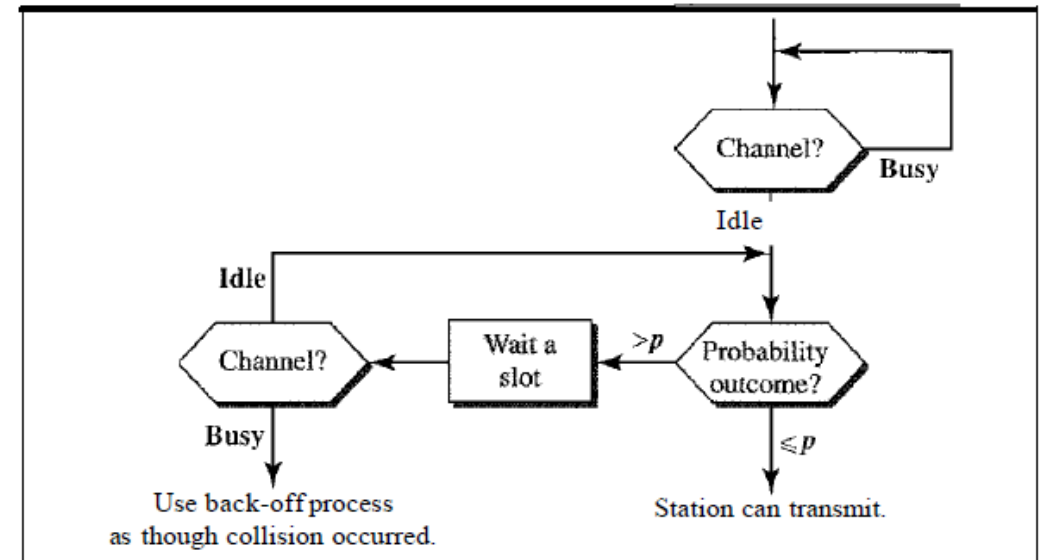


Figure : Flow diagram of P persistence

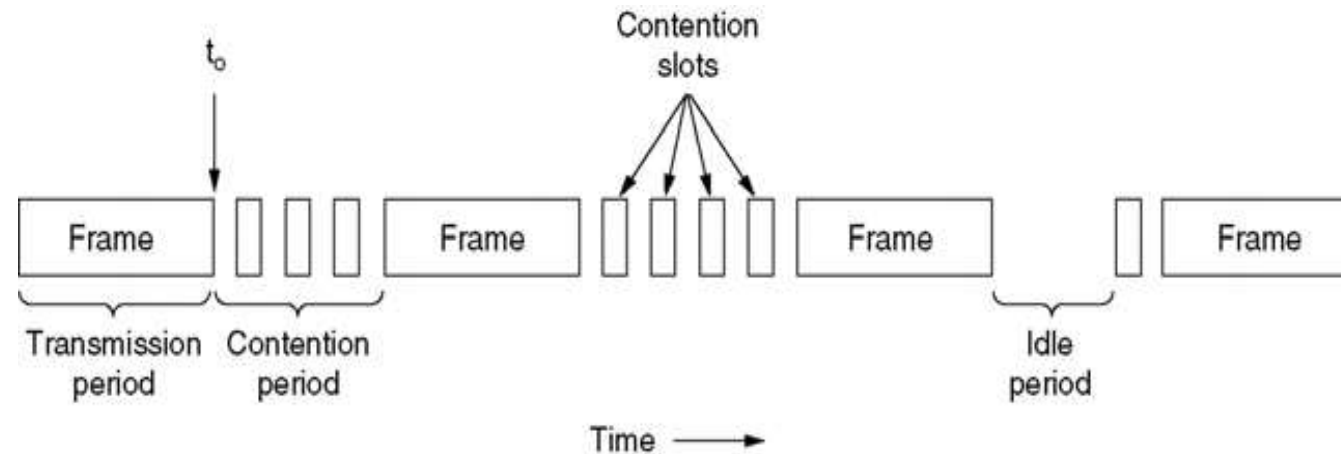


6.2.1.3. P-Persistence Method

- In this method, after the station finds the line idle it follows these steps:
 1. With probability p , the station sends its frame.
 2. With probability $q = 1 - p$, the station waits for the beginning of the next time slot and checks the line again.
 - I. If the line is idle, it goes to step 1.
 - II. If the line is busy, it acts as though a collision has occurred and uses the back off procedure.

6.2.2 CSMA/CD (Collision Detection)

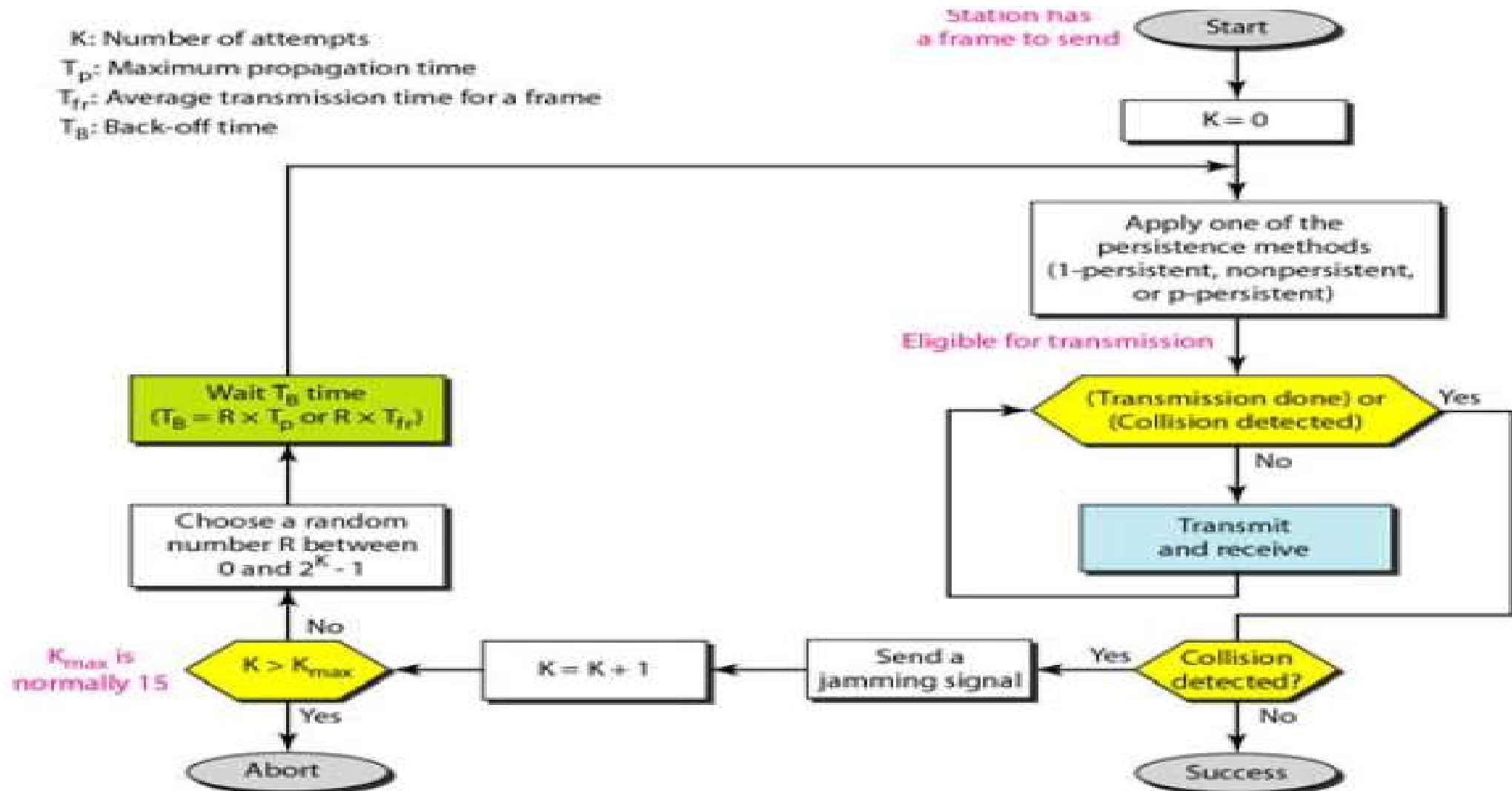
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again



- In CSMA/CD Channel can be in one of the three states: contention, transmission, and idle.

6.2.2 CSMA/CD Procedure

K : Number of attempts
 T_p : Maximum propagation time
 T_{fr} : Average transmission time for a frame
 T_B : Back-off time



6.2.2 CSMA/CD Procedure

- Procedure is similar to ALOHA but with certain differences
- The main differences are:-
 - Addition of the persistence process before transmission
 - Transmission is continuous process
 - Jamming signal is used in it

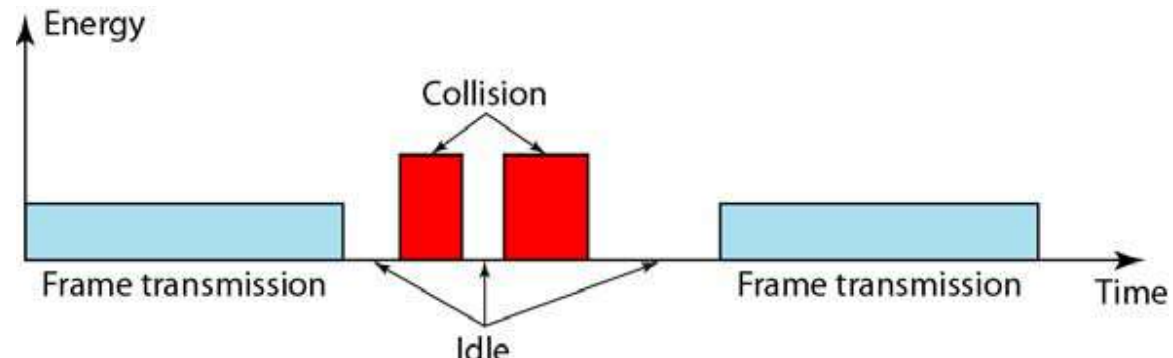


Figure : Energy Level During Transmission

6.2.2 CSMA/CD *Throughput*

- The throughput of *CSMA/CD* is greater than that of pure or slotted ALOHA
- The maximum throughput occurs at a different value of G and is based on the persistence method and the value of p in the p -persistent approach.
- For 1-persistent method the maximum throughput is around 50 percent when $G = 1$
- For non-persistent method, the maximum throughput can go up to 90 percent when G is between 3 and 8

6.2.3 CSMA/CA (Collision Avoidance)

- Collisions are avoided through the use of CSMA/CA's three strategies:
 1. Inter Frame Space
 2. Contention window
 3. Acknowledgments

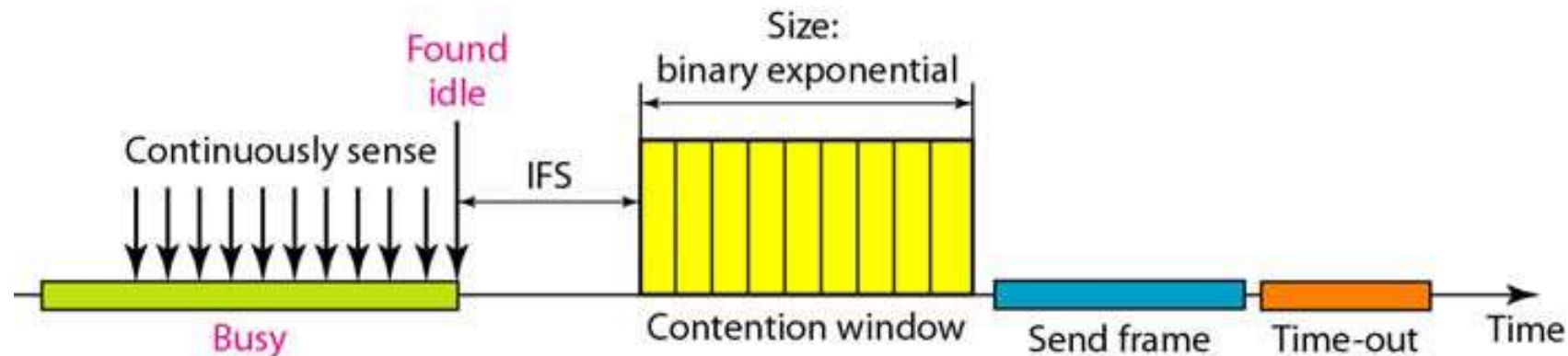


Figure : Timing in CSMA/CA

6.2.3 CSMA/CA Inter Frame Space

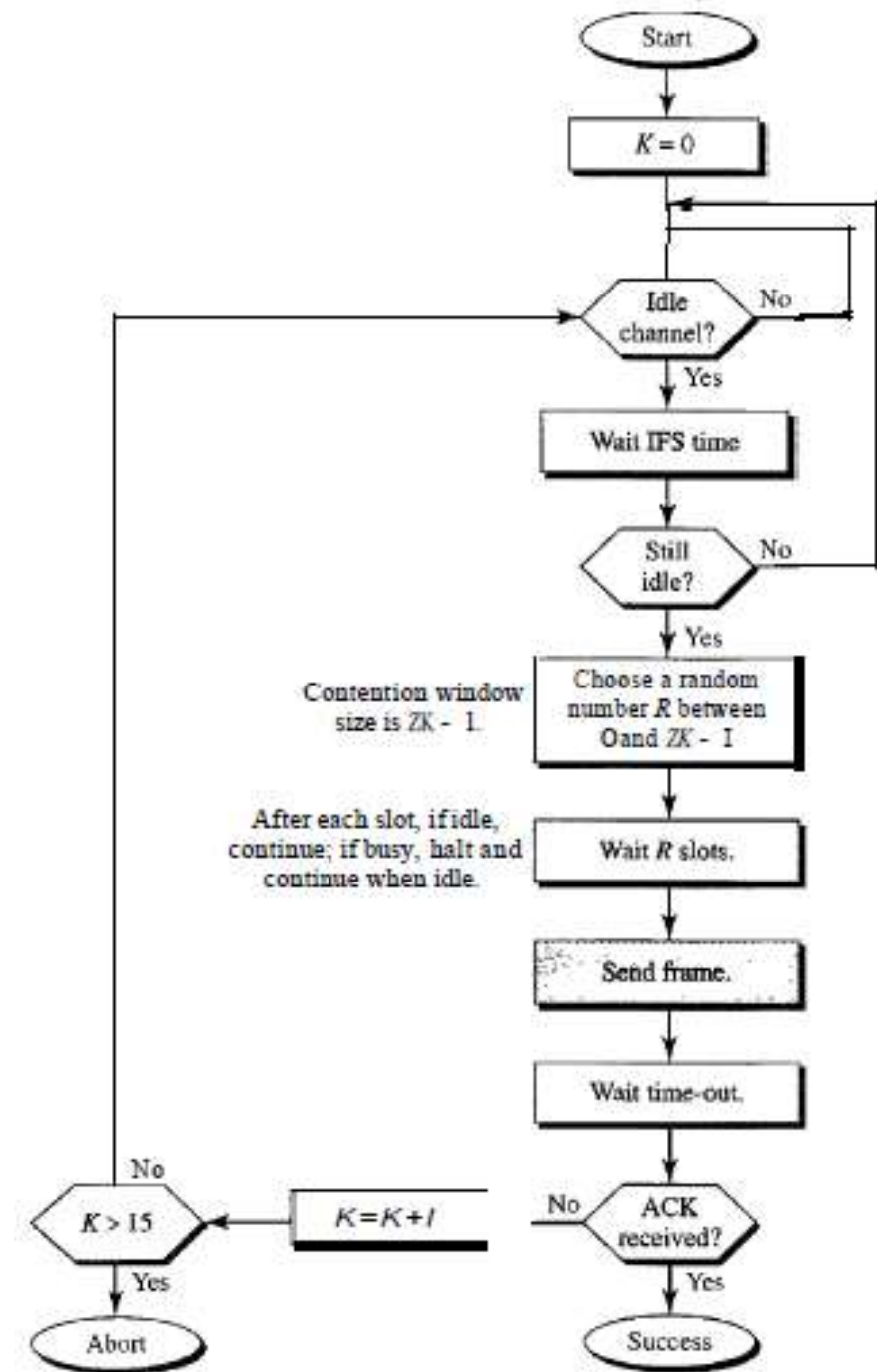
- When an idle channel is found, the station does not send immediately
- Station waits for a period of time called the inter frame space or IFS
- In CSMA/CA, the IFS can also be used to define the priority of a station or a frame
 - For EX: a station that is assigned a shorter IFS has a higher priority while sending

6.2.3 CSMA/CA Contention Window

- Contention window (random wait time) is an amount of time divided into slots
- A station that is ready to send chooses a random number of slots as its wait time
- The number of slots in the window changes according to the binary exponential back-off strategy
- Binary exponential back-off strategy means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time
- Restarts content window timer when the channel becomes idle

6.2.3 CSMA/CA Procedure

- Channel needs to be sensed before and after the IFS and sensed during the contention time
- For each time slot of the contention window, the channel is sensed
- If it is found idle, the timer continues else if the channel is found busy, the timer is stopped and continues after the timer becomes idle again.



7. IEEE Data Link Layer Protocol/Standards

- Here we are discussing about the protocols and standard used in data link layer.
- Here 802 commonly refer to data link layer specifically(MAC Sub layer)

Standards

- **IEEE 802.3**
- **IEEE 802.4**
- **IEEE 802.5**

7.1. IEEE 802.3 Ethernet

- IEEE 802.3 frame format (refer section 3.3)
- It uses mainly **CSMA** as channel access mechanism

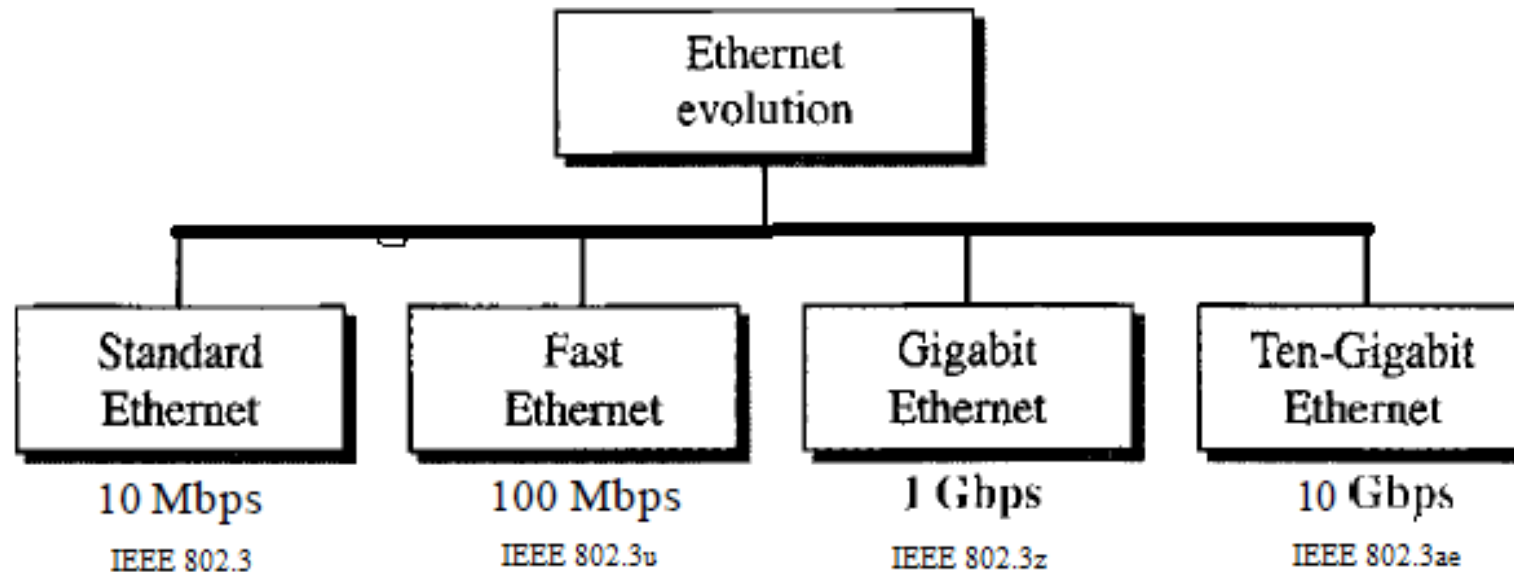


Figure : Different IEEE 802.3 standards

7.1.1. IEEE 802.3 Standard Ethernet

- Maximum data rate is up to **10Mbps**
- Standard Ethernet uses **1-persistent CSMA/CD**
- Uses 48 bit addressing
- It uses following Technologies

10Base2 - Thin Co-axial cable (Also called Thinnet / Thin Ethernet)

10Base5 - Thick Co-axial cable (Also called Thicknet / Thick Ethernet)

10BaseT – Unsheilded Twisted Pair Cable (Also called Twisted pair Ethernet)

10BaseF – Optical Fiber Cable

7.1.1. IEEE 802.3 Standard Ethernet

	10BASE5	10BASE2	10BASE-T	10BASE-FP
Transmission medium	Coaxial cable (50 ohm)	Coaxial cable (50 ohm)	Unshielded twisted pair	850-nm optical fiber pair
Signaling technique	Baseband (Manchester)	Baseband (Manchester)	Baseband (Manchester)	Manchester/on-off
Topology	Bus	Bus	Star	Star
Maximum segment length (m)	500	185	100	500
Nodes per segment	100	30	—	33
Cable diameter (mm)	10	5	0.4 to 0.6	62.5/125 μm

7.1.2. IEEE 802.3u Fast Ethernet

- Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps

Features

1. Upgrade the data rate to 100 Mbps
2. Make it compatible with Standard Ethernet
3. Keep the same 48-bit address
4. Keep the same frame format
5. Keep the same minimum and maximum frame lengths
6. Can connect Point to point / Star

7.1.2. IEEE 802.3u Fast Ethernet

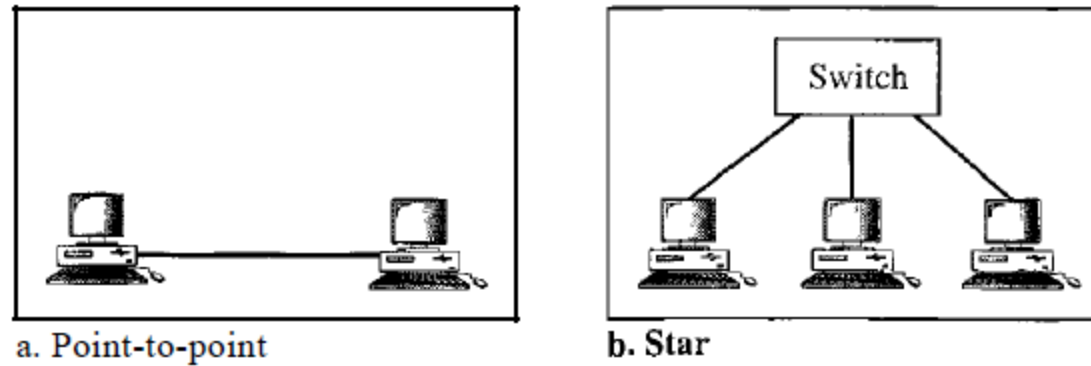


Figure : Fast Ethernet Connection Topologies

- 100BaseTX UTP Cat5 Two wire Implementation
- 100BaseFX Fiber Optic Cable
- 100BaseT4 UTP Cat3 Four Wire Implementation

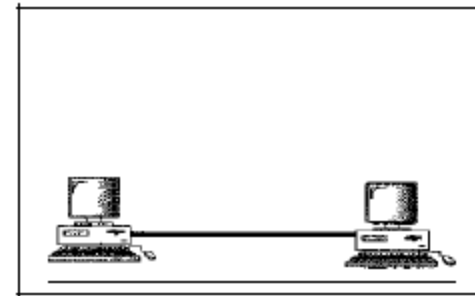
7.1.3. IEEE 802.3z GigaBit Ethernet

- Higher data rate than fast ethernet (1000 Mbps)

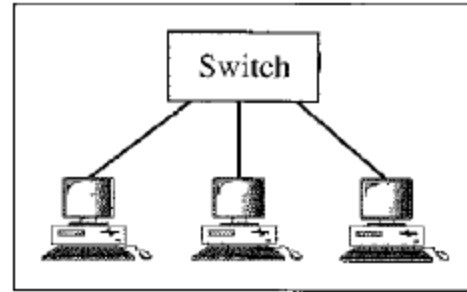
Features

1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with Standard or Fast Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. To support auto negotiation as defined in Fast Ethernet

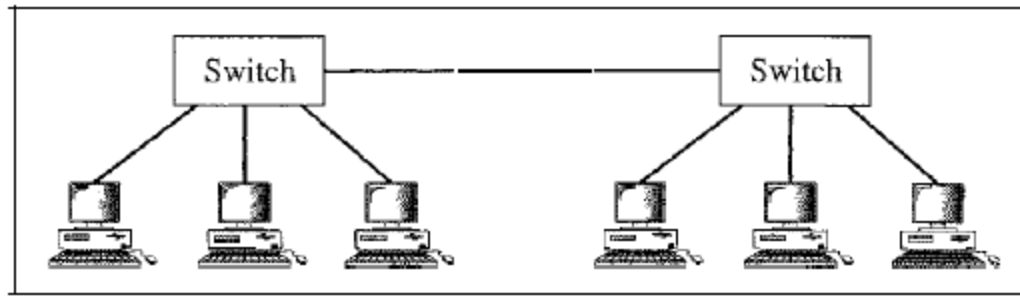
7.1.3. IEEE 802.3z Gigabit Ethernet



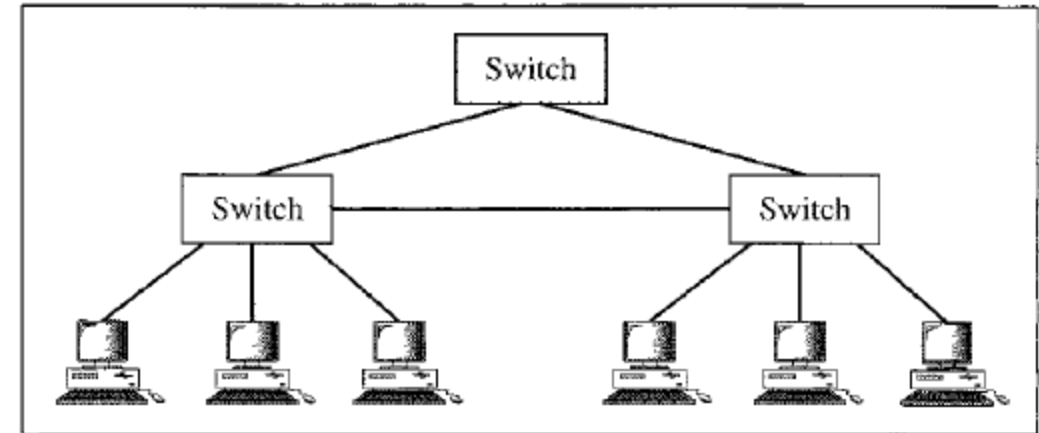
a. Point-to-point



b. Star



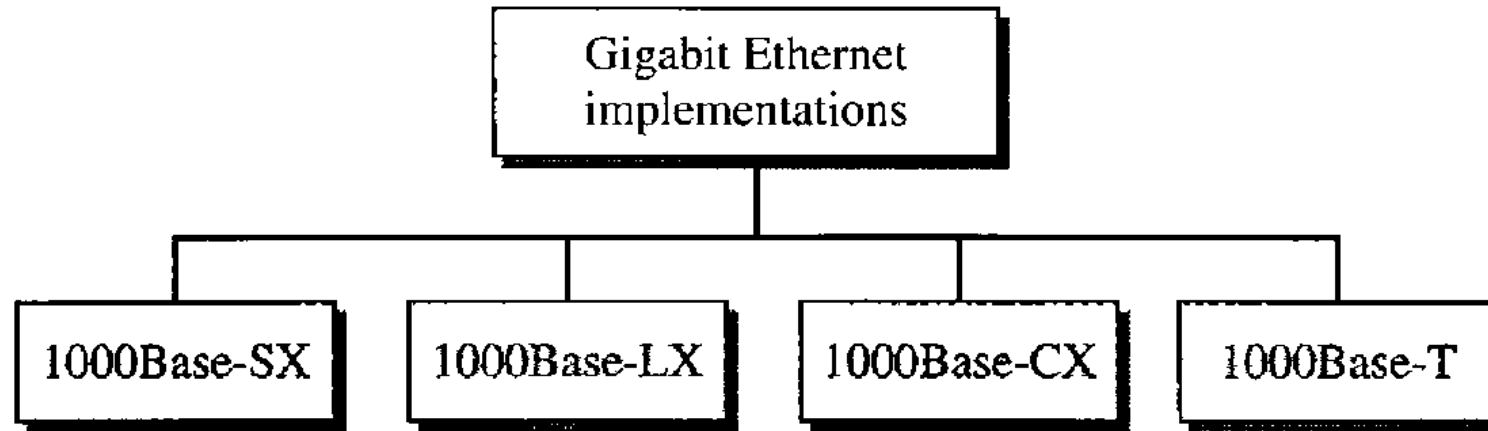
c. Two stars



d. Hierarchy of stars

Figure : Topologies of Gigabit Ethernet

7.1.3. IEEE 802.3z Gigabit Ethernet



- 1000BaseSX – Fiber Optic Short wave (2 wire)
- 1000BaseLX – Fiber Optic Short wave (2 wire)
- 1000BaseCX – Copper STP Cable (2 wire)
- 1000BaseSX – Fiber Optic Short wave (4 wire)

7.1.4. IEEE 802.3ae 10 GigaBit Ethernet

Features

1. Upgrade the data rate to 10 Gbps.
2. Make it compatible with Standard, Fast, and Gigabit Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network (WAN).
7. Make Ethernet compatible with technologies such as Frame Relay and ATM

7.1.4. IEEE 802.3ae 10 GigaBit Ethernet

- Ten-Gigabit Ethernet is designed for using fiber-optic cable over long distances

<i>Characteristics</i>	<i>10GBase-S</i>	<i>10GBase-L</i>	<i>10GBase-E</i>
Media	Short-wave 850-nm multimode	Long-wave 1310-nm single mode	Extended 1550-nm single mode
Maximum length	300m	10km	40km

Figure : 10 Gigabit Ethernet Implementation

7.2. IEEE802.4 Token Bus

- The 802.4 IEEE standard defines the Token Bus protocol for a token-passing access method on a bus topology.
- In a token-passing access method, a special packet called a token is passed from station to station and only the token holder is permitted to transmit packets onto the LAN.
- No collisions can occur with this protocol(Only One Station can transfer)
- When a station is done transmitting its packets, it passes the token to the "next" station.
- The next station does not need to be physically closest to this one on the bus, just the next logical station.

7.2. 802.4 Token Bus

- A station can hold the token for only a certain amount of time before it must pass it on -even if it has not completed transmitting all of its data.
- This assures access to all stations on the bus within a specified period of time.

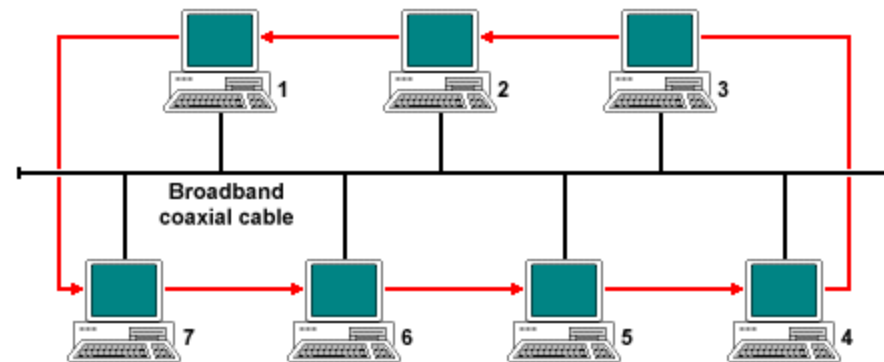


Figure : Token Bus Network (Red Arrow Indicates Token Passing Sequence)

7.3. 802.5 Token Ring

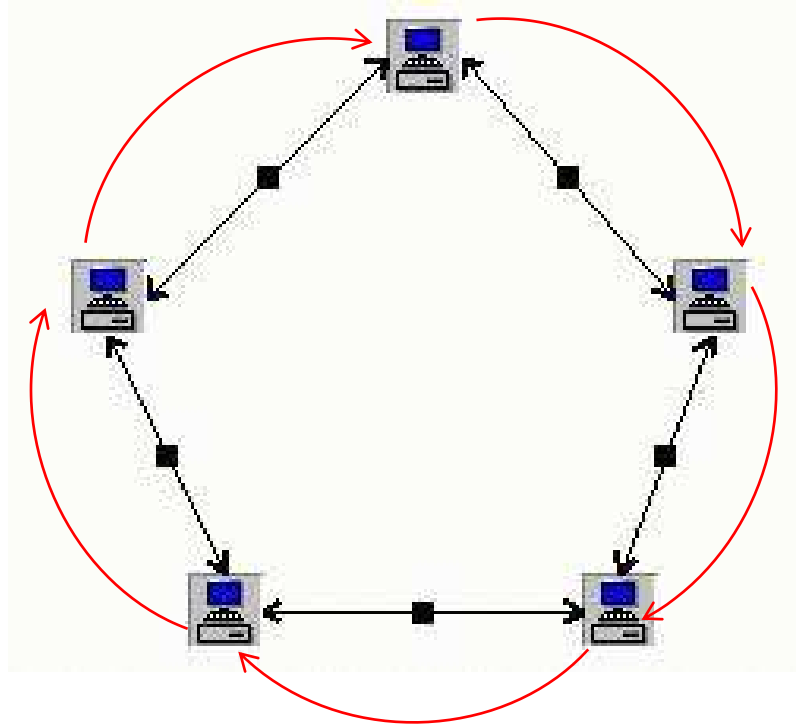


Figure : Token Bus Network (Red Arrow Indicates Token Passing Sequence)

7.3. 802.5 Token Ring

- The 802.5 IEEE standard defines the Token Ring protocol which, like Token Bus, is another token-passing access method, but for a ring topology
- A ring topology consists of a series of individual point-to-point links that form a circle
- A token is passed from station to station in one direction around the ring, and only the station holding the token can transmit packets onto the ring

7.3. 802.5 Token Ring

- Data packets travel in only one direction around the ring
- When a station receives a packet addressed to it, it copies the packet and puts it back on the ring
- When the originating station receives the packet, it removes the packet.

Chapter 5

Network Layer

Prepared By R.G.B

Visit For Notes: <http://sites.google.com/site/rohitgbal>

Email: rohitgbal@gmail.com

Contents

- Internet Protocol
 - Version 4
 - Address depletion problem
 - NAT
 - Sub netting
 - Version 6
 - Header IPv4
 - Header IPv6
- Routing
 - Classless and Classful
 - Static and dynamic
 - Interior and exterior
 - Distance vector and Link state
 - Routing Algorithms
 - RIP
 - OSPF
 - BGP

Need for Network layer

- The network layer is responsible for host-to-host delivery
- Routing the packets through the routers or switches
- The network layer at the source is responsible for creating a packet from the data coming from another protocol
- The network layer is responsible for checking its routing table to find the routing information

1 IP Address v4

- An IPv4 address is 32 bits long
- The IPv4 addresses are unique and universal
- IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (Maximum available theoretically)
- IPv4 have 2 types of notations:
 1. Dotted decimal
Denoted in decimal format each byte is separated by dot eg: 117.149.29.2
Mostly used by human configurations
 2. Binary notation
In binary format eg: 01110101 10010101 00011101 00000010
Mostly used by devices for processing

1.1 IPv4 Classes(Classfull Address)

- The address space is divided into five classes: A, B, C, D, and E
- Division is based on the first byte in doted decimal format

Class A

Range of first octet or byte is between 0 to 127

First byte is network and last 3 bytes are Host (N.H.H.H)

First bit always will be zero (0xxxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx)

Used for unicasting, valid host IP

Class B

Range of first octet or byte is between 128 to 191

First 2 bytes is network and last 2 byte are Host (N.N.H.H)

First bit always will be zero (10xxxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx)

Used for unicasting, valid host IP

1.1 IPv4 Classes

Class C

Range of first octet or byte is between 192 to 223

First 3 bytes is network and last byte are Host (N.N.N.H)

First bit always will be zero (110xxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx)

Used for unicasting, valid host IP

Class D

Range of first octet or byte is between 224 to 239

First 2 bytes is network and last 2 byte are Host (N.N.H.H)

First bit always will be zero (1110xxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx)

Used for Multicasting, Special Address

Class E

Range of first octet or byte is between 240 to 255

First 2 bytes is network and last 2 byte are Host (N.N.H.H)

First bit always will be zero (1111xxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx)

Used for research purpose

1.1.1 Netid & Host ID

- **Class A** :- first byte netid and last 3 bytes hostid (N.H.H.H)
- **Class B** :- first 2 bytes netid and last 2 bytes hostid (N.N.H.H)
- **Class C** :- first 3 bytes netid and last byte hostid (N.N.N.H)
- Subnet mask helps to identify netid and hostid
- CIDR value is total number of network bits in subnetmask

1.1.2 Subnet Mask and CIDR in Classful IPv4

- The mask can help us to find the netid and the hostid
 - *For example, the mask for a class A address has eight 1s, which means the first 8 bits of any address in class A define the netid; the next 24 bits define the hostid.*
- CIDR value is number 1's (ones) in the subnet mask(network bits), usually for class A,B,C CIDR values will be 8,16,24 respectively

Given below table shows various subnet mask, CIDR values of class A,B,C

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

1.2 Address Depletion Problem in Internet

- Because of limited number of IP and increasing demand of IP in internet over years lead to depletion of IP address
- Solution of depletion are mainly
 1. NAT
 2. Sub netting
 3. IPv6

1.3 Network Address Translation(NAT)

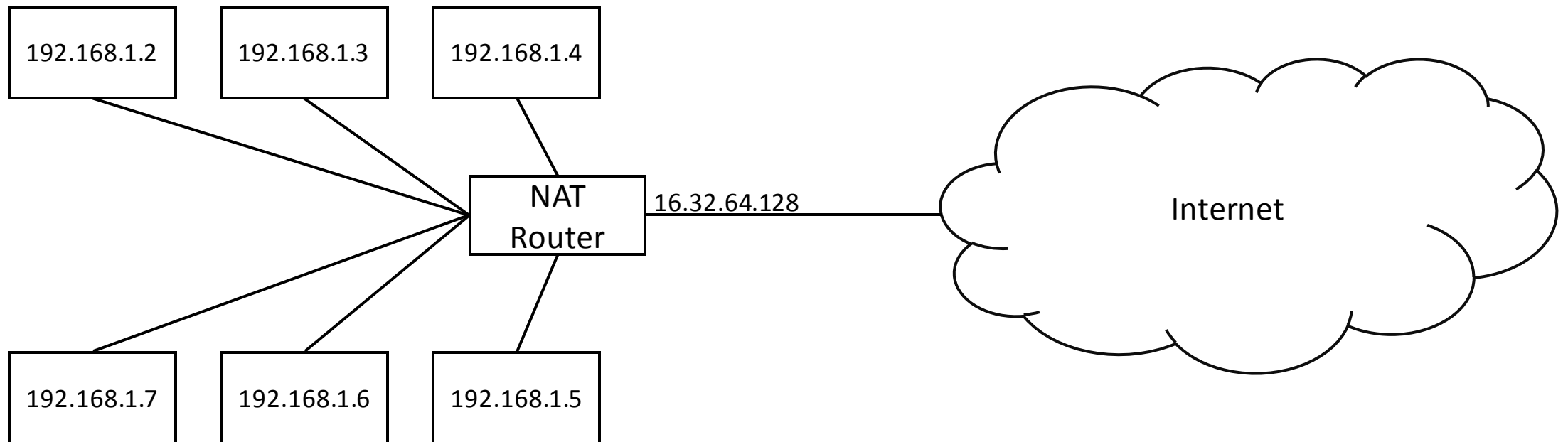
- IP address have public range and private range
- Public range is used for communication in internet and can used only with permission of internet authorities
- Private IP can be used for local communication without permission of Internet authorities

Given below table shows private ranges of class A,B,C

<i>Range</i>			<i>Total</i>
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

1.3 Network Address Translation(NAT)

- Public IP should be unique globally
- Private IP should be unique inside a organization, not globally
- NAT router consist of public IP in exit interface and internal interface consist of Private IPs



1.3 Network Address Translation(NAT)

- Address Translation : Replace outgoing packets Source IP address as NAT router public IP and replaces incoming packet Destination IP with private (Private to public and public to private)
- Translation is done with help of translation table which consist of IP address of private range and public range and port address

Below table showing Translation table in NAT

<i>Private Address</i>	<i>Private Port</i>	<i>External Address</i>	<i>External Port</i>	<i>Transport Protocol</i>
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
...

1.4 Classless Addressing

- There is no classes hierarchy in the IP address but address is still granted in blocks.

Restriction

- To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:
 1. The addresses in a block must be contiguous, one after another.
 2. The number of addresses in a block must be a power of 2 (1, 2, 4, 8, ..)
 3. The first address must be evenly divisible by the number of addresses.

1.4.1 Subnetting

- Subnetting means creating subnetwork
- Subnetting means increasing networks bits(i.e. 1s) in subnet mask
- If network bit is increased host bits will be decreased, so number of host will be decreased
- A Class A network have 8 bits for network (2^{24} IP address available) if you wanted smaller block IP from class A increase the network bits / decreasing host bits

1.4.2. Supernetting

- Supernetting means creating bigger network from smaller one
- Supernetting means decreasing networks bits(i.e. 1s) in subnet mask
- If network bit is decreased host bits will be increased, so number of host will be decreased
- A Class C network have 24 bits for network (2^8 IP address available) if you wanted bigger block IP from class C decrease the network bits / increasing host bits
- Supernetting just opposite of subnetting

1.4.3. VLSM (Variable Length Subnet Mask)

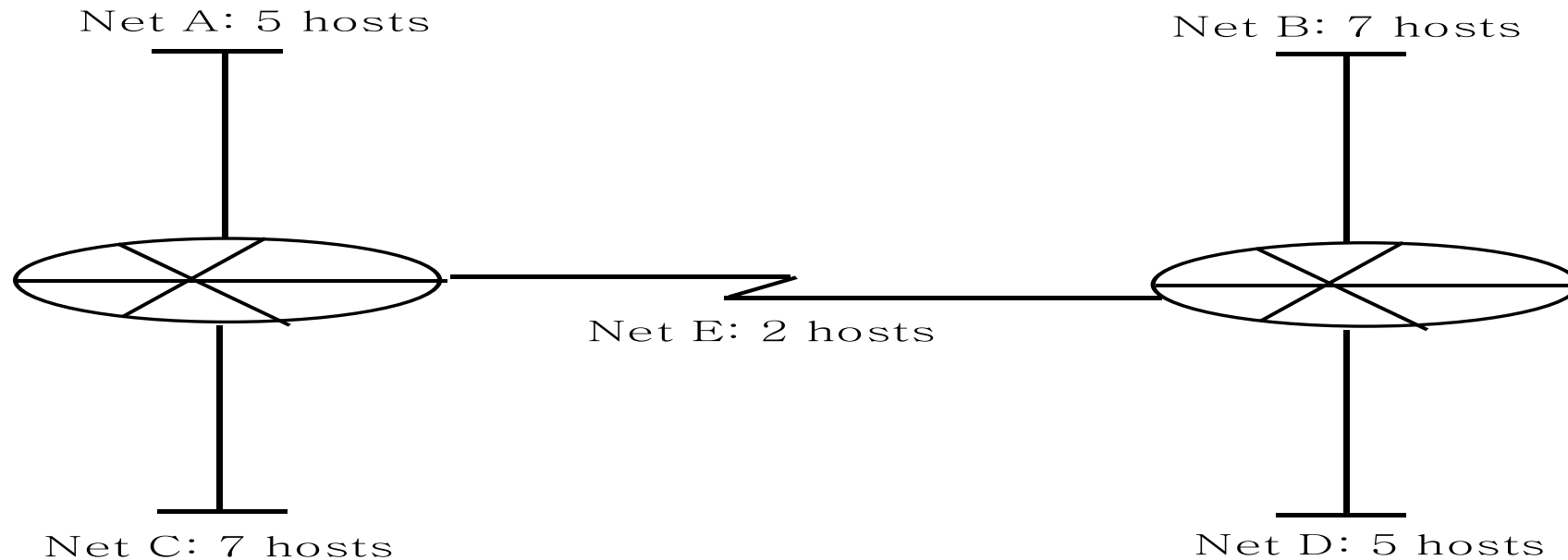
- Subnetting and supernetting is achieved by varying default subnet mask
- Usually in classful IP address have 8,16,24 default CIDR values for Class A, B, C respectively, but in classless IP no default CIDR value / subnet mask is available CIDR value may be varying

1.4.4. Subnetting/supernetting Steps

- Identify needed block size (always in power of 2 i.e. $2^2, 2^3, 2^4, \dots 2^{31}$)
 - If multiple block size is needed assign largest block first
- Find the host bits from block size (if block size 2^n no of host bit is n)
- From host bits find the CIDR (CIDR=32-n)
- Find subnet mask convert CIDR into doted decimal format (ex:255.255.240.0)
- Find wild card mask (255.255.255.255 - 255.255.240.0= 0.0.15.255)
- Add the first IP in the range to get last IP address

1.5 Subnetting Problem Example

- Class C network of 200.15.5.0 is given, subnet the network in order to create the network in the given figure with the host requirement shown.



1.5 Subnetting Problem Example

- Network Requirements

Network	No of Hosts	Total no of IP	Block size
A	5	7	8
B	7	9	16
C	7	9	16
D	5	7	8
E	2	4	4

- Number of hosts represents only valid HOST IP
- Total no of IP represents Host IP+ Network ID + broadcast ID
- Rule : Block size \geq Total no IP
- Assign blocks in ascending order(B,C,A,D,E)

Network B

Host IP needed = 7

No of IP required = 9 (Including Network ID and Broadcast ID)

Block size required $16 = 2^4$ (8 blocks is not enough because only 6 valid host)

No of host bit = 4

CIDR = $32 - 4 = 28$

Subnet mask = 255.255.255.240

Wild card mask = 0.0.0.15

200.15.5.0 + → First IP (given in Question)

0.0.0.15 → Wildcard mask

200.15.5.15 → Last IP in range

Valid host IP is in the range

200.15.5.0/28 → Network id

200.15.5.1/28

.

.

.

200.15.5.14/28



Valid Hosts

200.15.5.15/28 → Broadcast id

Network C

Host IP needed = 7

No of IP required = 9 (Including Network ID and Broadcast ID)

Block size required $16 = 2^4$ (8 blocks is not enough because only 6 valid host)

No of host bit = 4

CIDR = $32 - 4 = 28$

Subnet mask = 255.255.255.240

Wild card mask = 0.0.0.15

200.15.5.16 + → First IP (200.15.5.15 is already assigned)

0.0.0.15 → Wildcard mask

200.15.5.31 → Last IP in range

Valid host IP is in the range

200.15.5.16/28 → Network id

200.15.5.17/28

.

.

.

200.15.5.30/28

Valid Hosts

200.15.5.31/28 → Broadcast id

Network A

Host IP needed = 5

No of IP required = 7 (Including Network ID and Broadcast ID)

Block size required $8 = 2^3$

No of host bit = 3

CIDR = $32 - 3 = 29$

Subnet mask = 255.255.255.248

Wild card mask = 0.0.0.7

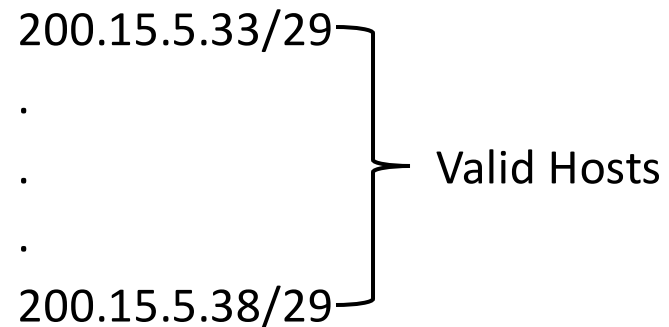
200.15.5.32 + → First IP (200.15.5.31 is already assigned)
0.0.0.7 → Wildcard mask

200.15.5.39 → Last IP in range

Valid host IP is in the range

200.15.5.32/29 → Network id

200.15.5.33/29
.
.
.
200.15.5.38/29



Valid Hosts

200.15.5.39/29 → Broadcast id

Network D

Host IP needed = 5

No of IP required = 7 (Including Network ID and Broadcast ID)

Block size required $8 = 2^3$

No of host bit = 3

CIDR = $32 - 3 = 29$

Subnet mask = 255.255.255.248

Wild card mask = 0.0.0.7

200.15.5.40 + → First IP (200.15.5.40 is already assigned)

0.0.0.7 → Wildcard mask

200.15.5.46 → Last IP in range

Valid host IP is in the range

200.15.5.38/29 → Network id

200.15.5.39/29

.

.

.

200.15.5.44/29



Valid Hosts

200.15.5.45/29 → Broadcast id

Network E

Host IP needed = 2

No of IP required =4 (Including Network ID and Broadcast ID)

Block size required $4 = 2^2$

No of host bit = 2

CIDR = $32-3=30$

Subnet mask =255.255.255.252

Wild card mask= 0.0.0.3

200.15.5.46 + → First IP (200.15.5.31 is already assigned)


0.0.0.3 → Wildcard mask

200.15.5.49 → Last IP in range

Valid host IP is in the range

200.15.5.46/30 → Network id

200.15.5.47/30
200.15.5.48/30



Valid Hosts

200.15.5.49/30 → Broadcast id

1.6. Limitations of IPv4

- Exponential growth of the Internet and the impending exhaustion of the IPv4 address space
- Need for simpler configuration
- Requirement for security at the IP level
- Need for better support for prioritized and real-time delivery of data

1.7. IPv6

- An IPv6 address consists of 16 bytes (octets); it is 128 bits long
- IPv6 specifies hexadecimal colon notation. In this notation,
- 128 bits is divided into eight sections, each 2 bytes in length. Two bytes in hexadecimal
- notation requires four hexadecimal digits. Therefore, the address consists of 32 hexadecimal
- digits, with every four digits separated by a colon
- 128 bits = 16 bytes = 32 hexadecimal digits
- IPv6 has a much larger address space; 2^{128} addresses are available

1.7. IPv6

Example IPv6

FDEC: 0074 : 0000 : 0000 : 0000 : BOFF : 0000 : FFFO

- Types of IPv6 Address
- Unicast address : Packet delivered to one node
- Multicast address : Packet delivered to group of nodes
- Any cast address : Similar to multicast but delivered to nearest node
- Reserved Address

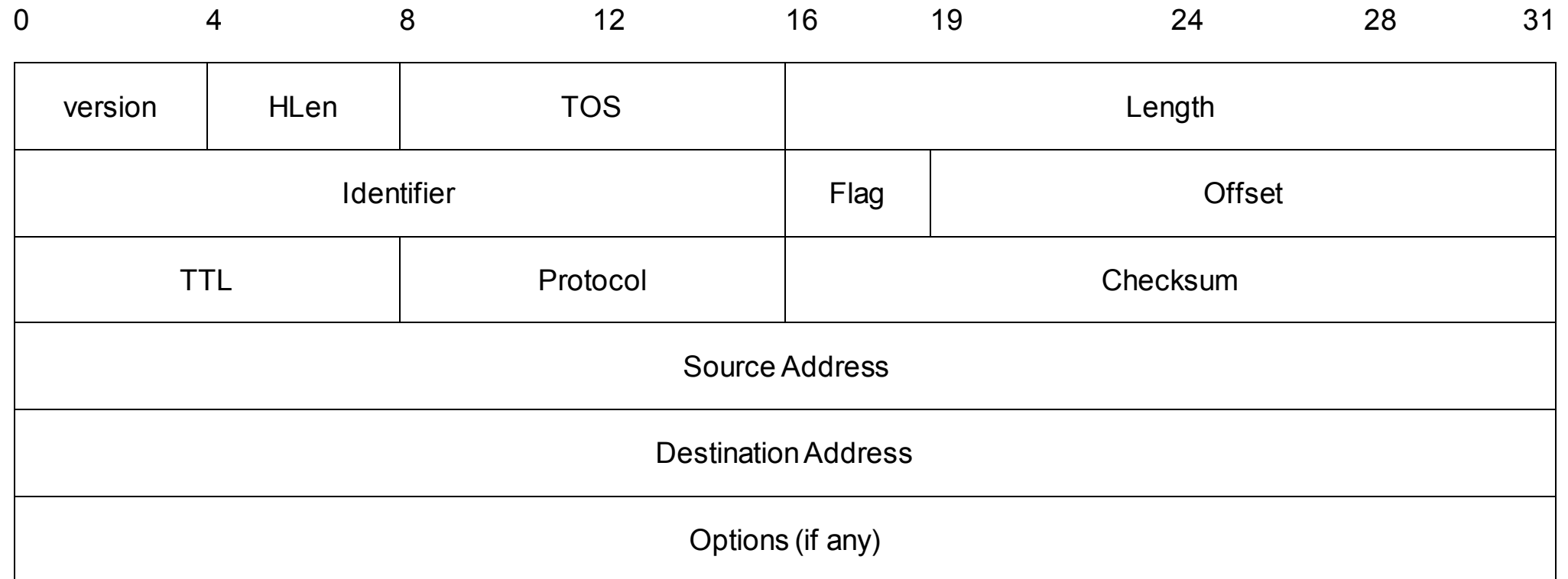
1.7.1. IPv6 Features

1. New header format
2. Large address space
3. Stateless and stateful address configuration
4. IPsec header support required
5. Better support for prioritized delivery
6. New protocol for neighboring node interaction
7. Extensibility

Comparison of IPv4 and IPv6

Feature	IPv4	IPv6
Address length	32 bits	128 bits
IPsec header support	Optional	Required
Prioritized delivery support	Some	Better
Fragmentation	Hosts and routers	Hosts only
Packet size	576 bytes	1280 bytes
Checksum in header	Yes	No
Options in header	Yes	No
Link-layer address resolution	ARP (broadcast)	Multicast Neighbor Discovery messages
Multicast membership	IGMP	Multicast Listener Discovery (MLD)
Router Discovery	Optional	Required
Uses broadcasts	Yes	No
Configuration	Manual, DHCP	Automatic, DHCPv6

1.8. IPv4 Header Format



1.8. IPv4 Header Format

- **Version (4 bits):** Indicates the version number, In this case 4
- **HLEN (Header Length ,4 bits):** Length of header in 32 bit words. The minimum value is five for a minimum header length of 20 octets
- **TOS (Type-of-Service , 8 bit):** The Type-of-Service field contains an 8-bit binary value that is used to determine the priority of each packet
- **Length (8 bits):** Total datagram/ packet length ,in bytes (octets)
- **Identifier (16 bits):** A sequence number that, together with the source address, destination address, and user protocol, is intended to uniquely identify a packet

1.8. IPv4 Header Format

- Flags(3 bits): Only two of the bits are currently defined
 1. MF(More Fragments) bit
 2. DF(Don't Fragment) bit
 3. Future use bit
- Fragment Offset : A router may have to fragment a packet when forwarding it from one medium to another medium that has a smaller MTU *. When fragmentation occurs, the IPv4 packet uses the Fragment Offset field and the MF flag in the IP header to reconstruct the packet when it arrives at the destination host.

* *MTU - Maximum Transfer Unit*

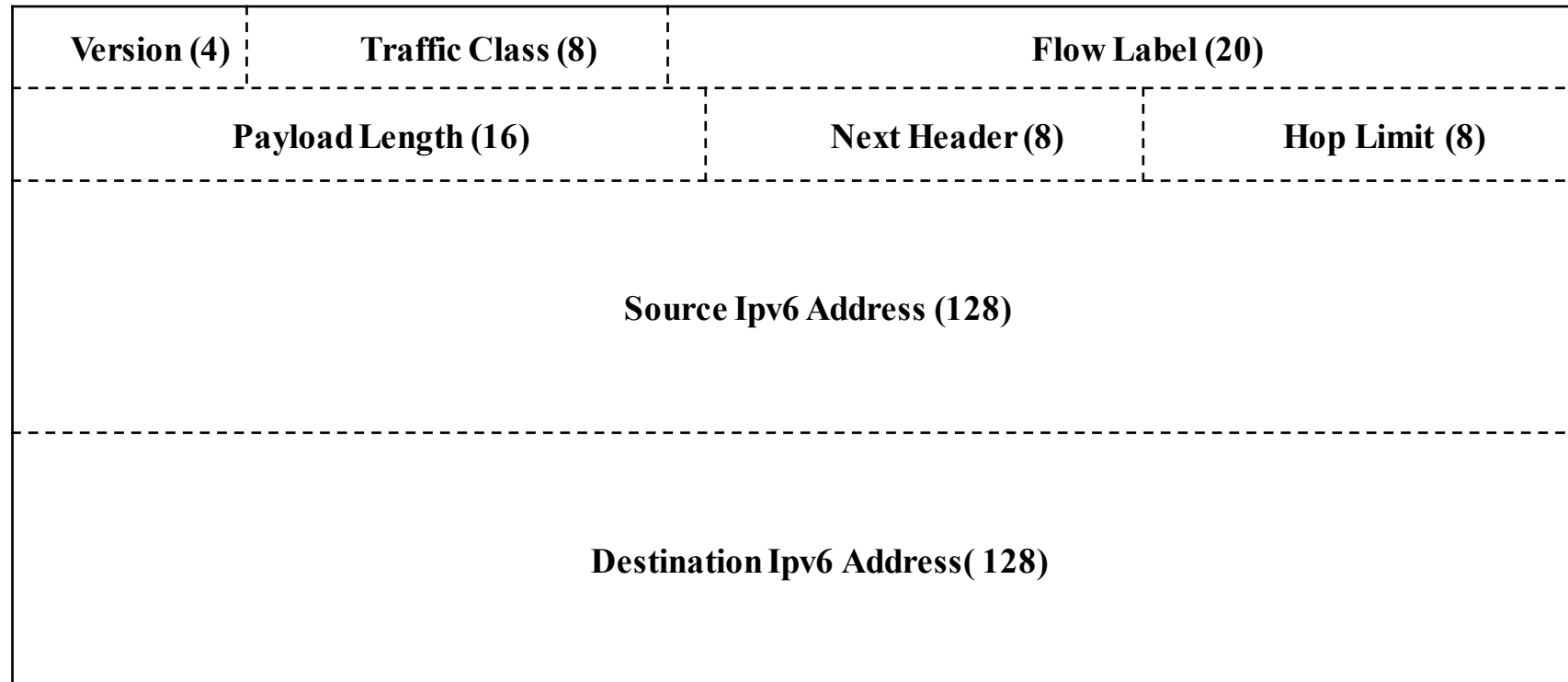
1.8. IPv4 Header Format

- **TTL (Time-to-Live, 8-bit):** Indicates the remaining "life" of the packet
- The TTL value is decreased by at least one each time the packet is processed by a router (that is, each hop). When the value becomes zero, the router discards or drops the packet and it is removed from the network data flow
- **Protocol (8-bits):** Indicates the data payload type that the packet is carrying (TCP/UDP).

1.8. IPv4 Header Format

- **Destination Address(32 bits):** value that represents the packet destination Network layer host address
- **Source Address (32 bit):** value that represents the packet source Network layer host address

1.9. IPv6 Header Format



1.9. IPv6 Header Format

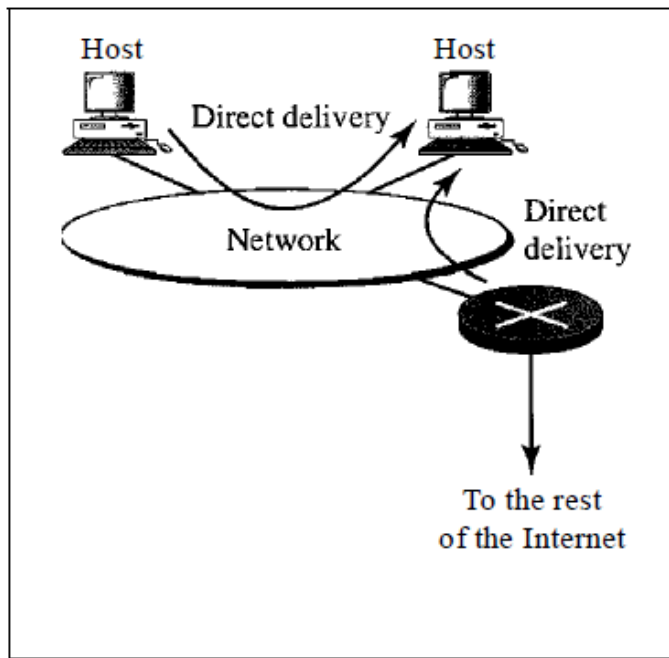
- **Version (4 bit):** Indicates version (6) of IP packet.
- **Traffic Class (8 bit):** Facilitates the handling of real time data by router. It Prioritize the packets (packet is send /dropped based on priority)
- **Flow Control (20 bit):** Used to label sequences of packets that require the same treatment for more efficient processing on routers.
- **Payload Length (16 bit):** Length of data carried after IPv6 header.

1.9. IPv6 Header Format

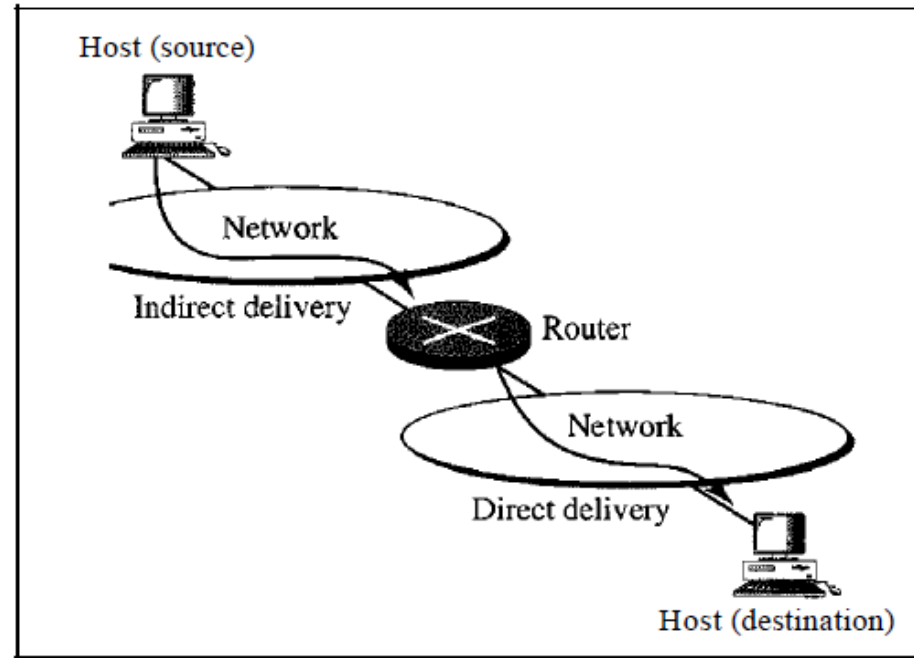
- **Next Header (8 bit):** Identifies the higher level protocol(identify the start of higher level header) **Hop Limit (8 bit):** This field indicates how long packet can remain in network.
- **Source Address (128 bit):** This Field indicates the IPv6 address from which packet is generated.
- **Destination Address (128 bit):** This field indicates the IPv6 address to which packet is going

2. Routing

- There is two types of packet delivery
 1. Direct delivery : inside a network(LAN)
 2. Indirect : between different network



a. Direct delivery



b. Indirect and direct delivery

2.1 Forwarding Techniques(Packet Forwarding)

- Forwarding means to place the packet in its route to its destination
- Forwarding requires a host or a router to have a routing table
- Forwarding techniques(based on routing table entry)
 1. Next hop method Vs Route method
 2. Network specific Vs Host specific
 3. Default route

2.1.1 Route based vs Next hop method

a. Routing tables based on route

Destination	Route
HostB	R1, R2, host B

Destination	Route
HostB	R2, host B

Destination	Route
HostB	HostB

Routing table
for host A

Routing table
for R1

Routing table
for R2

b. Routing tables based on next hop

Destination	Next hop
Host B	R1

Destination	Next hop
HostB	R2

Destination	Next hop
Host B	



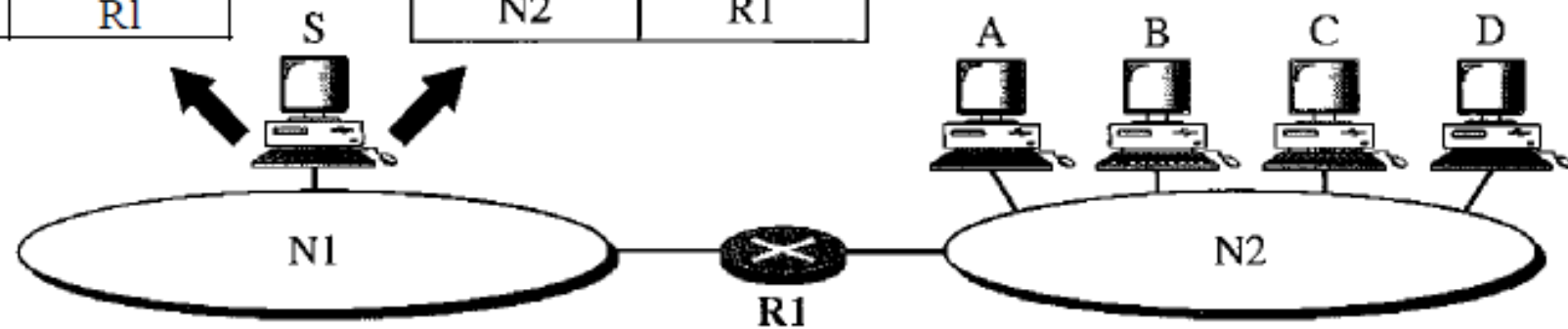
2.1.2. Host specific vs Network specific

Routing table for host S based on host-specific method

Destination	Next hop
A	R1
B	R1
C	R1
D	R1

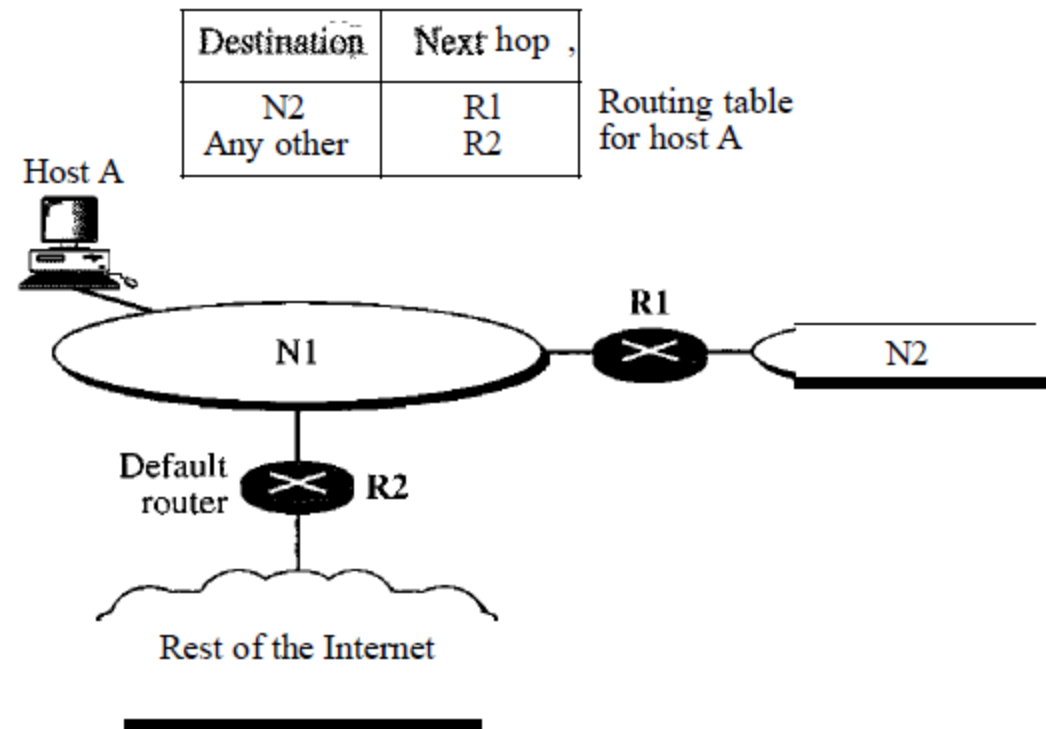
Routing table for host S based on network-specific method

Destination	Next hop
N2	R1



2.1.3. Default route

- Default route is entered in routing table with help of 0.0.0.0 (IP) which means any network.



2.2. Static Routing Table

- **Static routing table** contains information entered manually
- The administrator enters the route for each destination into the table
- The table must be manually altered by the administrator.
- A static routing table can be used in a small internet that does not change very often, or in an experimental internet for troubleshooting
- It is poor strategy to use a static routing table in a big network such as the Internet.

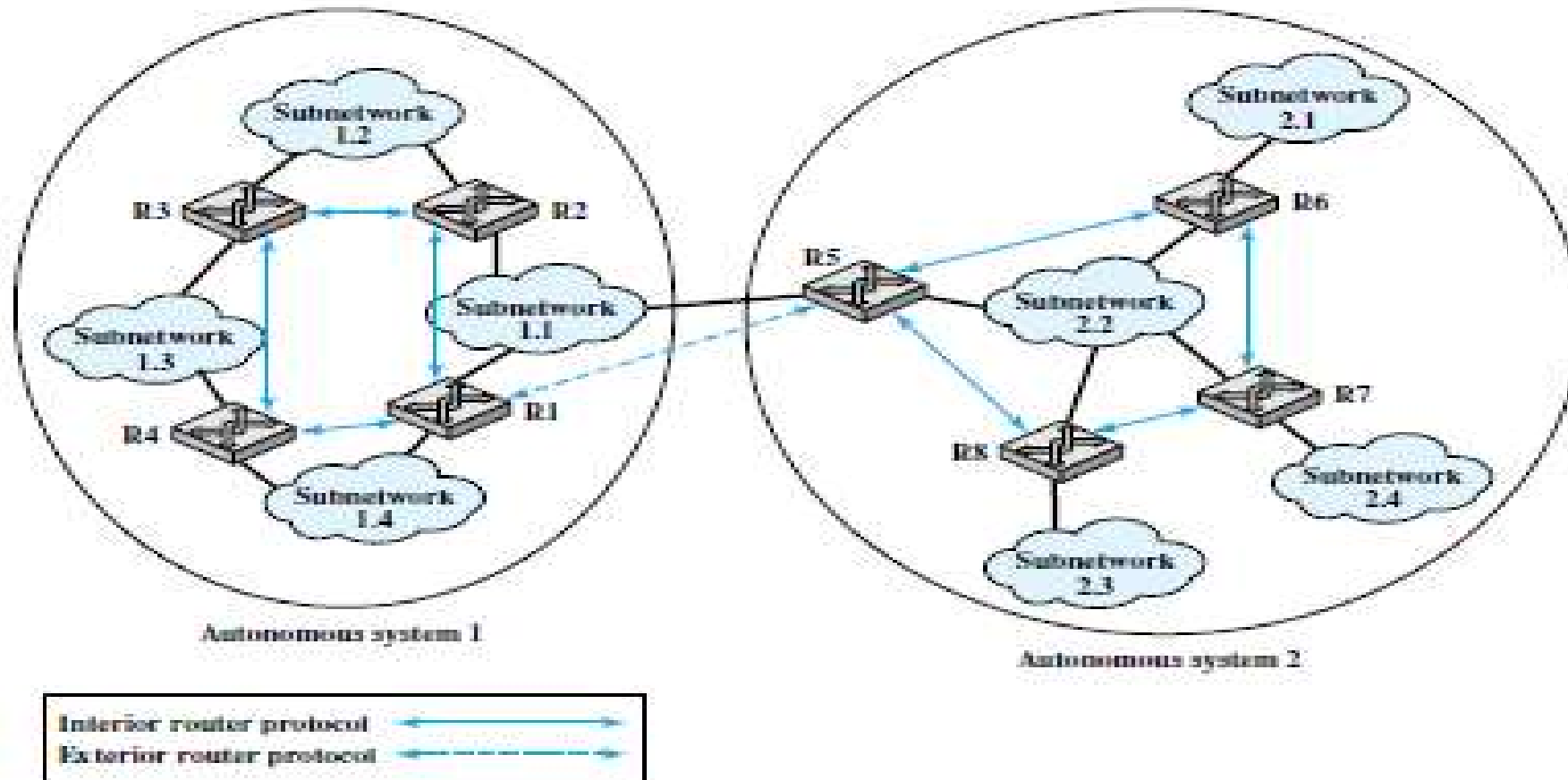
2.3. Dynamic Routing

- A dynamic routing table is updated periodically by using one of the dynamic routing protocols such as RIP, OSPF, or BGP.
- Whenever there is a change in the Internet, such as a shutdown of a router or breaking of a link, the dynamic routing protocols update all
- the tables in the routers (and eventually in the host) automatically.
- The routers in a big internet such as the Internet need to be updated dynamically for efficient delivery of the IP packets

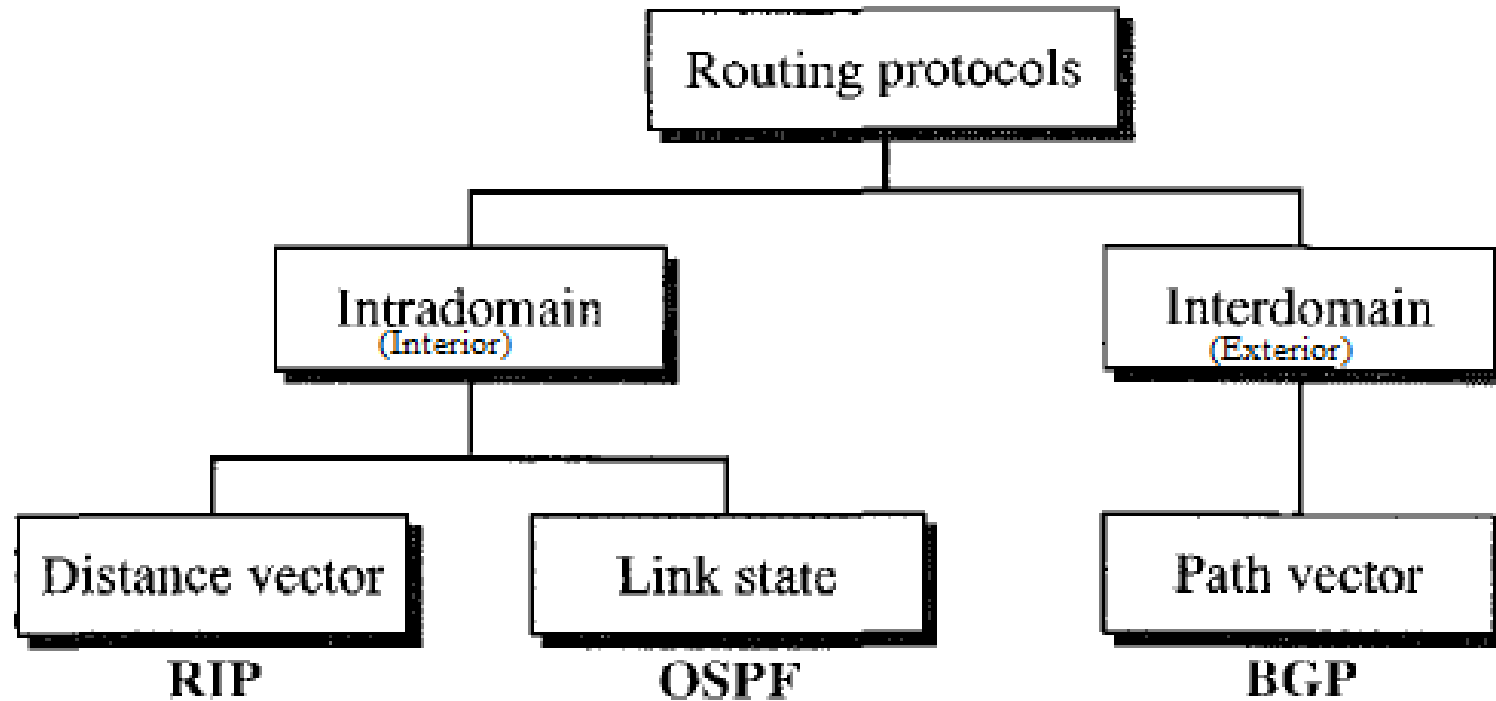
2.4. Autonomous System (AS)

- Large internet is divided into group of small networks
- AS is a group of networks and routers under the **authority of a single administration**
- Dynamic routing is divided into **interior and exterior** routing protocol
- Routing inside an autonomous system is referred to as **intra-domain routing (Interior Routing)**
- Routing between autonomous systems is referred to as **inter-domain routing (Exterior Routing)**
- Autonomous system can have one or more **intra-domain** routing protocols to handle routing inside the autonomous system

2.4.1 Interior and Exterior Routing in AS



2.4.1 Interior and Exterior Routing Protocols



2.5. Metrics

Metric in real world means measure

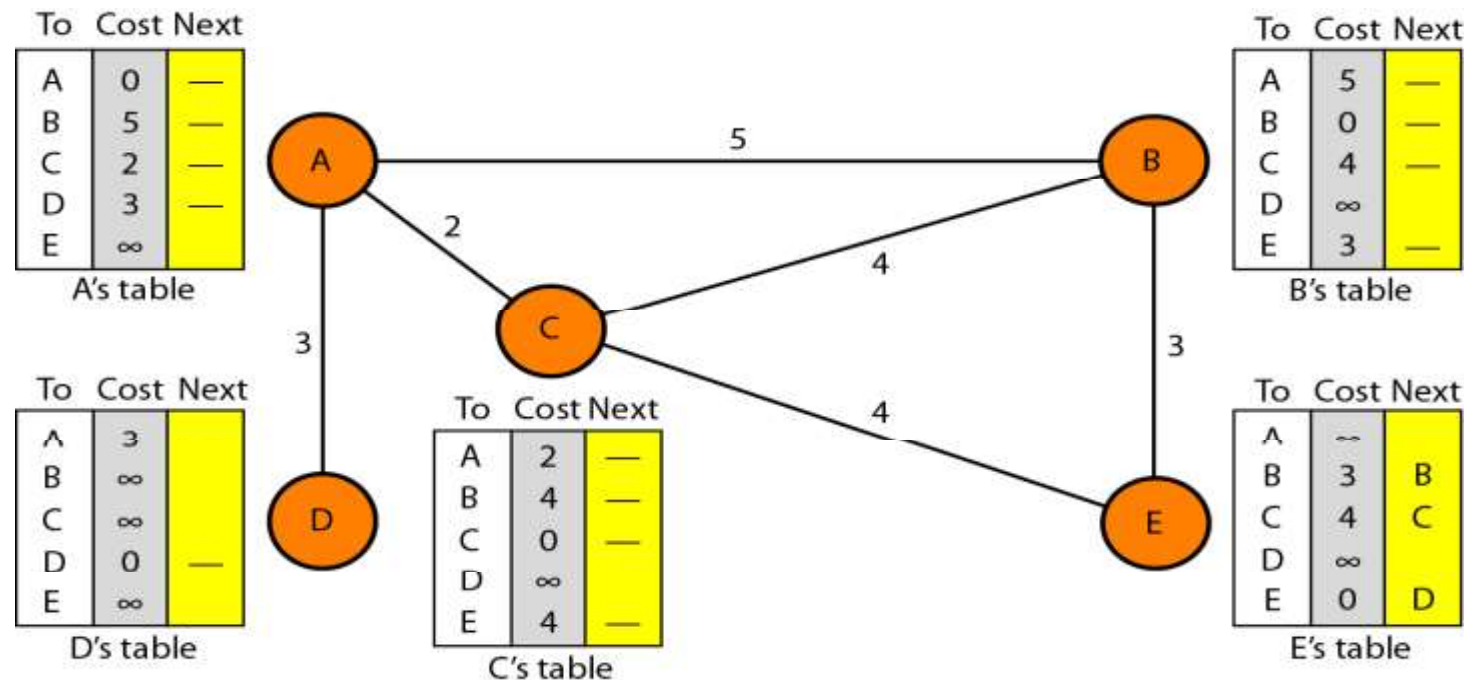
- **Router metrics** are metrics used by a router to make routing decisions
- Metric is the cost assigned for passing through a network
- The total metric of a particular route is equal to the metrics of networks that comprise the route
- A router chooses the route with smallest metric

2.6. Distance Vector Routing (RIP)

- Least-cost route between any two nodes is the route with minimum distance
- Each node maintains a set of triples(**Destination, Cost, NextHop**)
- The table at each node(router) also guides the packets to the desired node by showing the next stop in the route
- There is 2 steps in the route learning process
 1. Initialization
 2. Sharing

2.6.1. Initialization

- Initially routing table in each node consists the distance between itself and its immediate neighbours, those directly connected to it
- Not directly connected is marked infinite()

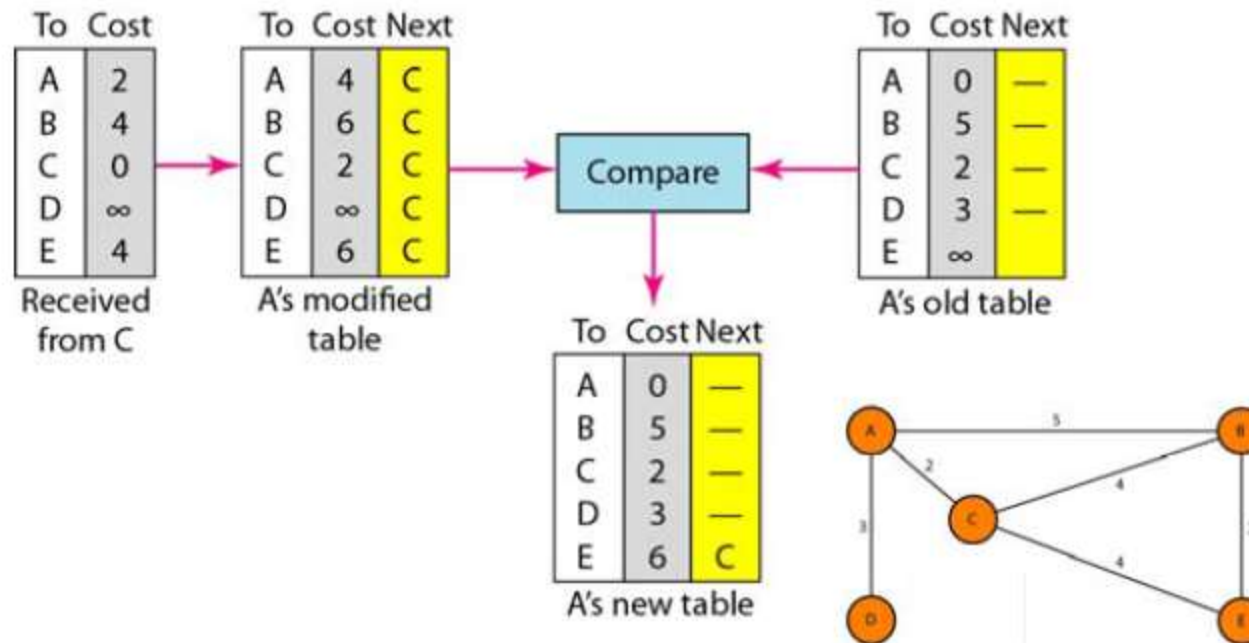


2.6.2. Sharing

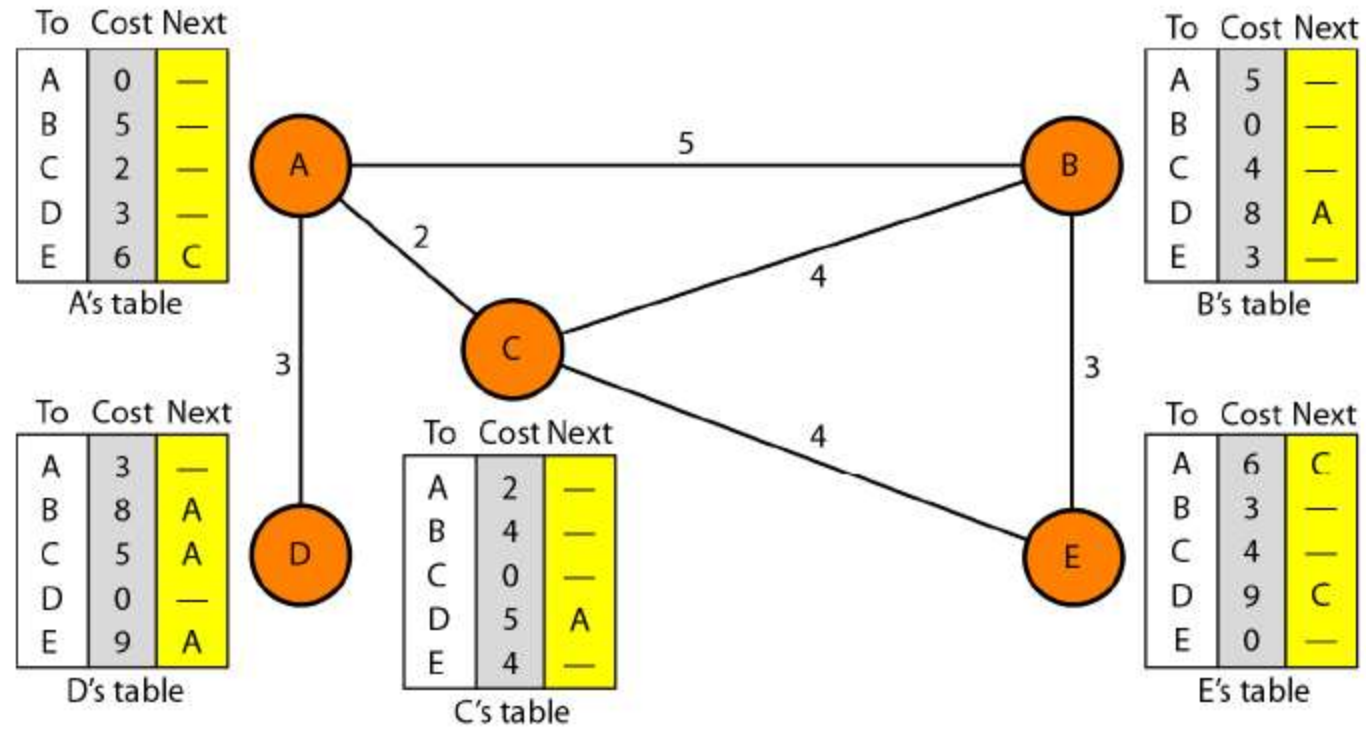
- 2 types of sharing(updates)
 1. Periodic
 2. Triggered
- Directly connected neighbours exchange(share) updates periodically (on the order of several seconds 30 sec)
- Whenever table changes (called *triggered* update)

2.6.3. Update Process

- Each update is a list of pairs: (**Destination, Cost**)
- Routing table will compare old routing table values with the shared table
- Updating of routing table is based on minimum cost



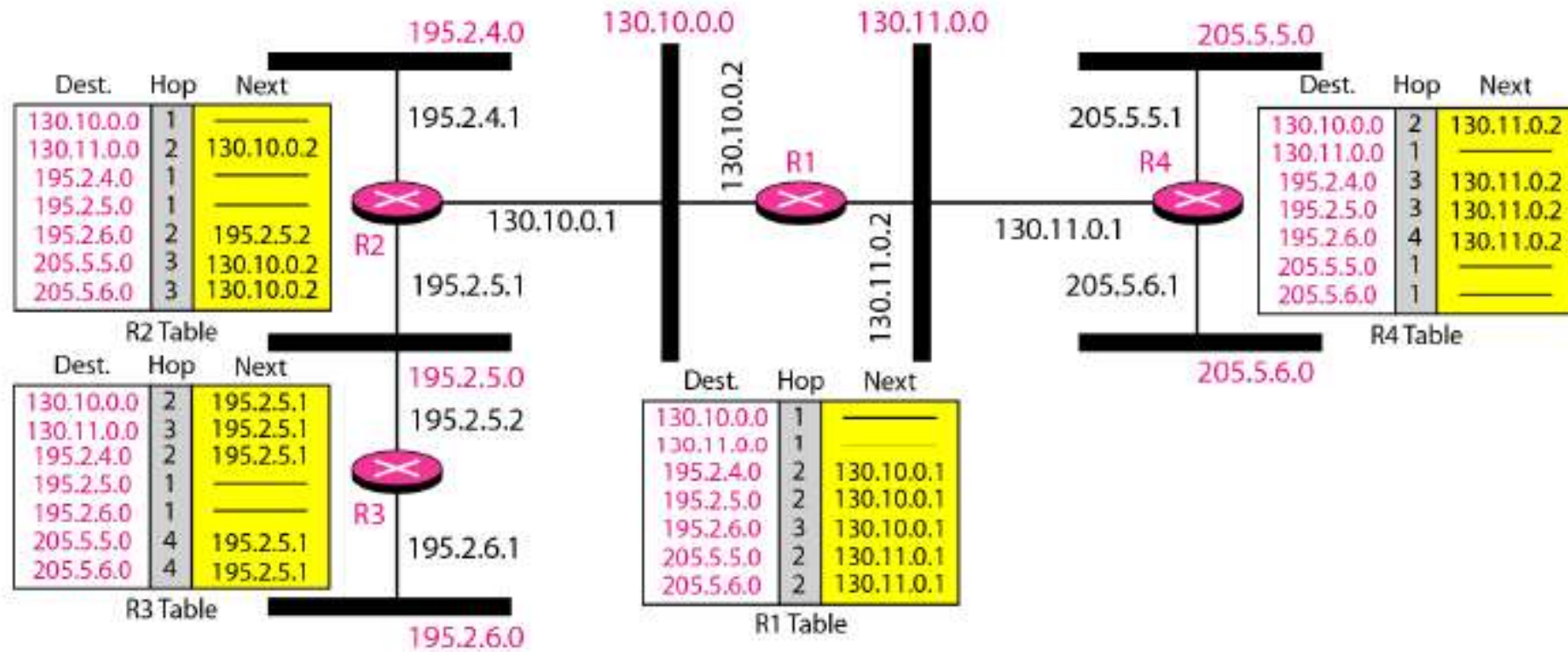
2.6.4. Final Routing Table



2.6.5. Routing Information Protocol(RIP)

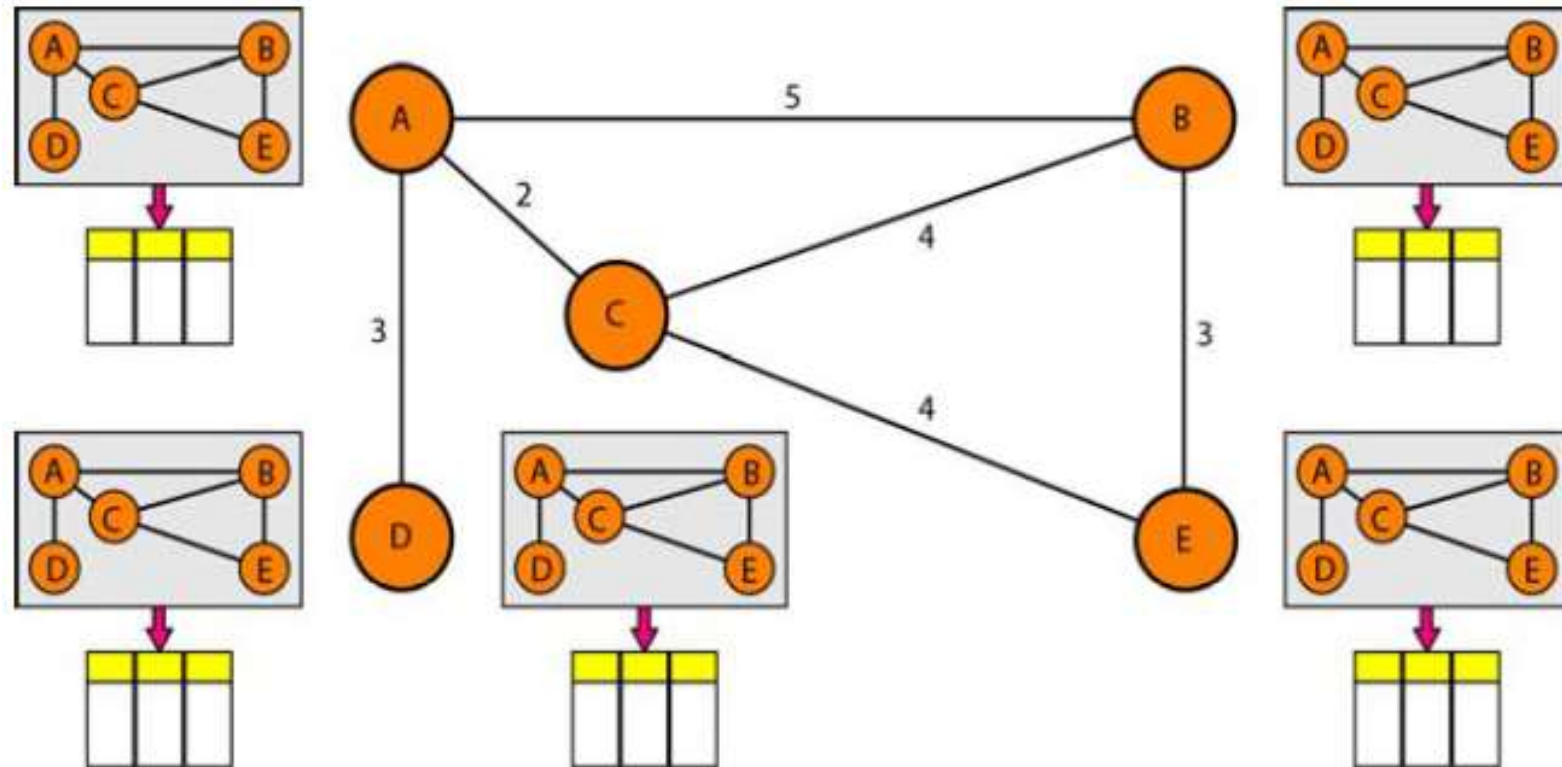
- RIP is based on Distance Vector(DV) routing protocol
- Interior routing protocol(Inside Autonomous System only)
- The destination in a routing table is a network, which means the first column defines a network address
- Distance is defined as the number of links (networks) to reach the destination(Hop counting)
- Metric in RIP is called a hop count(Number of router)
- Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops(Max 15 router)

2.6.6. RIP Routing Table



2.7. Link State Routing (OSPF)

- Each node in the domain has the entire topology of the domain.
- The node can use Dijkstra's algorithm to build a routing table.



2.7.1. Routing Table Updates in Link State

- Steps in Updating process
 1. Creation of the states of the links by each node, called the link state packet (LSP)
 2. Dissemination of LSPs to every other router, called **flooding**, in an efficient and reliable way
 3. Formation of a shortest path tree for each node
 4. Calculation of a routing table based on the shortest path tree

2.7.2. Link State packet

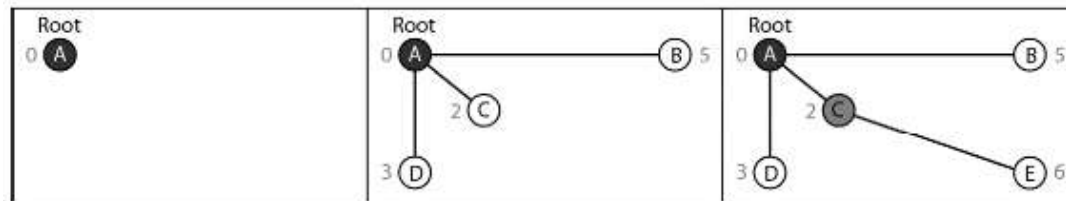
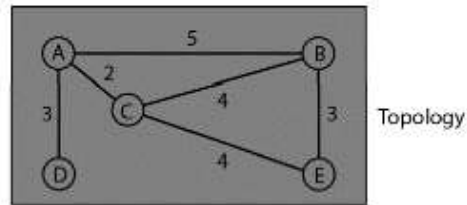
LSP consist of Following details

- ID of the node that created the LSP
- Cost of link to each directly connected neighbour
- Sequence number
- Time-to-live (TTL) for this packet
- Link State Packet Creation (LSP)
 1. *When there is a change in the topology of the domain*
 2. *Periodic (60 sec to 2 hours according to implementation)*

2.7.3. Routing table Updates

- Formation Shortest path tree In A

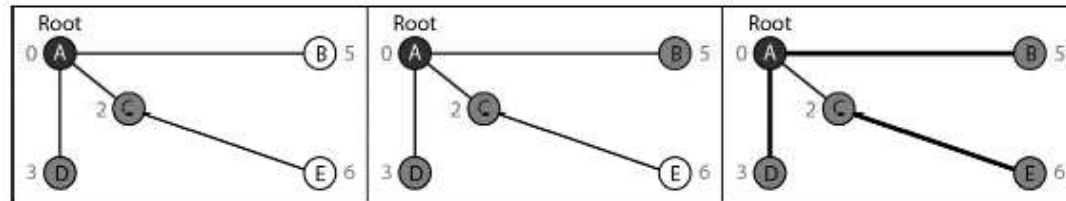
- Final Routing table of A



1. Set root to A and move A to tentative list.

2. Move A to permanent list and add B, C, and D to tentative list.

3. Move C to permanent and add E to tentative list.



4. Move D to permanent list.

5. Move B to permanent list.

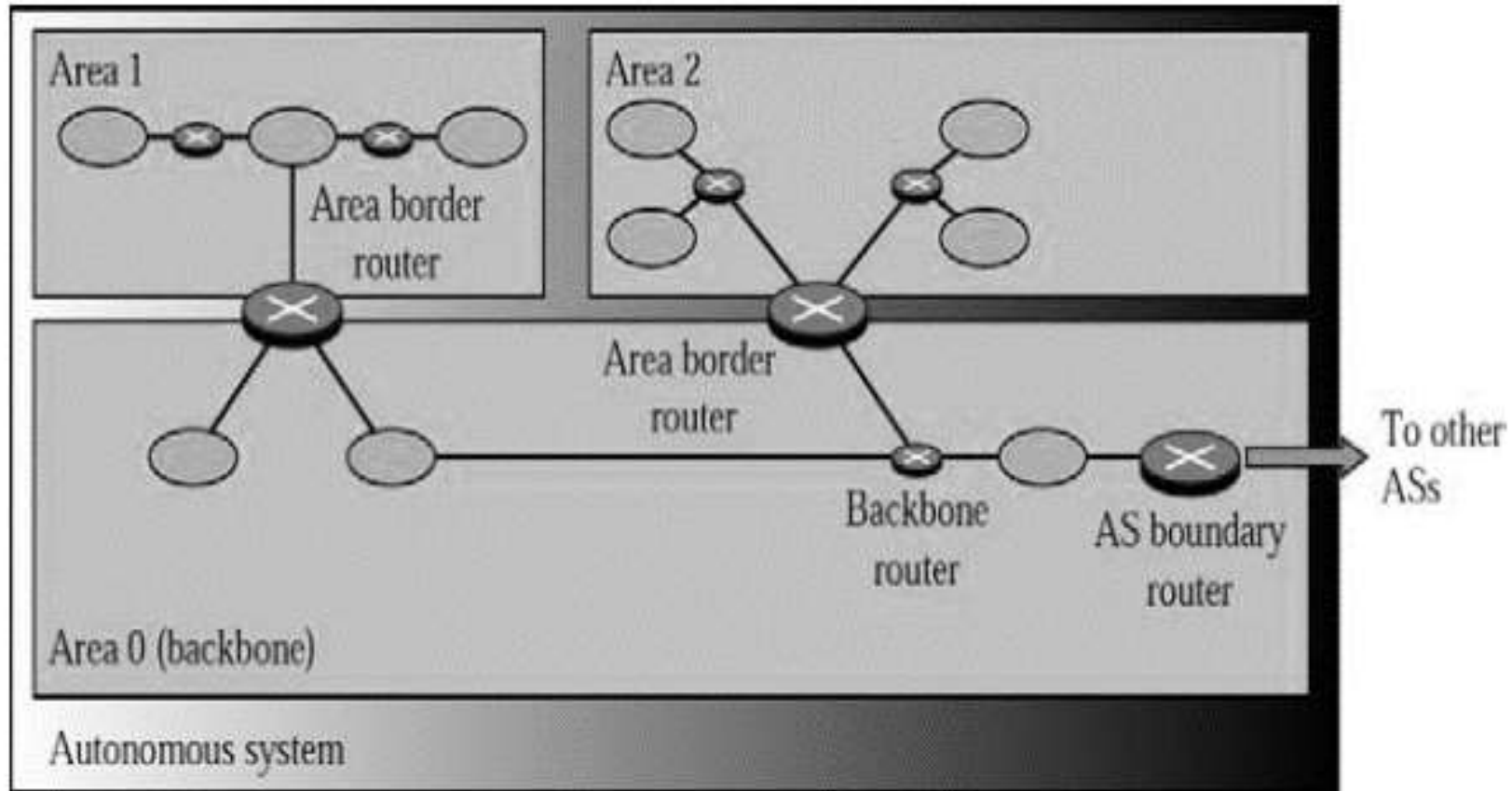
6. Move E to permanent list (tentative list is empty).

<i>Node</i>	<i>Cost</i>	<i>Next Router</i>
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

2.7.4. Open Shortest Path First(OSPF)

- OSPF divides an autonomous system into areas
- Each area is a collection of networks, hosts and routers
- Every router in the same area has the same link state database
- Special routers called autonomous system boundary routers are responsible for disseminate information about other autonomous systems into the current system.
- Metric used:
 - Administrator can assign the cost to each route based on type of service (minimum delay, maximum throughput...etc)

2.7.5. Autonomous System

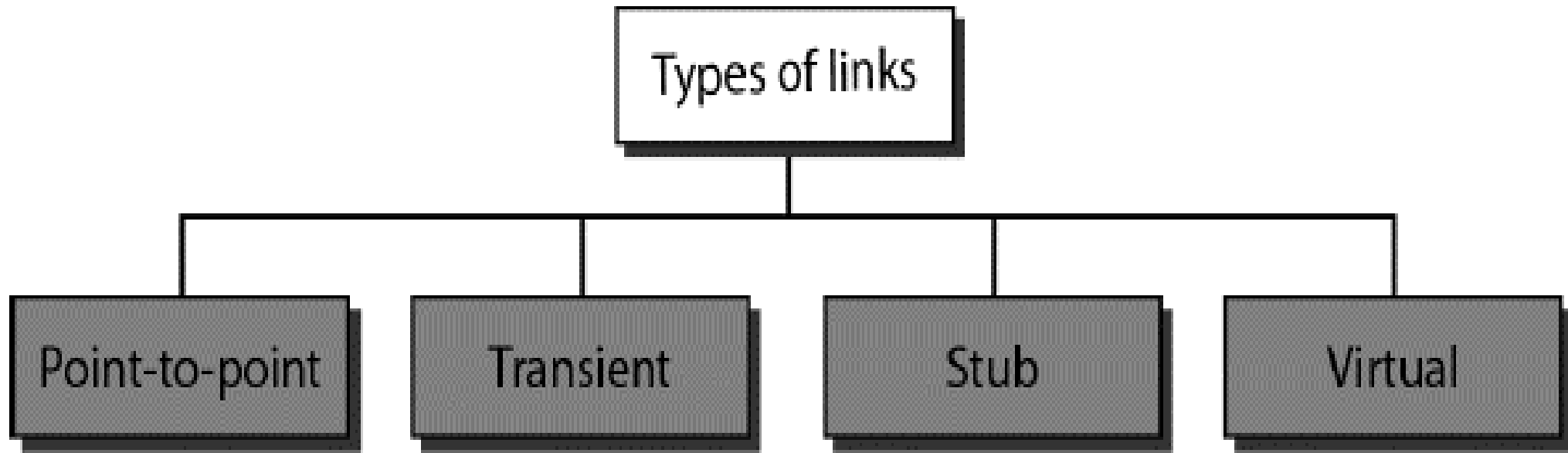


2.7.6. Areas in OSPF

- Area is a collection of networks, hosts, and routers all contained within an autonomous system.
- Routers inside an area flood the area with routing information.
- Area border routers: Summarize the information about the area and send it to other routers
- Backbone area [Primary area]: All the areas inside an autonomous system must be connected to the backbone
- Routers in the backbone area are called backbone routers. This area identification number is 0(in real world)

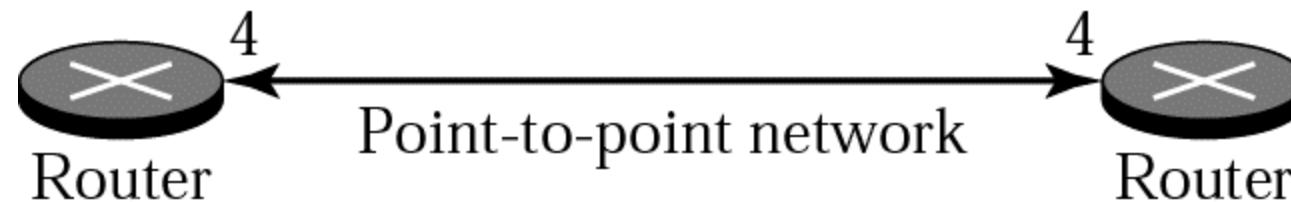
2.7.7. Types of Links in OSPF

- OSPF is based on Links
- There are 4 types of links



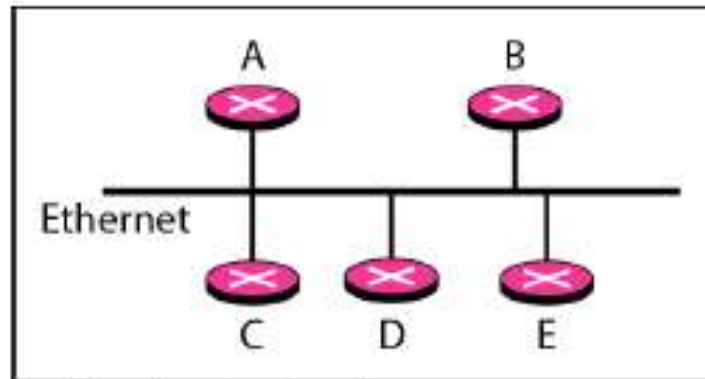
2.7.7.1. Point To Point

- Connects two routers without any other router or host in between.
- Directly connected routers using serial line.
- Only one neighbour for one router

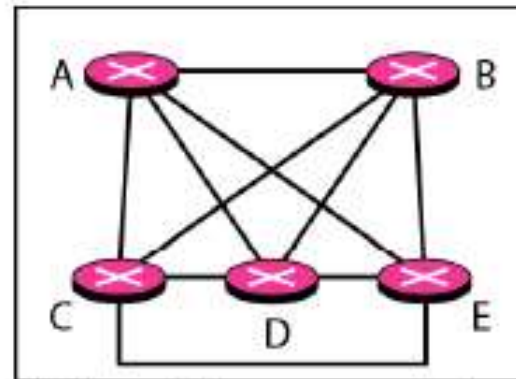


2.7.7.2. Transient Link

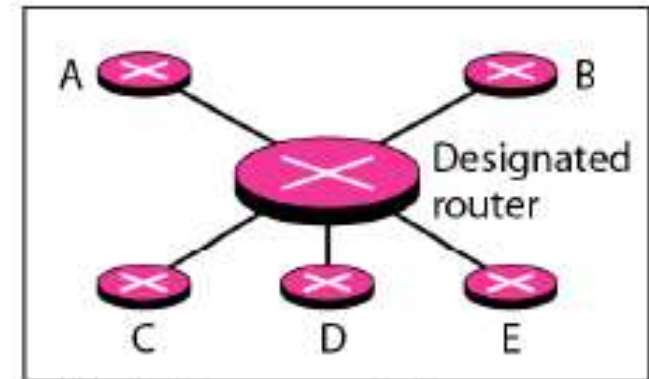
- A network with several routers attached to it
- Each router has many neighbours



a. Transient network



b. Unrealistic representation

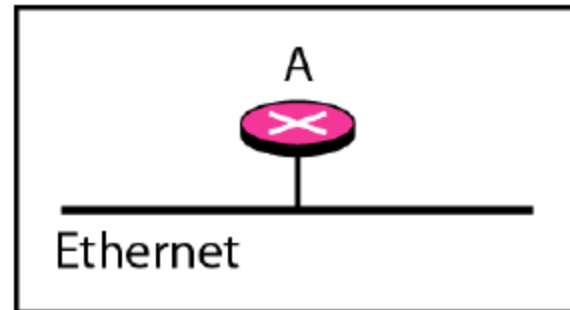


c. Realistic representation

NB : Ethernet in Figure A means all router is connected into a switch

2.7.7.3. Stub Link

- A **stub link** is a network that is connected to only one router
- The data packets enter the network through this single router and leave the network through this same router



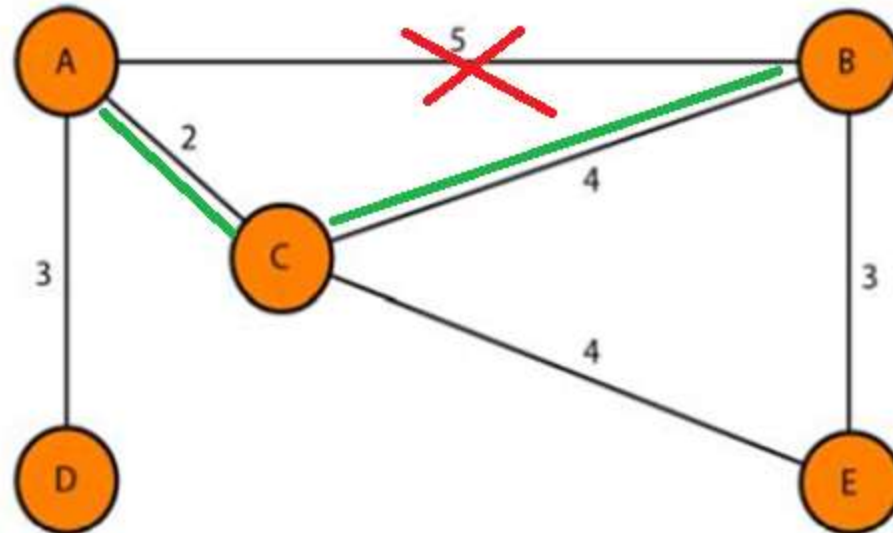
a. Stub network



b. Representation

2.7.7.4. Virtual Link

- When the link between two routers is broken, the administration may create a **virtual link** between them, using a longer path that probably goes through several routers
- Consider A to B (cost = 5) Link is broken , Link can be created from A to B through C (A-C-B , Cost =6)

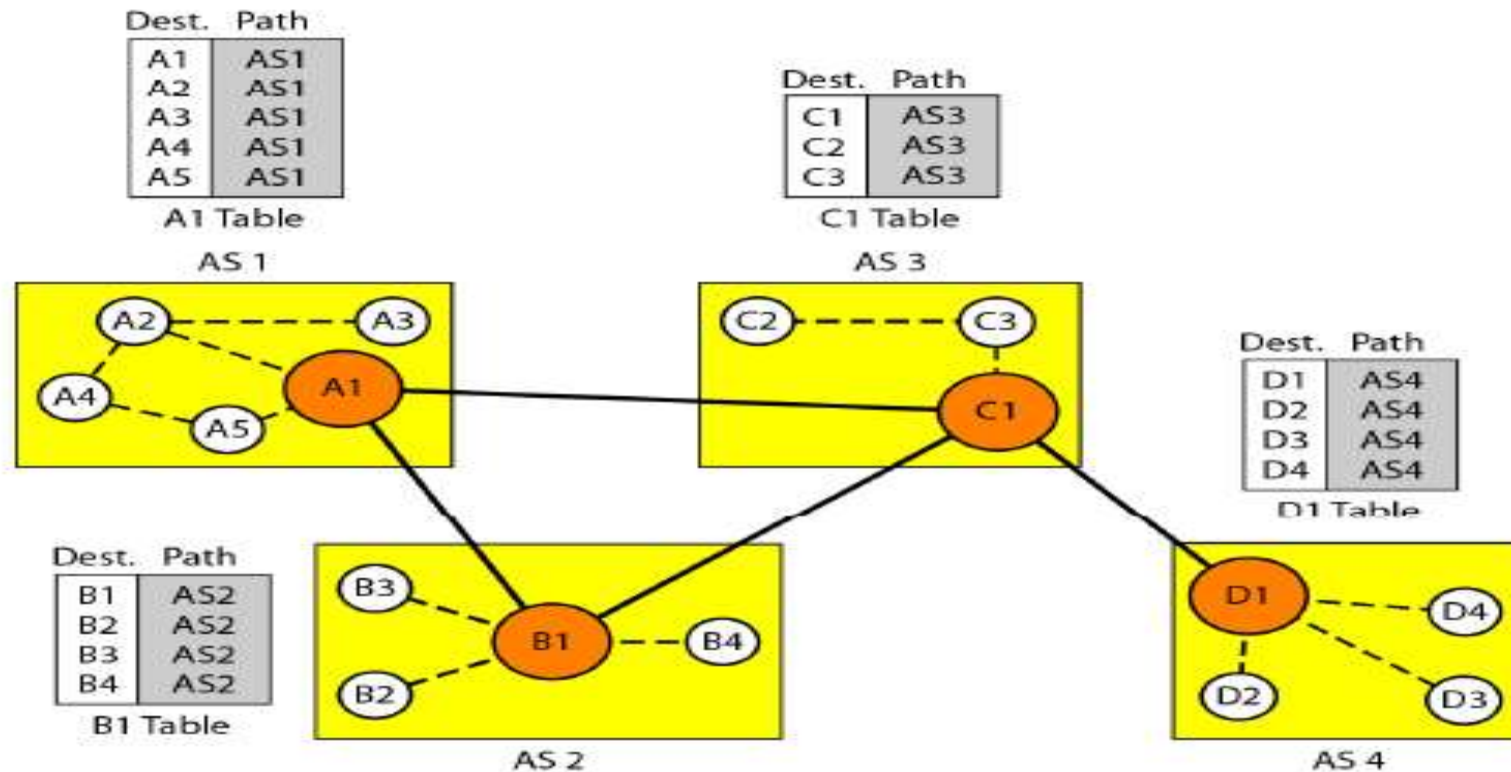


2.8. Path Vector (BGP)

- Path vector routing is inter domain routing protocol (exterior routing/ between AS)
- Each AS have at least one special node called speaker node
- Speaker node only can communicate with other AS
- In the Figure in next section A1, B1, C1, D1 are the speaker nodes.
- A speaker node advertises the path, not the metric of the nodes, in its autonomous system or other autonomous systems.

2.8.1. Initialization of Routing Tables

- Each speaker node have information of other node inside the AS only



2.8.2. Sharing & Updating of Routing Table

Sharing:

- Speaker nodes will share the information of AS to other AS

Updating:

- If multiple routes are received for a node path with minimum number of AS in between is selected.

2.8.3. Stable Routing Table

Dest.	Path
A1 ...	AS1
A5	AS1
B1 ...	AS1-AS2
B4	AS1-AS2
C1 ...	AS1-AS3
C3	AS1-AS3
D1 ...	AS1-AS2-AS4
D4	AS1-AS2-AS4

A1 Table

Dest.	Path
A1 ...	AS2-AS1
A5	AS2-AS1
B1 ...	AS2
B4	AS2
C1 ...	AS2-AS3
C3	AS2-AS3
D1 ...	AS2-AS3-AS4
D4	AS2-AS3-AS4

B1 Table

Dest.	Path
A1 ...	AS3-AS1
A5	AS3-AS1
B1 ...	AS3-AS2
B4	AS3-AS2
C1 ...	AS3
C3	AS3
D1 ...	AS3-AS4
D4	AS3-AS4

C1 Table

Dest.	Path
A1 ...	AS4-AS3-AS1
A5	AS4-AS3-AS1
B1 ...	AS4-AS3-AS2
B4	AS4-AS3-AS2
C1 ...	AS4-AS3
C3	AS4-AS3
D1 ...	AS4
D4	AS4

D1 Table

2.8.4. Border Gateway Protocol

- Inter domain (between AS) routing based on path vector
- Types of AS
 1. Stub AS
 2. Multihomed AS
 3. Transient AS
- Path attributes : List of attributes used by BGP to find best route
 1. Well Known Attribute
 2. Optional Attribute
- BGP Sessions: is a connection that is established between two BGP routers only for the sake of exchanging routing information
 1. E- BGP
 2. IBGP

2.8.4.1. Types of AS

- **Stub AS:** has only one connection to another AS. A host in one AS can send and receive data from another AS.
- **Multihomed AS:** Have many connections to a AS. It can send and receive data from many other AS. But will not allow data to pass through it.
- **Transient AS:** is a multihomed AS that also allows transient traffic (allow traffic to pass through)

2.8.4.2. Path Attributes

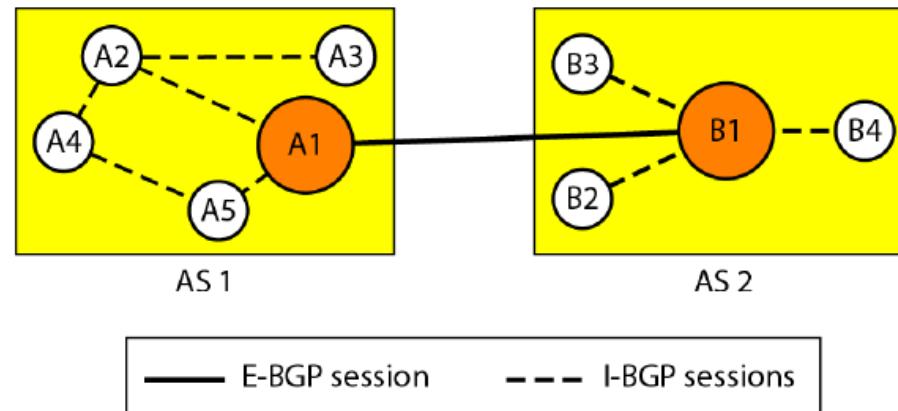
- **Well Known Attributes:** Attributes that BGP router must recognize, Its categories are:
 - **Well known mandatory :** is one that must appear in the description of a route.
 - **Well known discretionary :** is one that must be recognized by each router, but is not required to be included in every update message
- **Optional Attributes:** is one that needs not be recognized by every BGP router, Its categories are:
 - **Optional transitive attribute:** is one that must be passed to the next router by the router that has not implemented this attribute
 - **Optional nontransitive attribute:** is one that must be discarded if the receiving router has not implemented it

2.8.4.3. Path Attributes

- **Well Known Attributes:** Attributes that BGP router must recognize, Its categories are:
 - **Well known mandatory :** is one that must appear in the description of a route.
 - **Well known discretionary :** is one that must be recognized by each router, but is not required to be included in every update message
- **Optional Attributes:** is one that needs not be recognized by every BGP router, Its categories are:
 - **Optional transitive attribute:** is one that must be passed to the next router by the router that has not implemented this attribute
 - **Optional nontransitive attribute:** is one that must be discarded if the receiving router has not implemented it

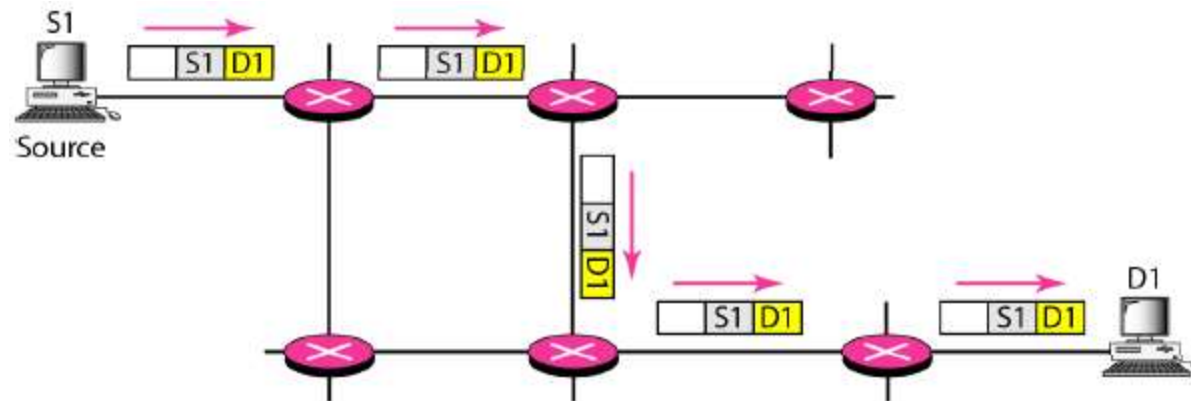
2.8.4.4. BGP Sessions

- A session is a connection that is established between two BGP routers only for the sake of exchanging routing information.
- BGP can have two types of sessions:
 1. **E-BGP(External) session:** is used to exchange information between two speaker nodes belonging to two different autonomous systems
 2. **I-BGP (Internal) session:** is used to exchange routing information between two routers inside an autonomous system



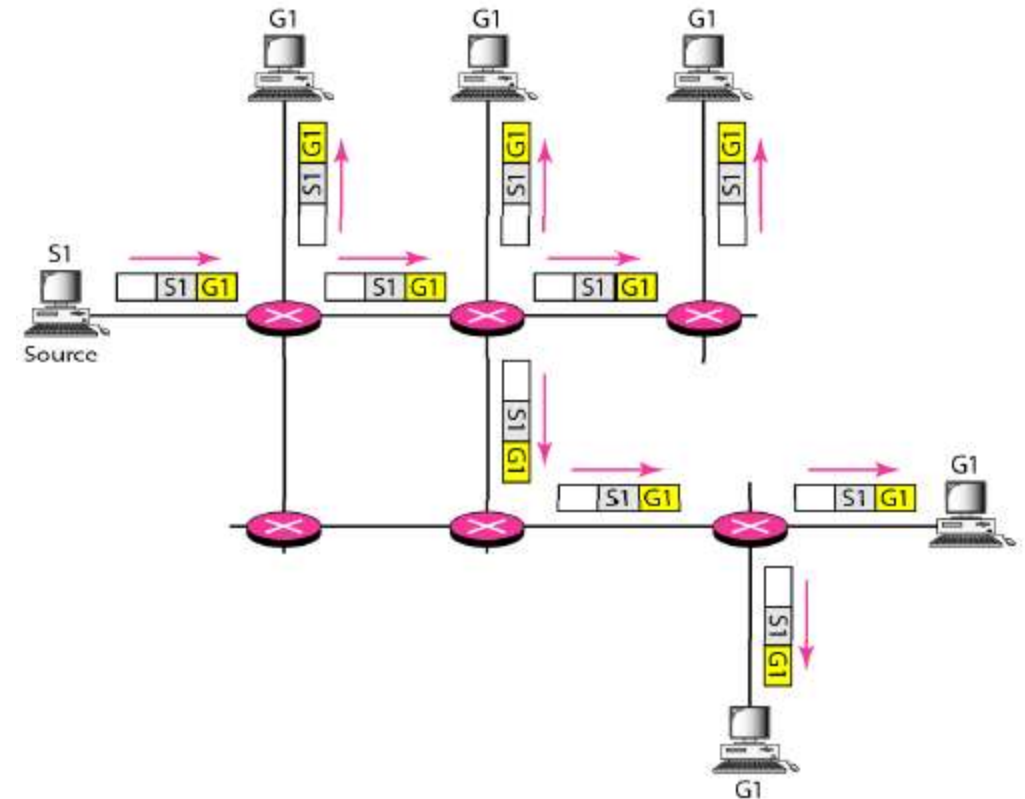
2.9. Unicasting vs Multicasting

- In unicast, the router forwards the received packet through only one of its interfaces
- Unicast (One to One)



2.9. Unicasting vs Multicasting

- In multicasting, the router may forward the received packet through several of its interfaces
- Multicasting (One to a Group)



Chapter 6

Transport Layer Protocols

Prepared By R.G.B

Visit For Notes: <http://sites.google.com/site/rohitgbal>

Email: rohitgbal@gmail.com

Contents

1. Process to Process delivery
 1. Multiplexing & De multiplexing
 2. Client Server
 3. Port Numbers
 4. Socket Address
2. Connection Oriented Vs Connection Less
3. Reliable Vs Unreliable
4. TCP
 1. Features
 2. TCP Segment
 3. 3-Way Handshaking Protocol
5. UDP
 1. Features
 2. UDP segments

Transport Layer overview

- Convert data from upper layer (Application) to segments
- Transport layer is responsible for process-to process delivery and congestion control
- Distinguish a particular process in a system using port number
- 3 type of delivery mechanisms available TCP, UDP,SCTP
- Connection oriented (TCP) and connection less(UDP)
- Reliable (TCP) and unreliable (UDP) services
- Port address provide process to process delivery

1. Process to Process Delivery

- The transport layer is responsible for process-to-process delivery
- Types of data delivering
 1. Node to node delivery (data link Layer)
 2. Host to host delivery (Network Layer)
 3. Process to process delivery (Transport Layer)
- Process to process delivery is needed because many process will be running in one host simultaneously
- To identify, from which process is sending the request source port address is assigned
- To identify, to which process request is send is destination address is assigned

1. Process to Process Delivery

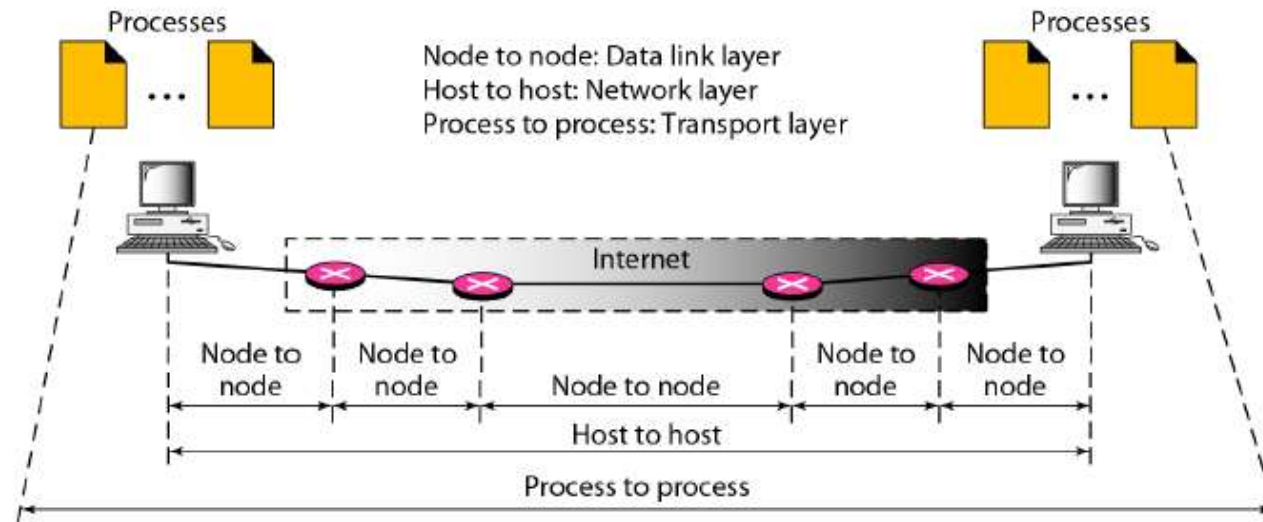
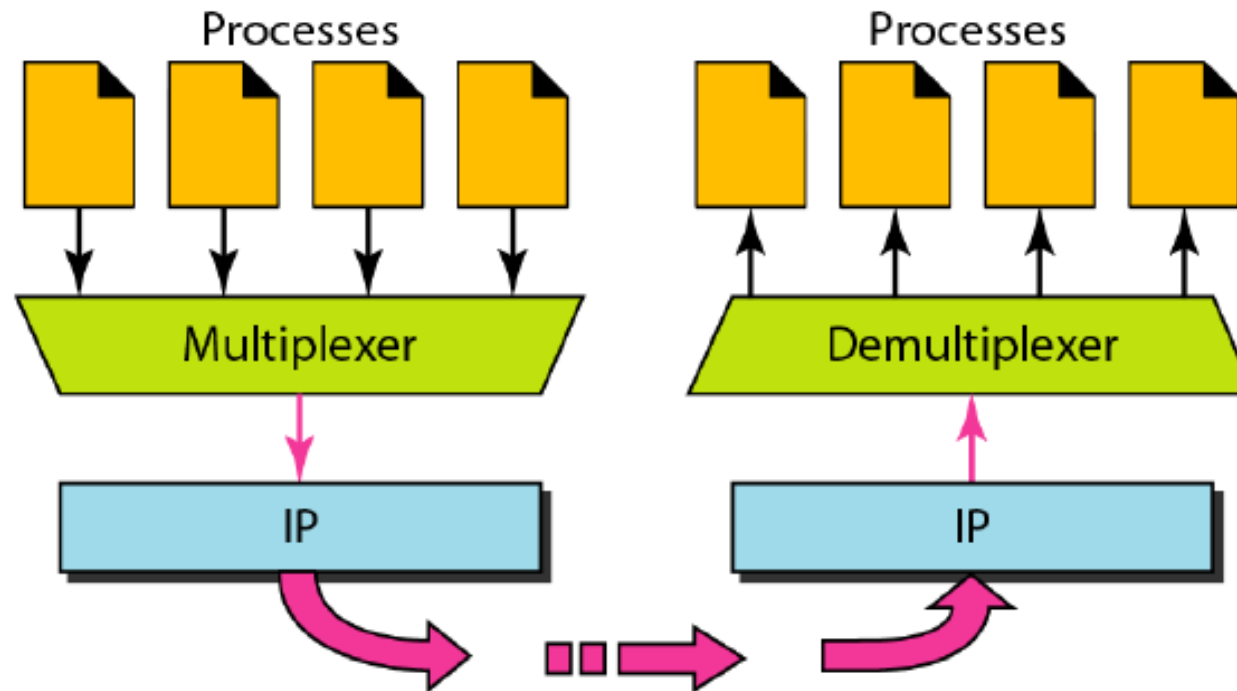


Figure: Process to Process Delivery

- Two processes communicate in a client/server relationship

1.1. Multiplexing & De-multiplexing

- The addressing mechanism allows multiplexing and De-multiplexing by the transport layer



1.1.1. Multiplexing

- At the sender site, there may be several processes that need to send packets. However, there is only one transport layer protocol at any time. This is a many-to-one relationship and requires multiplexing.
- The protocol accepts messages from different processes, differentiated by their assigned port numbers. After adding the header, the transport layer passes the packet to the network layer

1.1.2. De-multiplexing

- At the receiver site, the relationship is one-to-many and requires De-multiplexing. The transport layer receives datagrams from the network layer.
- After error checking and dropping of the header, the transport layer delivers each message to the appropriate process based on the port number

1.2. Client Server

- Most common way to achieve process-to-process communication in internet is through the client/server paradigm.
- A process on the local host, called a client, needs services from a process usually on the remote host, called a server
- Operating systems today support both multiuser and multiprogramming environments.
- A remote computer can run several server programs at the same time, just as local computers can run one or more client programs at the same time

1.2. Client Server

- Here 2 types of address is needed for communication **Host Address and Process Port number**
- For communication, we must define the following:
 1. Local host : IP address of Client
 2. Local process : Port number of client
 3. Remote host: IP address of Server
 4. Remote process: Port address of server

1.2. Client Server

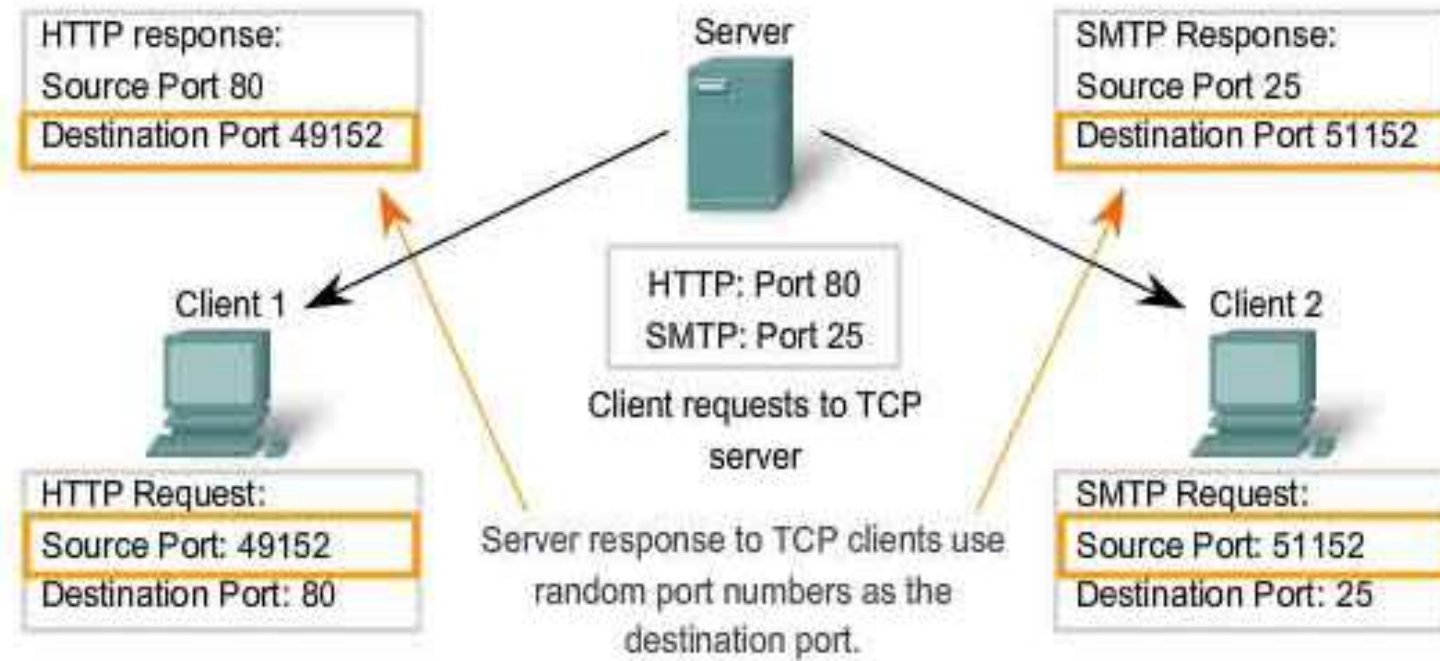


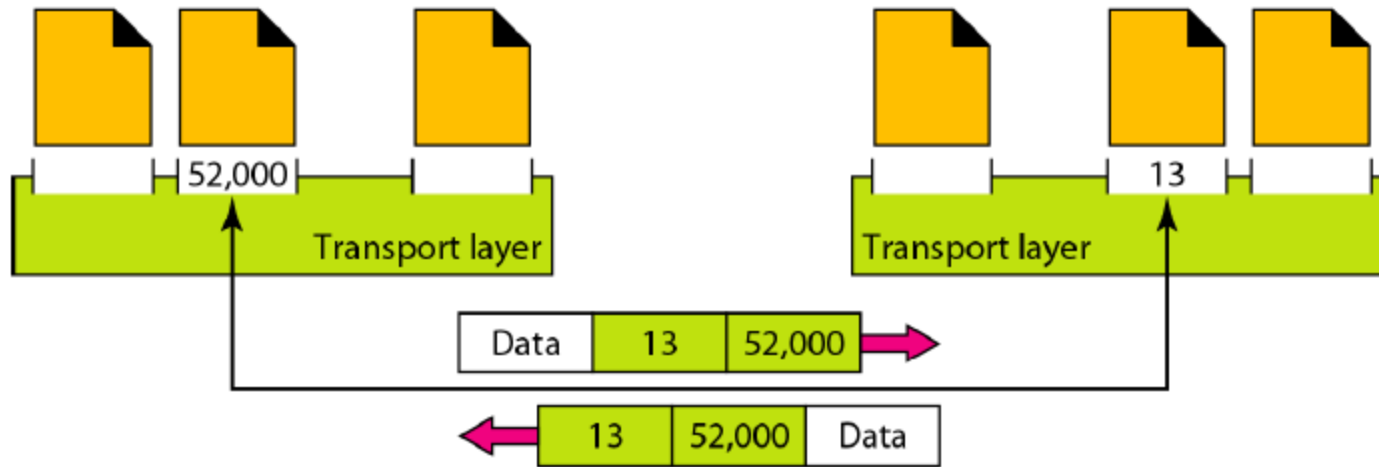
Figure Client sending

1.3. Port Numbers

- Port Address (Number) is needed to choose among multiple processes running on the destination host
- The destination port number is needed for delivery and the source port number is needed for the reply
- Port number is 16 bit integer
- Range between 0-65535
- Source port number is chosen randomly(Dynamic range)
- Destination port is chose based on application(For ex, HTTP-80, FTP-20,21)

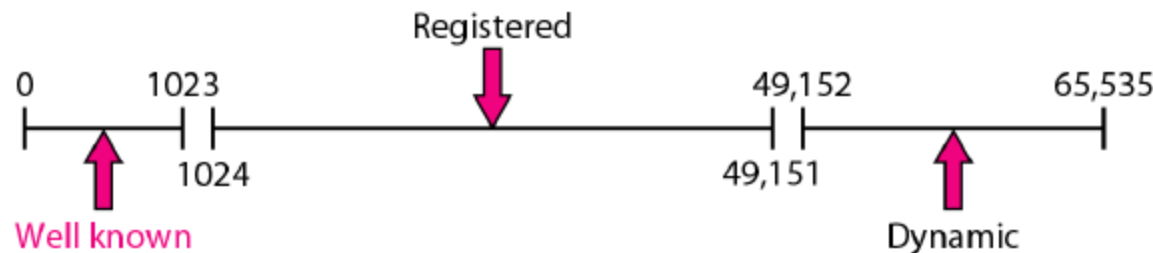
1.3. Port Numbers

- Data is sent from system one have process with port number 52000 and other system have a process with port number 13



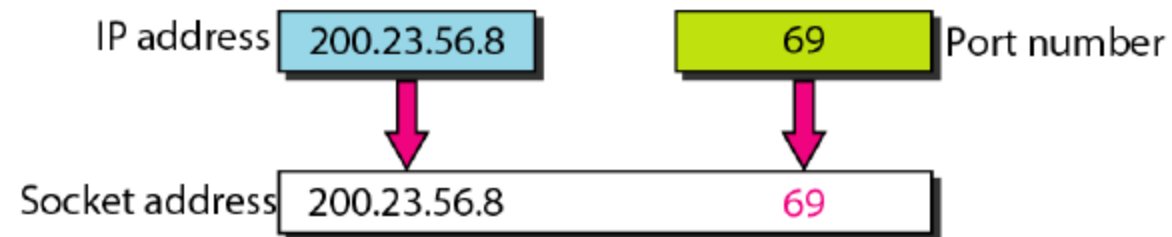
1.3.1. Port numbers- IANA ranges

- The IANA (Internet Assigned Number Authority) has divided the port numbers into three ranges:
- Well known ports (Range between 0-1023): Controlled by IANA
- Registered ports (Range between 1024-49151): not controlled by IANA but can be register to prevent duplication
- Dynamic(Private) ports (Range between 49152-65535): The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used by any process



1.4. Socket Address

- Process-to-process delivery needs **two identifiers, IP address** and the **port number**, at each end to make a connection
- Combination of an **IP address** and a **port number** is called a **socket address**
- The client socket address defines the client process uniquely just as the server socket address defines the server process uniquely
- A transport layer protocol (TCP/UDP) needs a pair of socket addresses: the source socket address and the destination socket address



2.1 Connection Less(UDP)

- Packets are sent from one party to another with no need for connection establishment or connection release
- The packets are not numbered
- They may be delayed or lost or may arrive out of sequence
- There is no acknowledgment
- UDP is connectionless

2.2 Connection Oriented(TCP)

- Connection is first established between the sender and the receiver
- Data are transferred
- Connection is released
- TCP and SCTP are connection-oriented protocols

3 Reliable vs Unreliable

Reliable

- Have error control
- Have Flow control
- Connection oriented
- Have ACK and sequence number
- TCP &SCTP

Unreliable

- No error control
- No Flow control
- Connectionless
- No ACK and sequence number
- UDP

4. Transmission Control Protocol(TCP)

- Connection oriented & Reliable Service
- TCP uses flow and error control mechanisms at the transport level
- TCP uses port numbers for communication

Well Known TCP Ports

- FTP- 20(data), 21(control)
- TELNET- 23
- SMTP-25
- DNS-53
- HTTP-80
- RPC-111

4.1. TCP Features

- Stream delivery (No boundary defined)
- Full duplex communication
- Numbering systems
 - TCP software keeps track of the segments being transmitted or received, there is no field for a segment number value in the segment header
 - The bytes of data being transferred in each connection are numbered by TCP. The numbering starts with a randomly generated number
- Sequence Number:
 - The sequence number for each segment is the number of the first byte (randomly assigned) carried in that segment

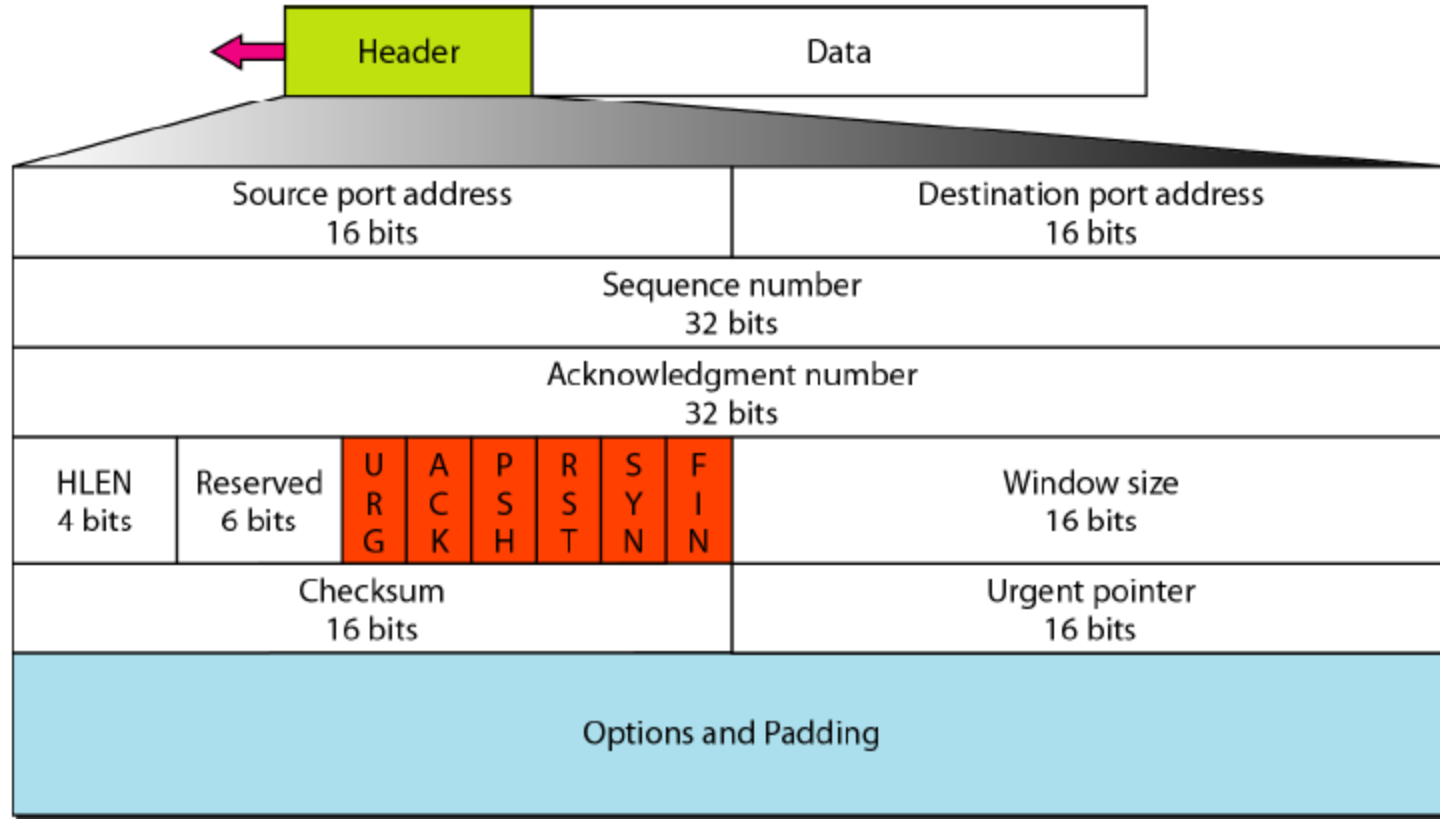
4.1. TCP Features

- Acknowledgment number:
 - Full duplex sequence number and Acknowledgment in same segment
 - If receiver receives x bytes Ack number is equal to $x+1$
- Flow control& Error control:
 - TCP uses byte oriented flow & error control
- Congestion control
 - Also control the congestion in the network

4.1.1 TCP Sequence numbering

- Suppose a TCP connection is transferring a file of 5000 bytes. The first byte is numbered 10,001. Each carrying segment carry 1000 bytes. The following shows the sequence number for each segment:
 - Segment 1 Sequence Number: 10,001 (range: 10,001 to 11,000)
 - Segment 2 Sequence Number: 11,001 (range: 11,001 to 12,000)
 - Segment 3 Sequence Number: 12,001 (range: 12,001 to 13,000)
 - Segment 4 Sequence Number: 13,001 (range: 13,001 to 14,000)
 - Segment 5 Sequence Number: 14,001 (range: 14,001 to 15,000)

4.2. TCP Segment Format



4.2. TCP Segment Format

- Source port address: Port address of sender
- Destination port address: port address of receiver
- Sequence number: 32 bit integer usually represented by first bytes number
- Acknowledge number: 32 bit integer, x bytes are received Ack will be $x+1$
- Header Length (HLEN) : usually between 20-60 bytes
- Reserved: future use

4.2. TCP Segment Format

- Flag (6 bits):
 1. URG: Urgent pointer is valid
 2. ACK: Acknowledgment is valid
 3. PSH: Request for push
 4. RST: Reset the connection
 5. SYN: Synchronize sequence numbers
 6. FIN: Terminate the connection
- Window size
 - This field defines the size of the window, in bytes, that the other party must maintain. 16 bit so maximum size of the window is 65,535 bytes. Usually determined by receiver

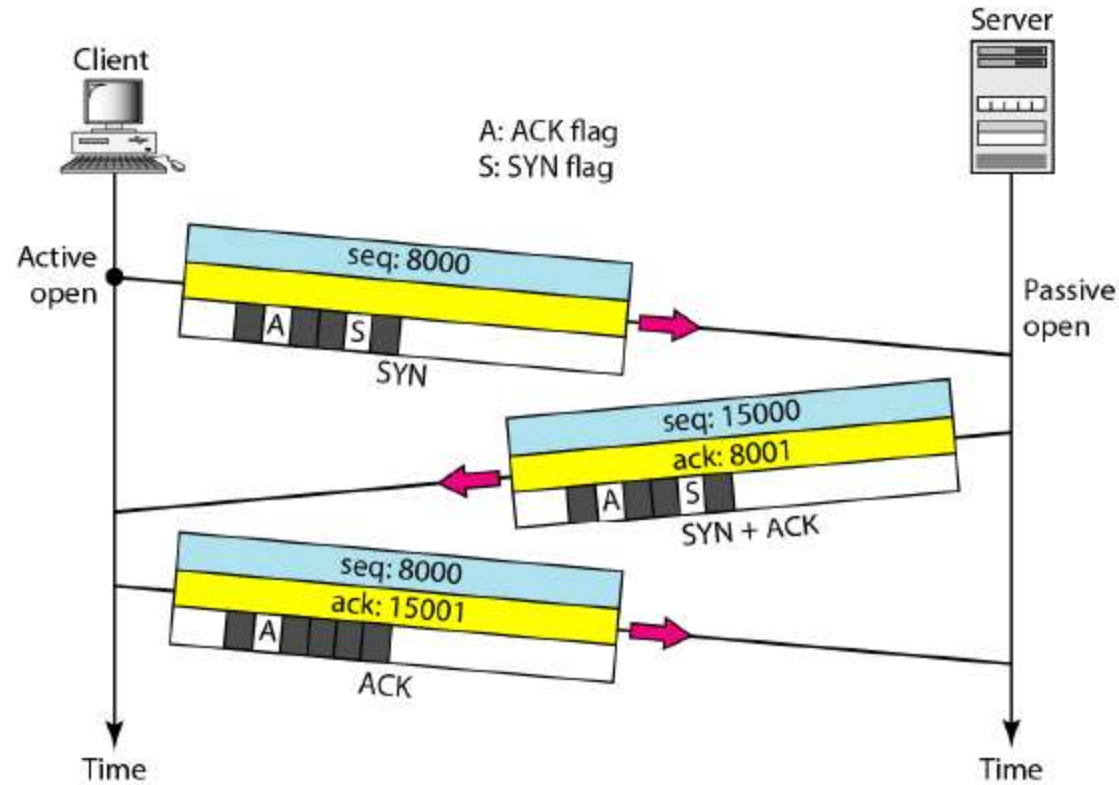
4.2. TCP Segment Format

- Urgent pointer.
 - This 16-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data.
- Options
 - There can be up to 40 bytes of optional information in the TCP header.

4.3. 3-Way Handshaking

- TCP is connection oriented which means before data transfer connection should be established
- Step in TCP communication
 1. Connection establishment
 2. Data Transfer
 3. Connection termination
- Connection is established with help of 3 way handshaking protocol
- Connection termination is also done with 3 way handshaking protocol

4.3.1. Connection Establishment (Handshaking)



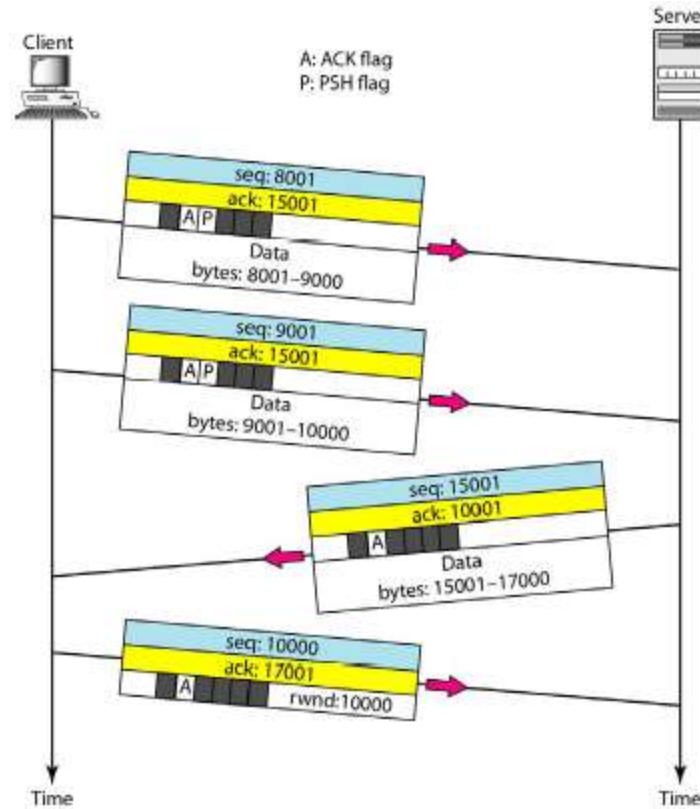
4.3.1. Connection Establishment (Handshaking)

- SYN-Synchronization message used for connection establishment
- ACK- Acknowledgement

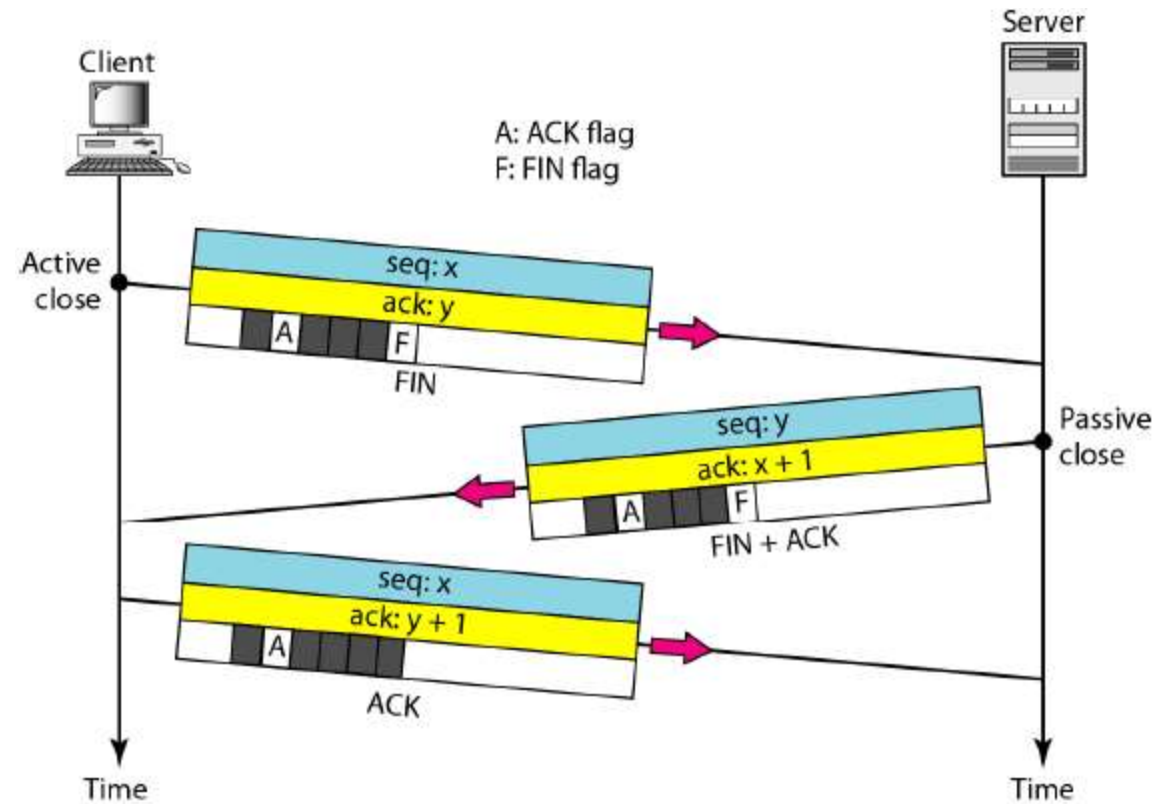
Steps

1. First client send SYN message to server
2. Server responds ACK to SYN and SYN to client
3. Client responds ACK to SYN and connection is established

4.3.2. Data Transfer(ACK Number + SEQ Number)



4.3.3. Connection Termination (Handshaking)



4.3.3. Connection Termination (Handshaking)

- FIN(Finish) – Connection Termination
- ACK- Acknowledgement

Steps

1. First client send FIN message to server
2. Server responds ACK to FIN from client and send FIN to client
3. Client responds ACK to FIN and connection is established

5. User Datagram Protocol(UDP)

- Connection less & Unreliable Service
- No flow and error control mechanisms at the transport level
- UDP uses port numbers for communication

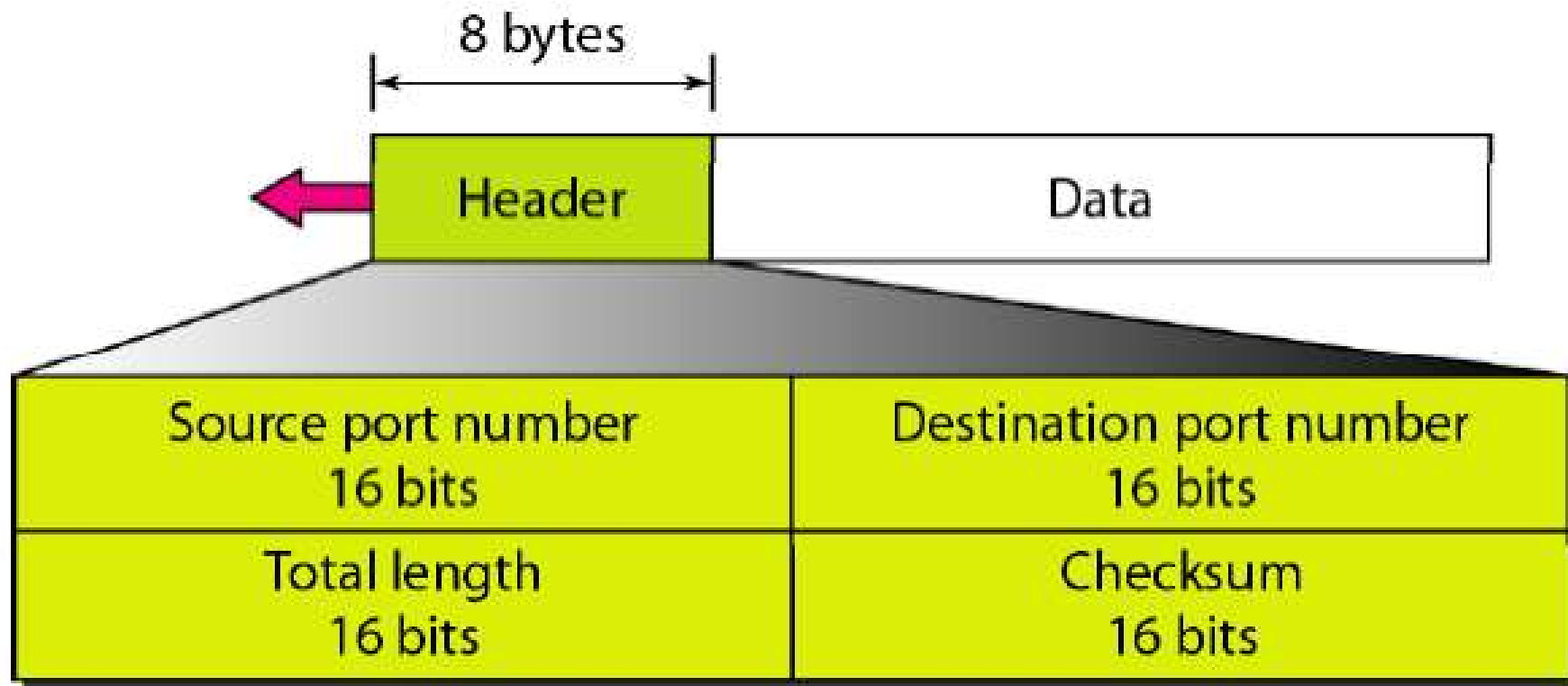
Well Known TCP Ports

- Daytime-13
- DNS-53
- TFTP-69
- RPC-111
- NTP-123

5.1. Features of UDP

- Connectionless:
 - No connection is established before data transfer
 - user datagram(segment) sent by UDP is an independent datagram
- Flow and Error Control:
 - No error flow control (Only optional error checking)
 - No retransmission
 - No acknowledgments

5.2. UDP Segment



5.2. UDP Segment

- Source port number(16 bits)
 - This is the port number used by the process running on the source host
 - Range 0-65535
- Destination port number(16 bits)
 - This is the port number used by the process running on the destination host
 - Range 0-65535
- Length
 - Defines the total length of the user datagram, header plus data.
 - Length ranges between 8 to 65,535 bytes
- Checksum
 - For error checking

Chapter 7

Congestion Control

&

Quality of Service

Prepared By R.G.B

Visit For Notes: <http://sites.google.com/site/rohitgbal>

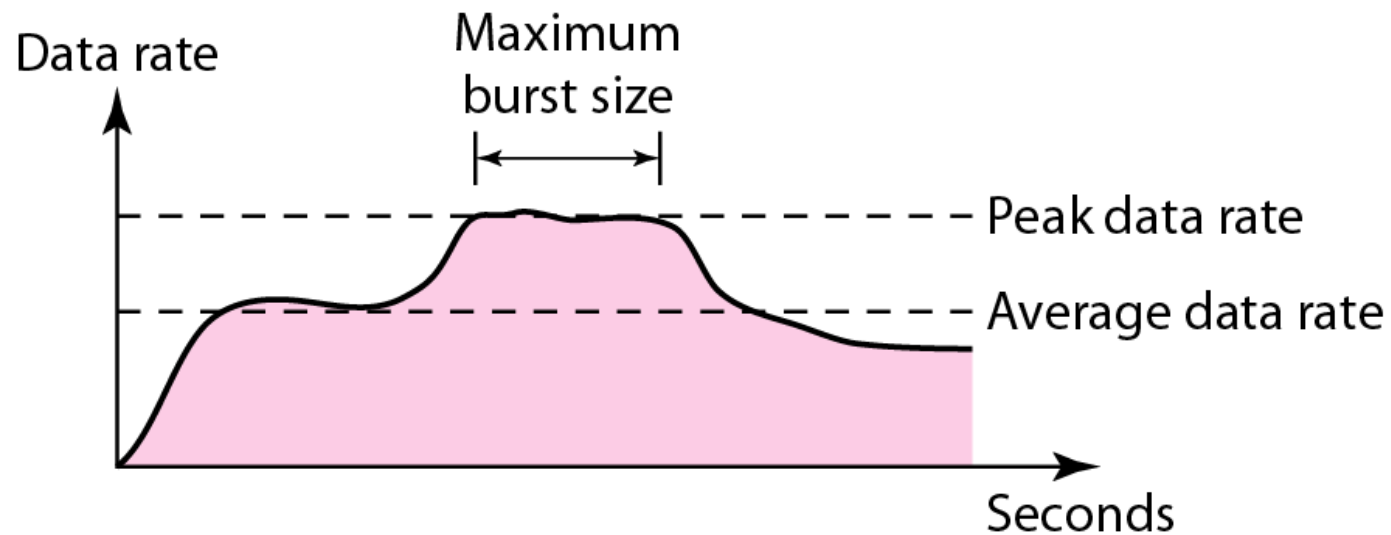
Email: rohitgbal@gmail.com

Contents

1. Congestion
2. Congestion Control
 1. Open Loop
 2. Closed Loop
3. Traffic Shaping
 1. Leakey Bucket
 2. Token Bucket
4. TCP Congestion Control

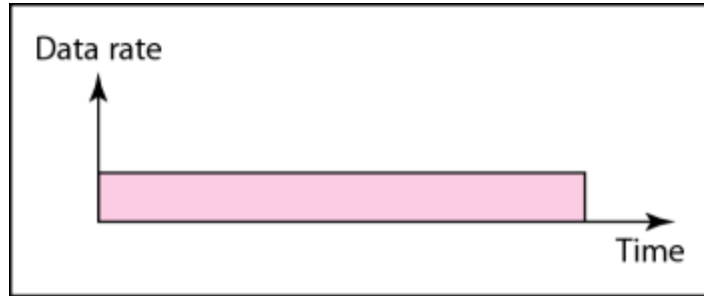
Introduction

- The main focus of congestion control and quality of service is data traffic
- Traffic descriptors are qualitative values that represent a data flow

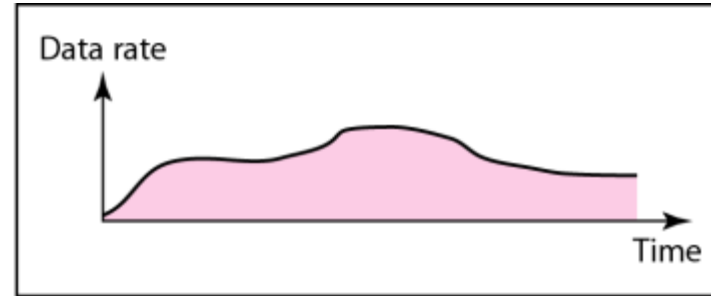


Introduction

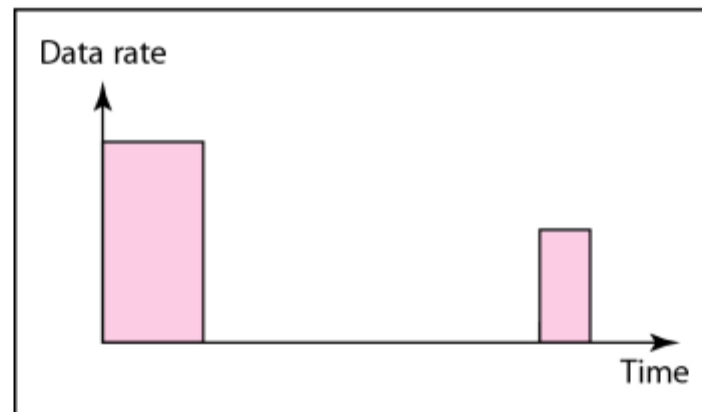
- 3 Traffic Profiles



a. Constant bit rate



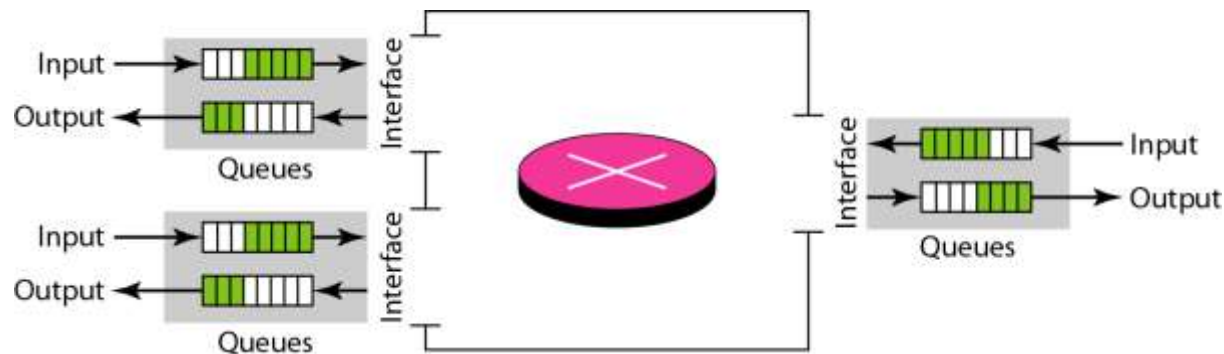
b. Variable bit rate



c. Bursty

1. Congestion

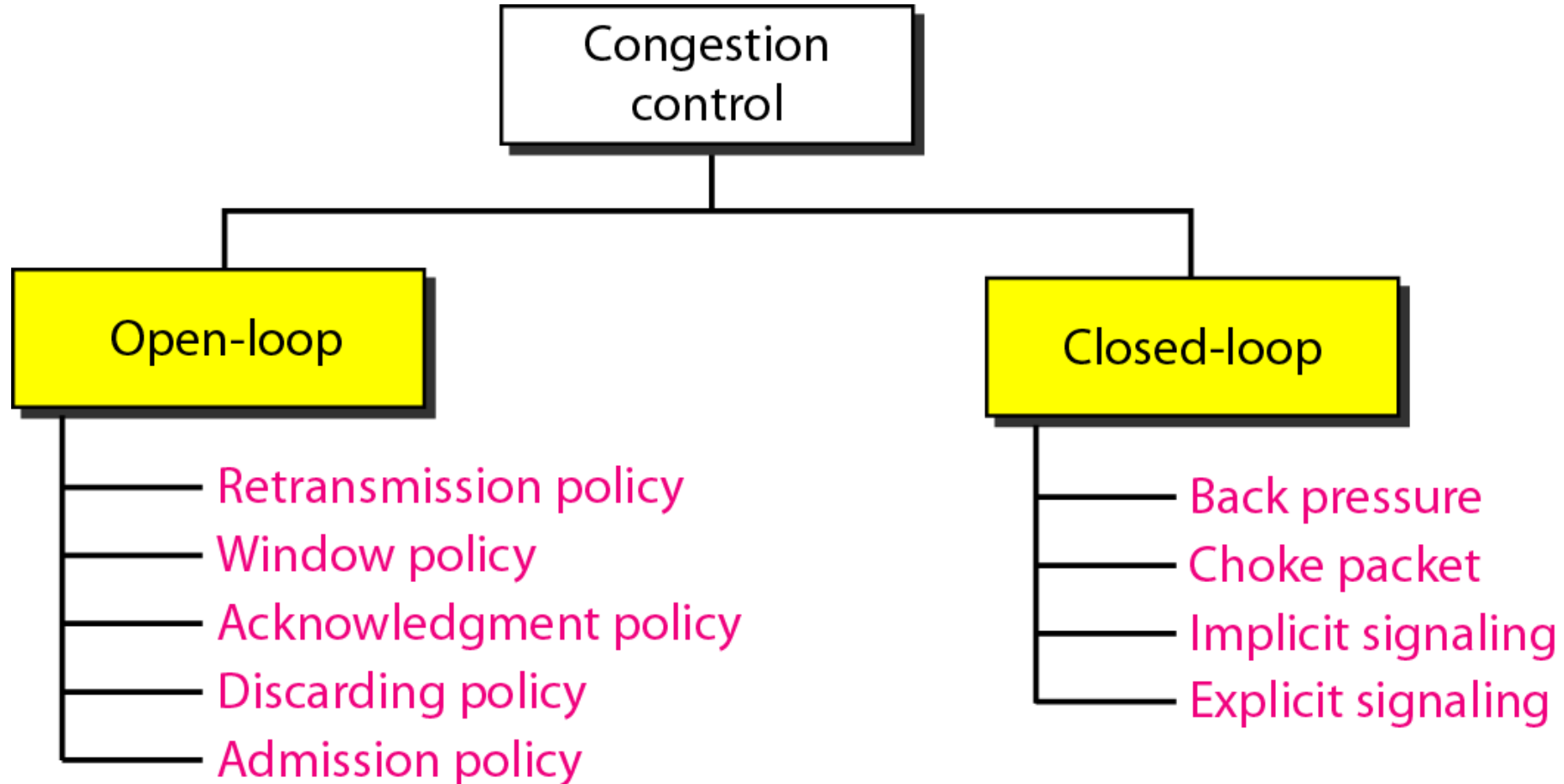
- Load of network → The number of packets sent to the network
- Capacity of network → The number of packets that can be handle
- Congestion occurs when the load of network is greater than capacity of network
- Congestion occurs because of the following factor
 1. Processing capacity of router
 2. No of Packets in input and output interface



2. Congestion Control

- Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened
- Congestion control mechanisms into two broad categories:
 1. Open-loop congestion control (prevention)
 2. Closed-loop congestion control (removal)

2. Congestion Control



2.1. Open Loop Congestion

- Congestion Prevention mechanism
- Policies are applied to prevent congestion **before it happens**
- Congestion control is handled by either the source or the destination
 1. Retransmission policy
 2. Windowing policy
 3. Acknowledge policy
 4. Discard policy
 5. Admission policy

2.1.1. Retransmission policy

- Retransmission is sometimes unavoidable
- If the sender feels that a sent packet is **lost or corrupted**, the packet needs to be **retransmitted**
- Retransmission in general may increase congestion in the network
- Good retransmission policy can prevent congestion
- The retransmission policy and the retransmission timers must be designed to **optimize efficiency** and at the same time **prevent congestion**

2.1.2.Windowing policy

- The Selective Repeat window is better than the Go-Back-N window for congestion control
- In the *Go-Back-N* window, when the timer for a packet times out, several packets may be resent, even if some may have arrived safe and sound at the receiver
- The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted

2.1.3. Acknowledge Policy

- Acknowledgments are also part of the load in a network
- The acknowledgment policy imposed by the receiver may also affect congestion
- If receiver acknowledges every packet there is change for congestion in network(Stop and wait)
- If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion. (Sliding window like **Go back-N** and **Selective repeat**)

2.1.4. Discard Policy

- A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission
- According to priority packet is discarded
- Less sensitive packets should be discarded

2.1.5. Admission Policy

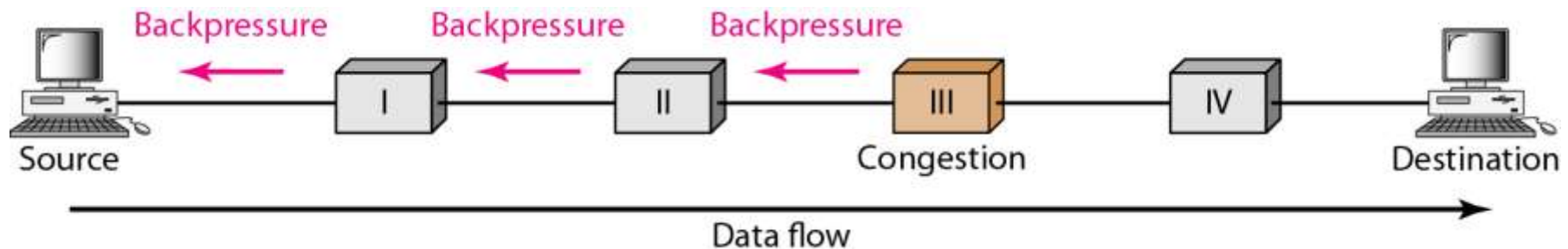
- Prevent congestion in virtual-circuit networks
- Before creating virtual circuit check the check the resource requirement
- A router can deny establishing a virtual circuit connection if there is congestion in the network or if there is a possibility of future congestion

2.2. Closed-Loop Congestion Control

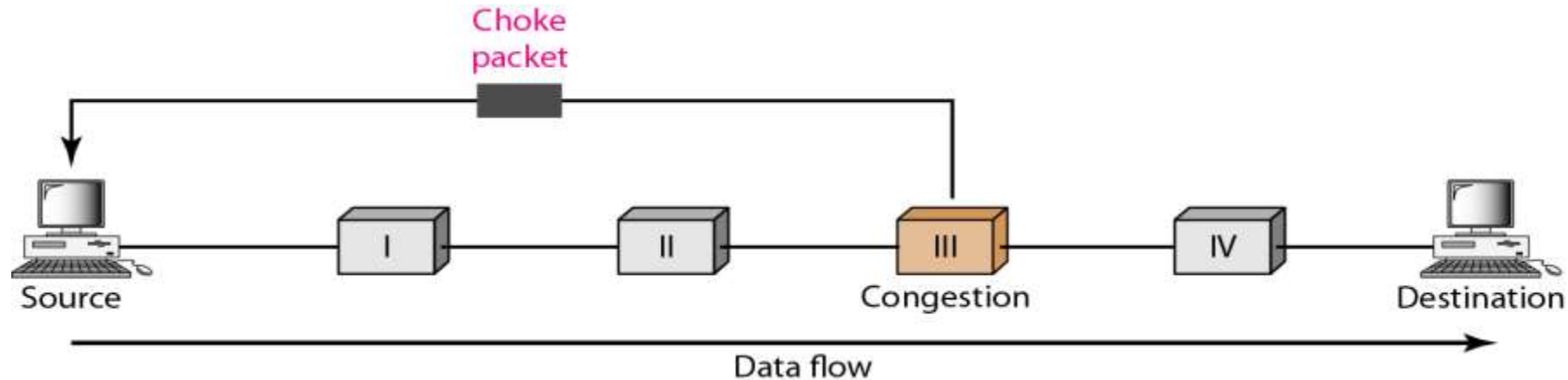
- Closed-loop congestion control mechanisms try to **alleviate congestion after it happens**
- Several mechanisms have been used by different protocols, They are
 1. Back pressure
 2. Choke packet
 3. Implicit signalling
 4. Explicit signalling
 1. Forward signalling
 2. Backward signalling

2.2.1. Back Pressure

- **Backpressure** refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes.
- Backpressure is a node-to-node congestion control
- Starts from congested node propagates, in the opposite direction of data flow, to the source
- Backpressure technique can be applied only to virtual circuit



2.2.2. Choke packet



- A choke packet is a packet sent by a node to the source to inform it of congestion
- Warning is from the congested encountered router to the source station directly
- Intermediate nodes doesn't know about congestion.

2.2.3. Implicit Signalling

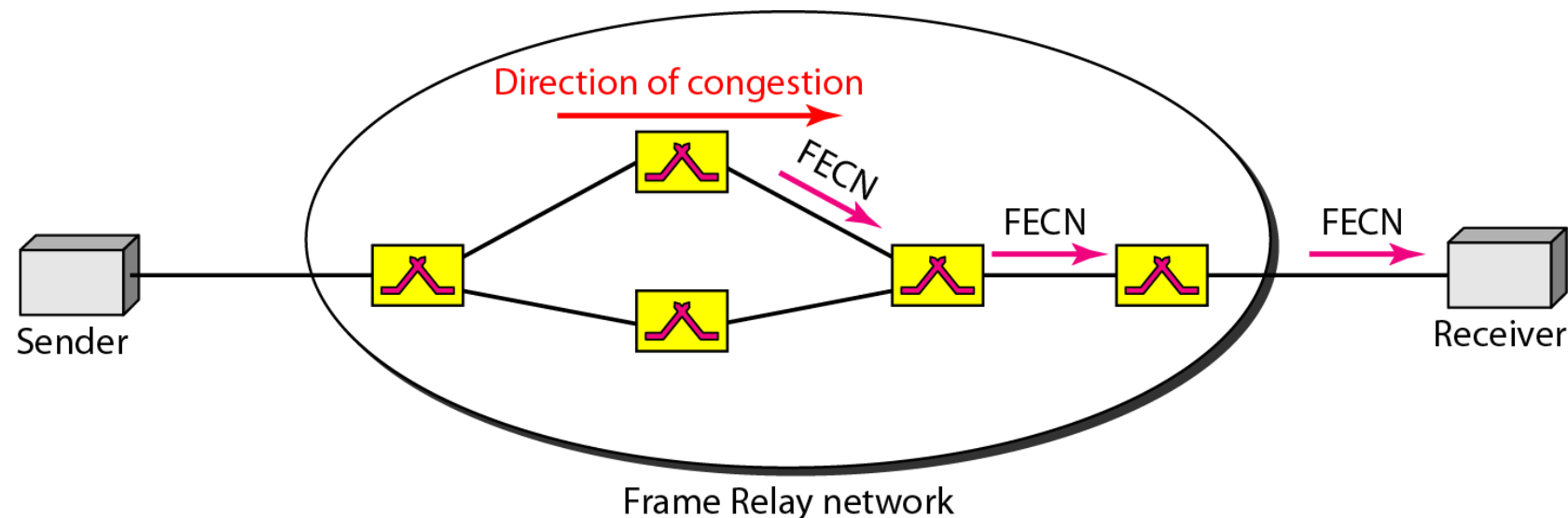
- No communication between the congested nodes and the source
- Source guesses that there is a congestion somewhere in the network from other symptoms
- Signals like acknowledgement is used
- If **ACK** is delayed the source assume there is congestion in destination and slows down the data transfer
- Used mainly in TCP network

2.2.4. Explicit Signalling

- The node that experiences congestion can explicitly send a signal to the source or destination
- Here only difference from choke packet is no separate packet is used where as in the choke packet separate packet is used
- It is used in Frame relay
- 2 types of signalling
 1. Forward signalling
 2. Backward signalling

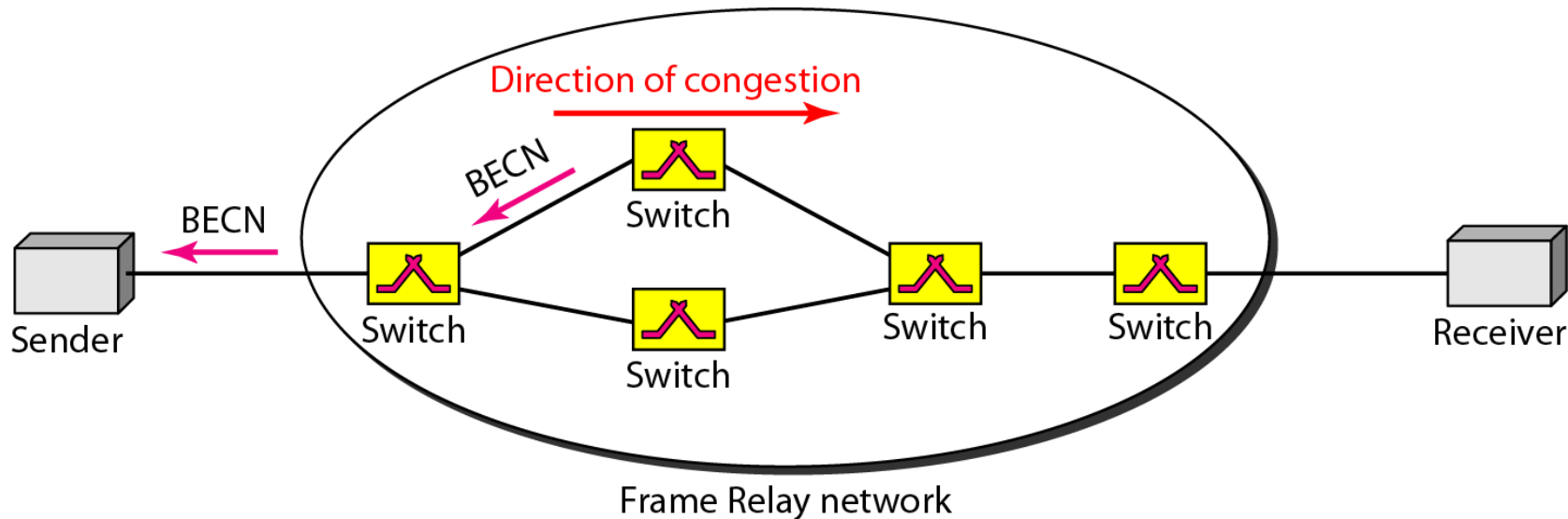
2.2.4.1. Forward Explicit Signalling

- A bit can be set in a packet moving in the direction of the congestion
- This bit can warn the destination that there is congestion
- The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the congestion.



2.2.4.2. Backward Explicit Signalling

- A bit can be set in a packet moving in the direction opposite to the congestion
- This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets



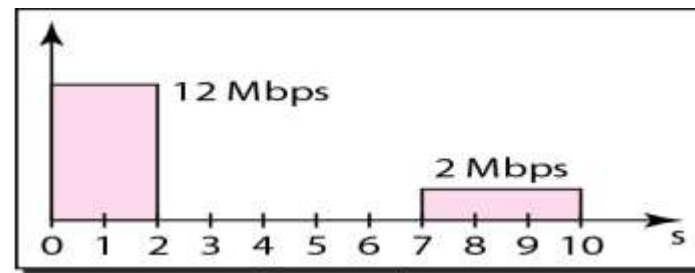
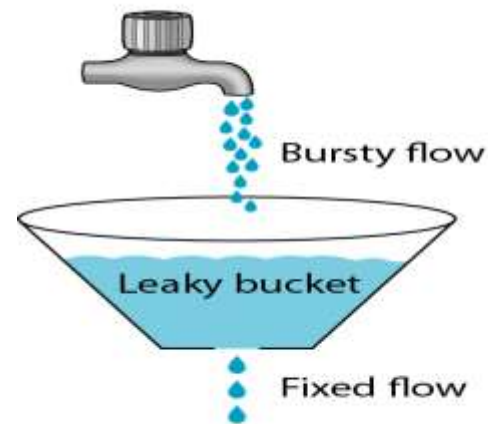
3. Traffic Shaping(QoS)

- Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network
- Two techniques can shape traffic
 1. Leaky bucket
 2. Token bucket

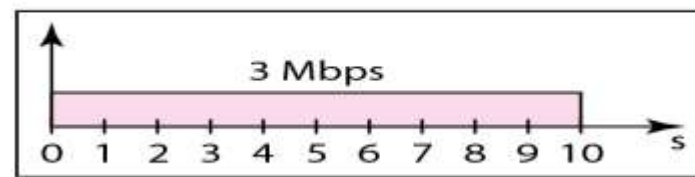
3.1. Leaky Bucket

If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket. The rate at which the water leaks does not depend on the rate at which the water is input to the bucket unless the bucket is empty

NB: In Network Bucket is router and water is data packets



Bursty data



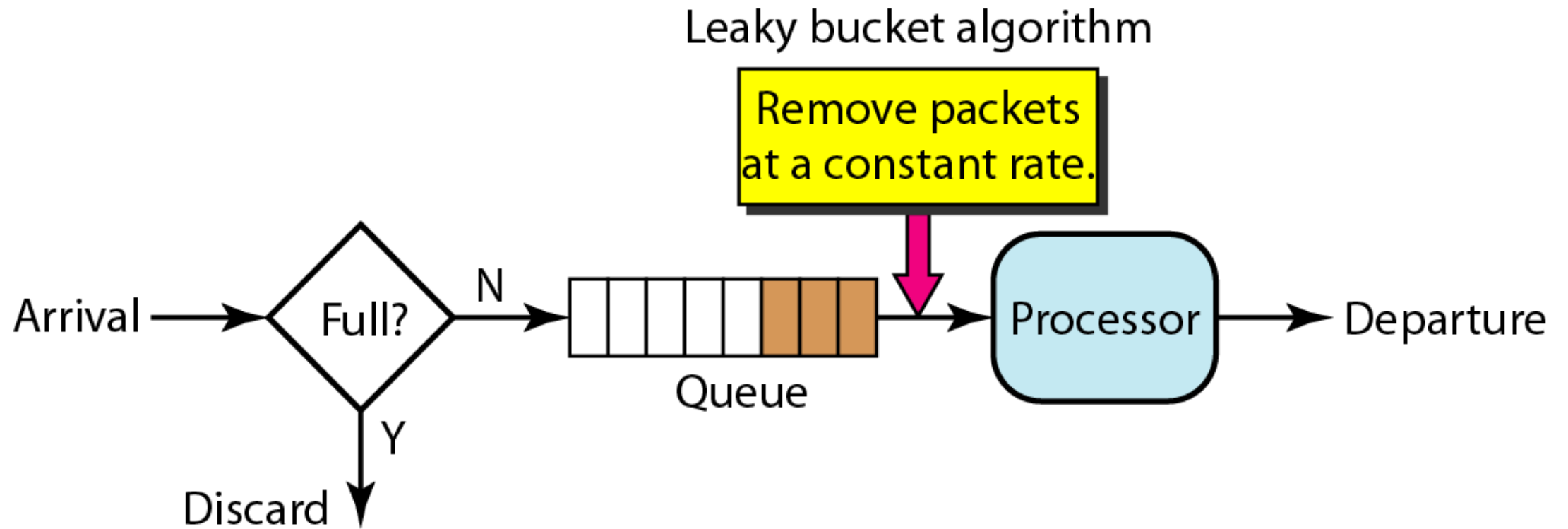
Fixed-rate data

3.1. Leaky Bucket

NB: In the figure, we assume that the network has committed a bandwidth of 3 Mbps for a host. The use of the leaky bucket shapes the input traffic to make it conform to this commitment. The host sends a burst of data at a rate of 12 Mbps for 2 s, for a total of 24 Mbits of data. The host is silent for 5 s and then sends data at a rate of 2Mbps for 3 s, for a total of 6 Mbits of data. In all, the host has sent 30 Mbits of data in 10 s

- The input rate can vary, but the output rate remains constant
- Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic, Bursty chunks are stored in router and sent out at an average rate
- It may also drop the packet if the bucket is full

3.1.1. Leaky bucket Implementation



3.1.1. Leaky bucket Implementation

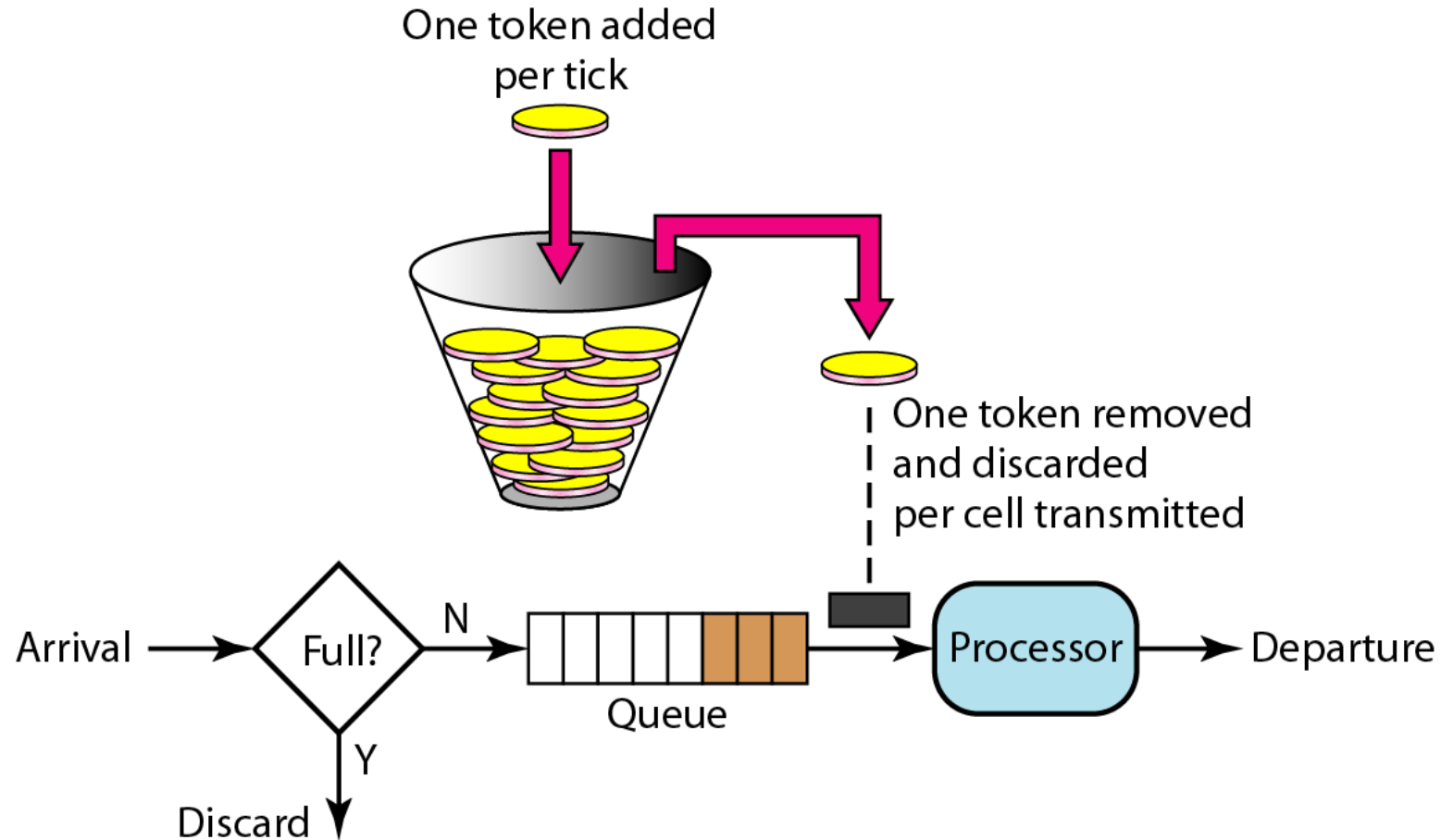
- Process removes a fixed number of packets from the queue at each tick of the clock
- If the traffic consists of variable-length packets, the fixed output rate must be based on the number of bytes or bits.
- The following is an algorithm for variable-length packets:
 1. Initialize a counter to n at the tick of the clock.
 2. If n is greater than the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.
 3. Reset the counter and go to step 1

3.1.2. Token Bucket

- The host can send bursty data as long as the bucket is not empty
- Token bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens
- For each tick of the clock, the system sends n tokens to the bucket
- The system removes one token for every cell (or byte) of data sent

For example, if n is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens. Now the host can consume all these tokens in one tick with 10,000 cells, or the host takes 1000 ticks with 10 cells per tick

3.1.2. Token Bucket



3.1.2. Token Bucket

- The token bucket can easily be implemented with a counter
 1. The token is initialized to zero
 2. Each time a token is added, the counter is incremented by 1
 3. Each time a unit of data is sent, the counter is decremented by 1
 4. When the counter is zero, the host cannot send data

4. Congestion Control in TCP

- TCP uses congestion control to avoid congestion or alleviate congestion in the network
 1. Congestion Window
 2. Congestion Policy
 1. Slow start
 2. Congestion Avoidance
 3. Congestion Detection

4.1. Congestion Window

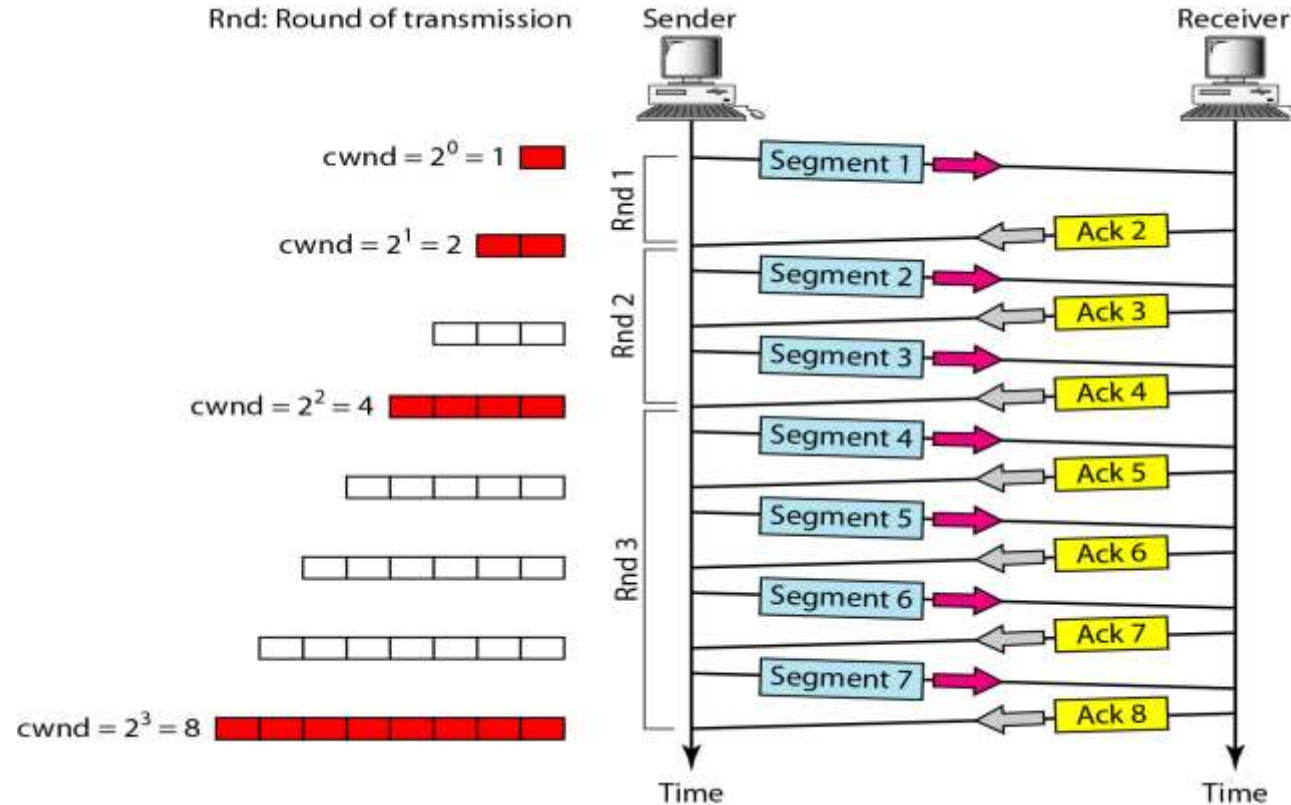
- Sender can send only that amount of data before waiting for an acknowledgment, the amount data is termed a **window size**
- The sender has two pieces of information:
 1. Receiver window size : Maximum available buffer size of receiver
 2. Congestion window size : Congestion window size is determined by congestion policy
- Window size \geq minimum of receiver window size , congestion window size

4.2. Congestion policy

- Handling of congestion is done by 3 phases
 1. Slow start
 2. Congestion avoidance
 3. Congestion detection

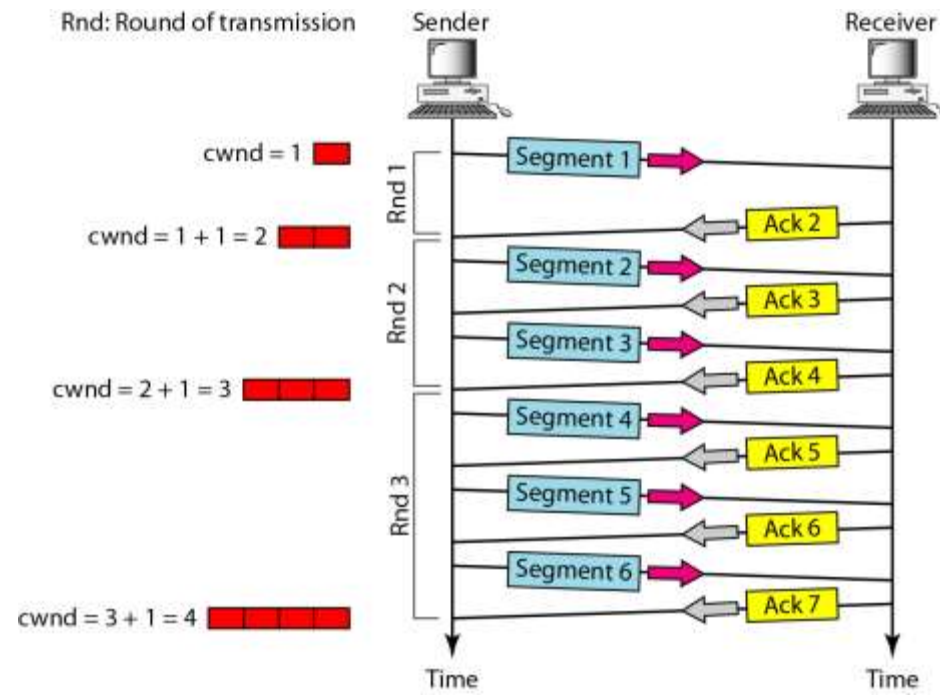
4.2.1. Slow Start

- Size of the congestion window increases exponentially until it reaches a threshold



4.2.2. Congestion Avoidance

- Congestion Avoidance uses Additive inverse
- Congestion window increases additively until congestion is detected
- Slow-start phase stops and the additive phase begins



4.2.3. Congestion Detection

- If congestion occurs, the congestion window size must be decreased
- The only way the sender can guess that congestion has occurred is by the need to retransmit a segment
- However, retransmission can occur in one of two cases:
 1. when a timer times out
 2. when three ACKs are received
- In both cases, the size of the threshold is dropped to one-half, a multiplicative decrease

Chapter 8

Application Layer, Servers & Protocols

Prepared By R.G.B

Visit For Notes: <http://sites.google.com/site/rohitgbal>

Email: rohitgbal@gmail.com

Contents

1. Domain Name System

1. Name Space
2. Server
3. Queries

2. HTTP

3. FTP

4. Proxy

5. DHCP

6. E-mail

1. SMTP
2. POP
3. IMAP

URL (Universal Resource Locator)

- URL is the abbreviation of **Uniform Resource Locator**
- **URL consist of following syntax**

protocol://host:port/path

1. Protocol : The *protocol* is the client/server program used to retrieve the document (eg: FTP, HTTP, HTTPS)
2. Host : Computer in which information is located
3. Path : the local path in which information is stores in the host
4. Port : The port number of the service used in the host

Example: <http://www.google.com:80/index.html>

URL is also called web address

1. Name Server (DNS- Domain Name System)

- All system communicate using IP(Numbers)
- Numbers are difficult to remember for human beings than name
 - Internet is very large there are millions of computer and servers
- Naming system is introduced(in 1983) for mapping of Host Name to IP address
- In DNS server, there is library procedure (program) called resolver that converts host name to IP
- **ICANN (Internet Corporation for Assigned Names and Numbers)** is responsible for managing the DNS in internet.
- Domain names are unique

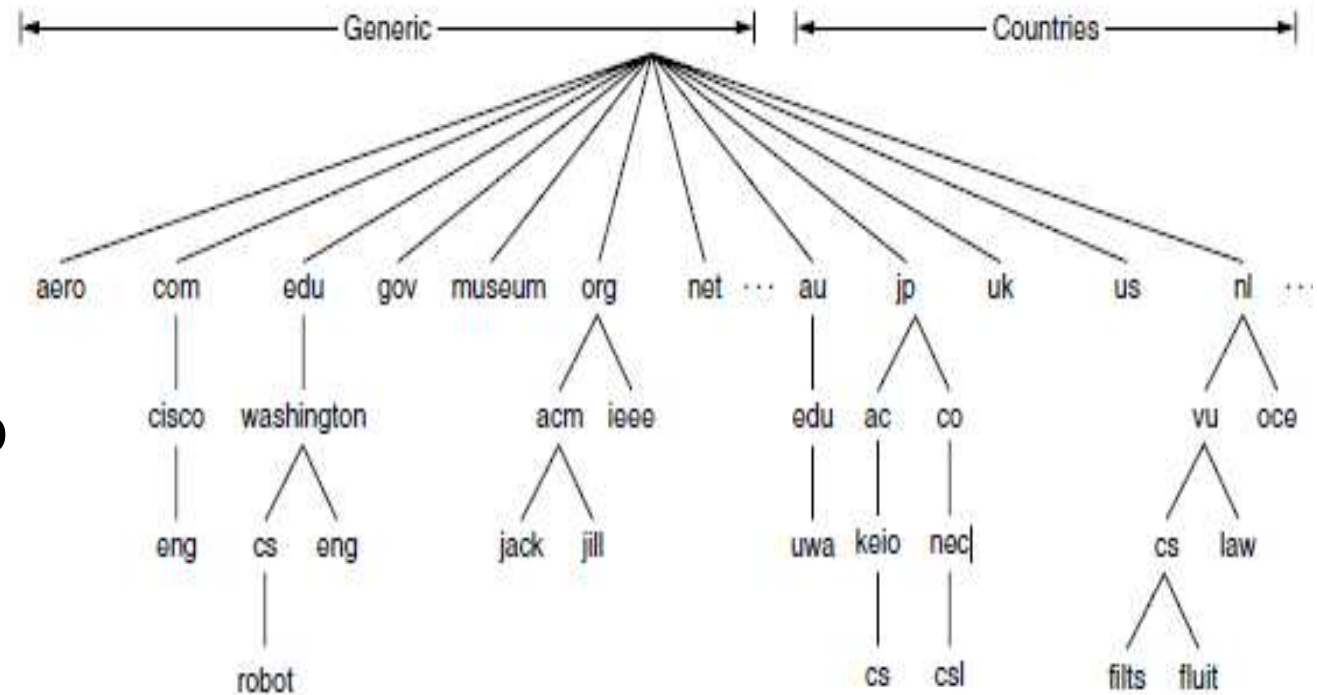
1.1. Name Spaces(Domain Name)

- Divided into 2 :
 1. Flat Structure
 2. Hierarchical Structure
- Hierarchical structure is used
 - Name space have tree structure
 - Example : www.xyz.com
 - *Here xyz.com is managed by central authority(ICANN) and www is name given by organization(here xyz)*

1.1.1. Domain Name Space

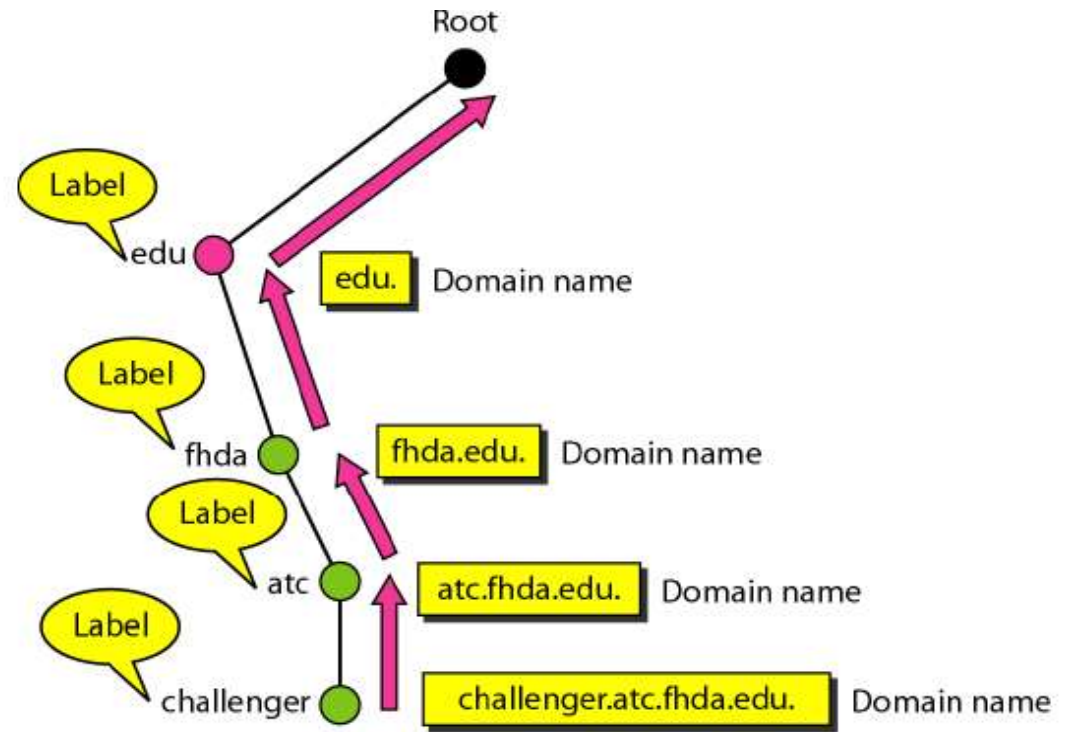
- Inverted Tree Structure, contains 0 to 127 (128) levels
- 0 is root level
- Internet have nearly 250 **top-level domains**, where each domain covers many hosts
- Each domain is partitioned into **subdomains**, and these are further partitioned, and so on

com, edu, gov are example of top level domain



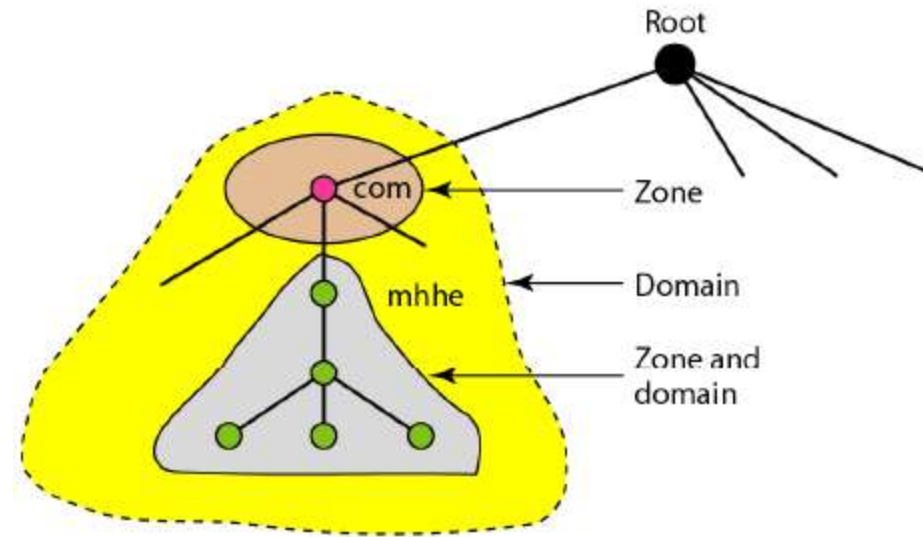
1.1.2. Domain Name

- All label is terminated by a null string(.), it is called a **FQDN (Fully Qualified Domain Name)**
- **Example:** *challenger.atc.tbda.edu.*
- Label is not terminated by a null string, it is called a **PQDN (Partially Qualified Domain Name)**
- A PQDN starts from a node, but it does not reach the root
- **Example :** *challenger.atc.tbda.edu*
- NB: **.(dot)** Is called root server



1.1.3. Zone

- Zone will keep track of all nodes in domain and all sub-domains under the domain.



1.2. Servers

- Root Server
 - A root server is a server whose zone consists of the whole tree
 - A root server usually does not store any information about domains but delegates its authority to other servers
- DNS defines two types of servers
 1. Primary Server
 - A primary server is a server
 - That stores a file about the zone for which it is an authority
 - It is responsible for **creating, maintaining, and updating the zone file**
 2. Secondary Server
 - A secondary server is a server that **transfers the complete information about a zone** from another server (primary or secondary) and stores the file on its local disk

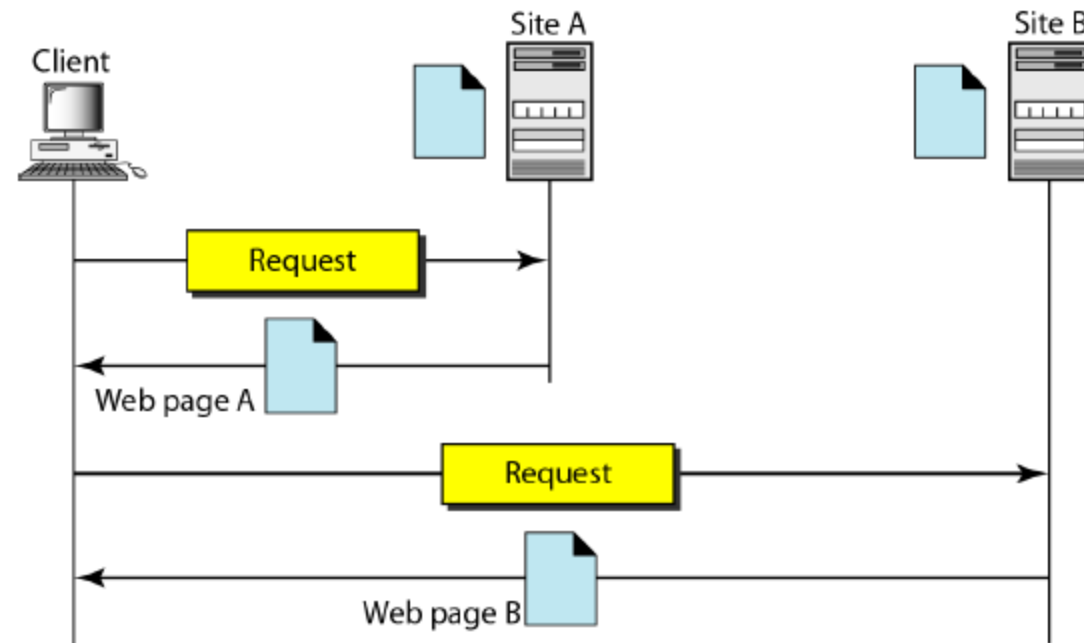
1.3. Query

- DNS has two types of messages
 1. **Query** - sent by DNS client to server, **Query message consists** of a header and question records
 2. **Response** – sent by DNS server to client, **Response message consists** of a header, question, records, answer records, authoritative records, and additional records
 - Query is a question to the server, Client ask about the **IP address** of the mentioned **URL**
 - **Response** is answer to the question provided by client from server, i.e. it sent information (IP address) of the mentioned URL

2. HTTP-(Hyper Text Transfer Protocol)

- The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web(WWW)
- It is similar to FTP because it transfers files and uses the services of TCP.
- It uses only one TCP connection
- HTTP uses the services of TCP on well-known **port 80**
- Accessing of web page is based on URL

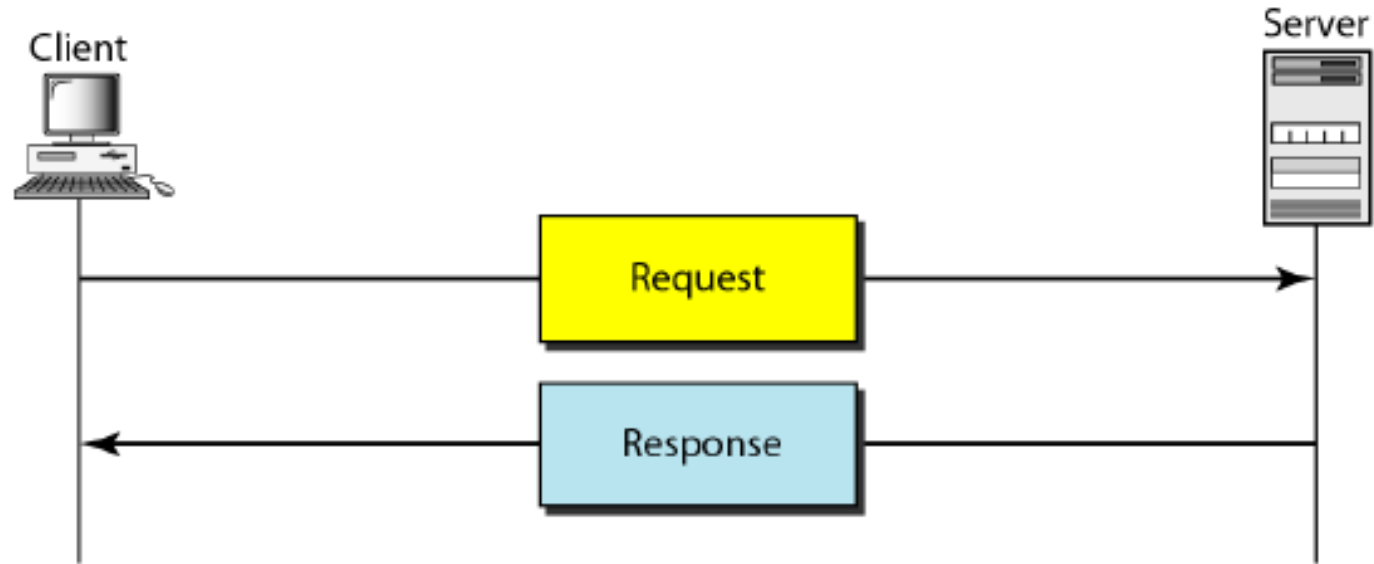
2.1. WWW Architecture



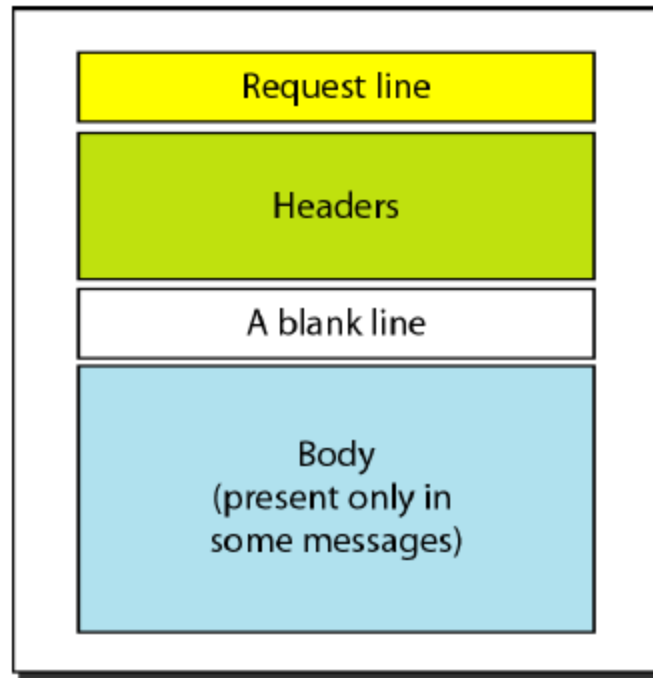
2.2. HTTP Transaction

- HTTP transaction between the client and server
- There are 2 transaction messages
- Request (sent from client to server for requesting a Page or other resource)
- Response (sent from server to client)

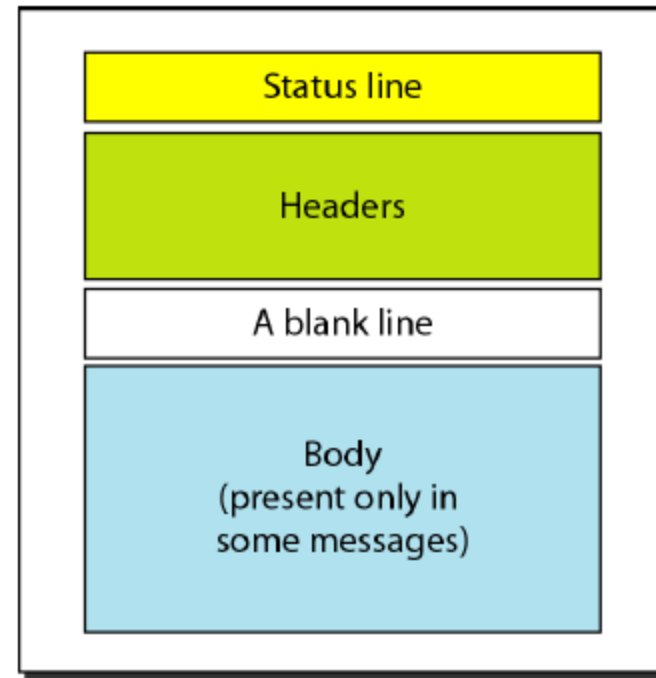
2.2. HTTP Transaction Figure



2.2.1 Message Format



Request message

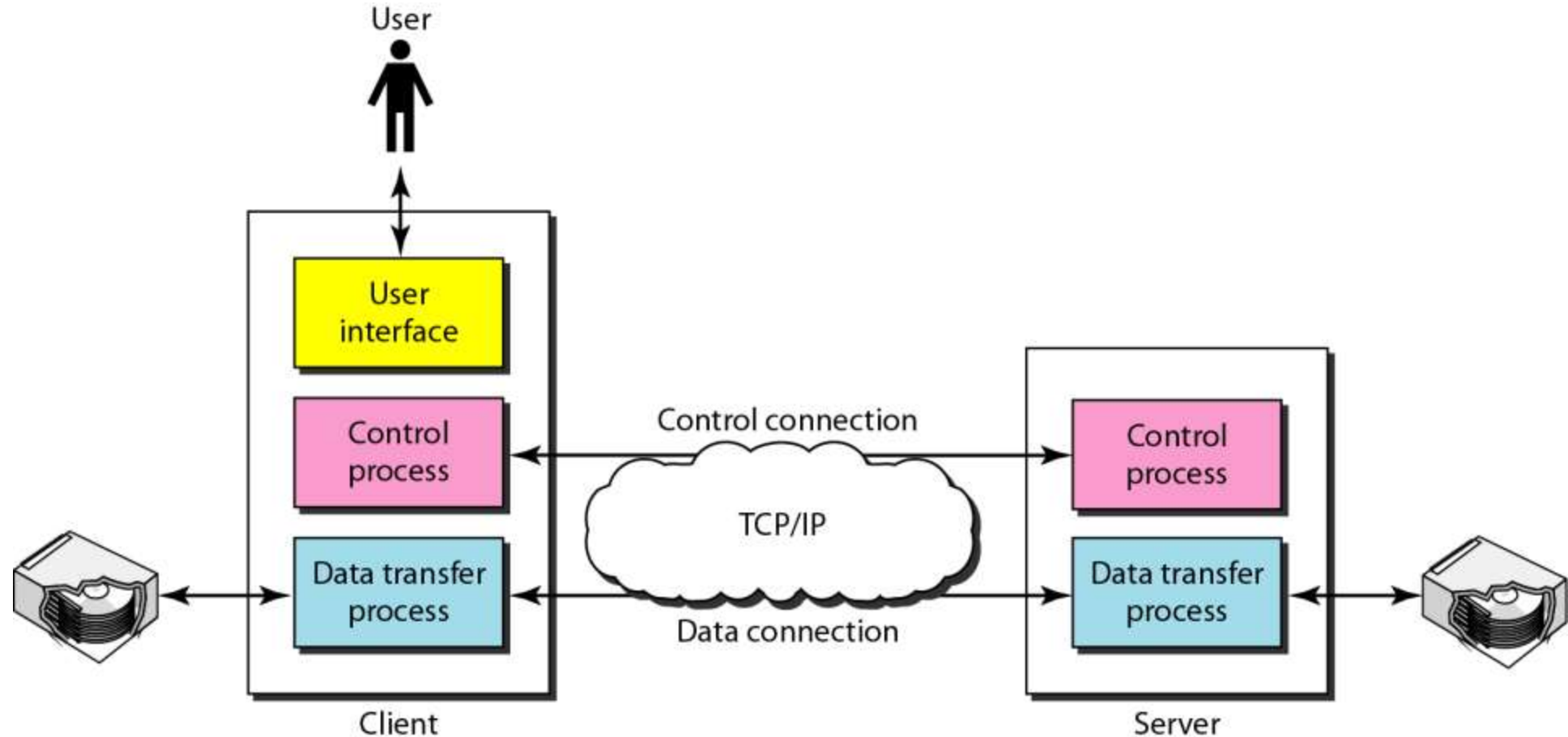


Response message

3. FTP (File Transfer Protocol)

- File Transfer Protocol (FTP) is the standard mechanism provided by *TCP/IP* for copying a file from one host to another
- FTP establishes two connections between the hosts
- One connection is used for data transfer, the other for control information (commands and responses)
- Separation of commands and data transfer makes FTP more efficient
- FTP uses **two** well-known TCP ports: **Port 21** is used for the control connection, and **port 20** is used for the data connection.

3.1. FTP Architecture



3.2. FTP Working

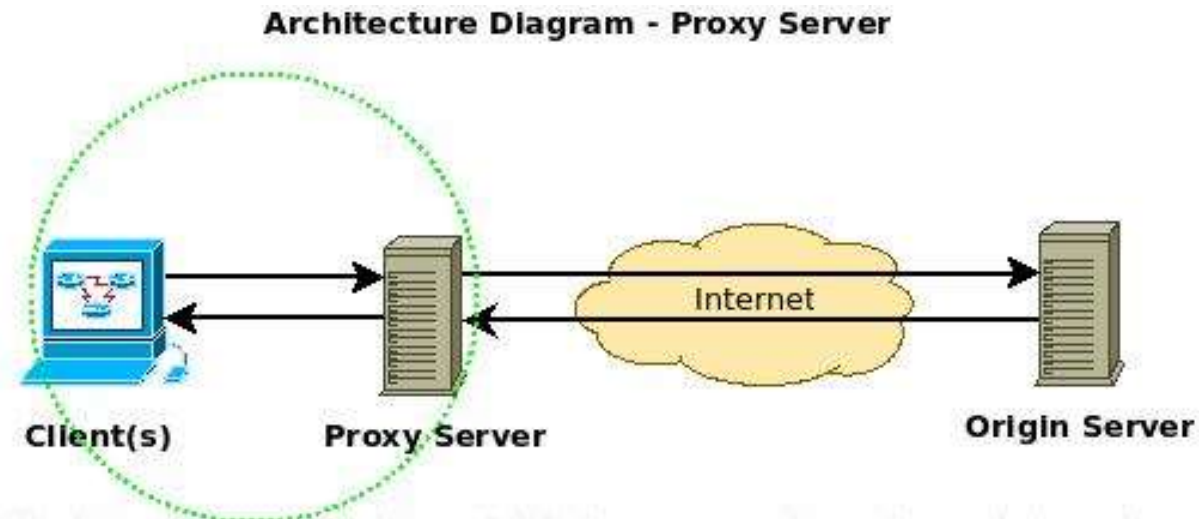
- FTP uses Transmission Control Protocol (TCP) for reliable network communication by establishing a session before initiating data transfer
- FTP client send command/ request for connection to FTP server establishing connection(Port 21)
- FTP server Responds to the commands about the status wheatear connected/ not connected (Port 21)
- FTP Client connect to FTP server using control connection i.e. using port 21
- After establishing connection port 20 is used for data transfer

4. Proxy Server

- A proxy server is a computer that keeps copies of responses to **recent requests**
- The HTTP client sends a request to the proxy server
- The proxy server checks its cache, If the response is not stored in the cache, the proxy server sends the request to the corresponding server
- Incoming responses are sent to the proxy server and stored for future requests from other clients
- The proxy server **reduces the load on the original server**, decreases traffic, and improves latency

4. Proxy Server

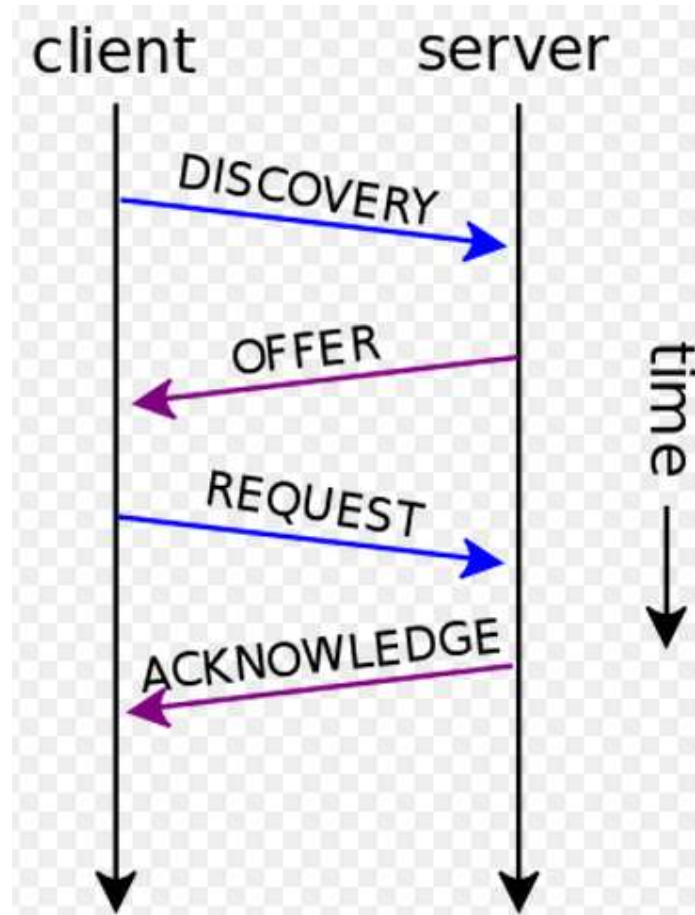
- However, to use the proxy server, the client must be configured to access the proxy instead of the target server



5. DHCP(Dynamic Host Configuration Protocol)

- Two possible way for configuring IP are:
 1. Manually
 2. Dynamically (DHCP)
- DHCP is service that provide IP addresses.
- Server that runs DHCP service is DHCP servers.
- Client that uses DHCP server for IP configuration is DHCP clients.
- DHCP server uses UDP port 67
- DHCP client uses UDP port 68

5.1. DHCP Operation



5.1.1. DHCP Discover Packet

- Sent by DHCP client to DHCP server(Broadcasting)
- DHCP client (*computer or device which wants IP*) broadcast broadcasts a request for an IP address on its network. It does this by using a DHCP DISCOVER packet
- Packet must reach the DHCP server
- A DHCP client may also request its last-known IP address with discover packet
- DHCP discover packet is for checking weather DHCP server is available in network and IP address lease request

5.1.2. DHCP Offer Packet

- Sent by DHCP server to DHCP client (Unicasting)
- When a DHCP server receives a DHCPDISCOVER message from a client, which is an IP address lease request, the server reserves an IP address for the client and makes a lease offer by sending a DHCPOFFER message to the client
- This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer

5.1.3. DHCP Request Packet

- Sent by DHCP client to DHCP servers (Broadcasting)
- In response to the DHCP offer, the client replies with a DHCP request, broadcast to the server, requesting the offered address.
- A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer
- Based on required server identification option in the request and broadcast messaging, servers are informed whose offer the client has accepted.
- When other DHCP servers receive this message, they withdraw any offers that they might have made to the client and return the offered address to the pool of available addresses.

5.1.4. DHCP Acknowledgement Packet

- Sent by DHCP servers to DHCP client (Unicasting)
- When the DHCP server receives the DHCP REQUEST message from the client, the configuration process enters its final phase.
- The acknowledgement phase involves sending a DHCP ACK packet to the client.
- This packet includes the lease duration and any other configuration information that the client might have requested.
- At this point, the IP configuration process is completed

6. E-mail

- Electronic mail, or more commonly **email**, used to communicate with different users in internet
- Email uses following protocols for storing & delivering messages, They are :
 1. SMTP (Simple Mail Transfer Protocol)
 2. POP (Post Office Protocol)
 3. IMAP (Internet Message Access Protocol)

6. E-mail

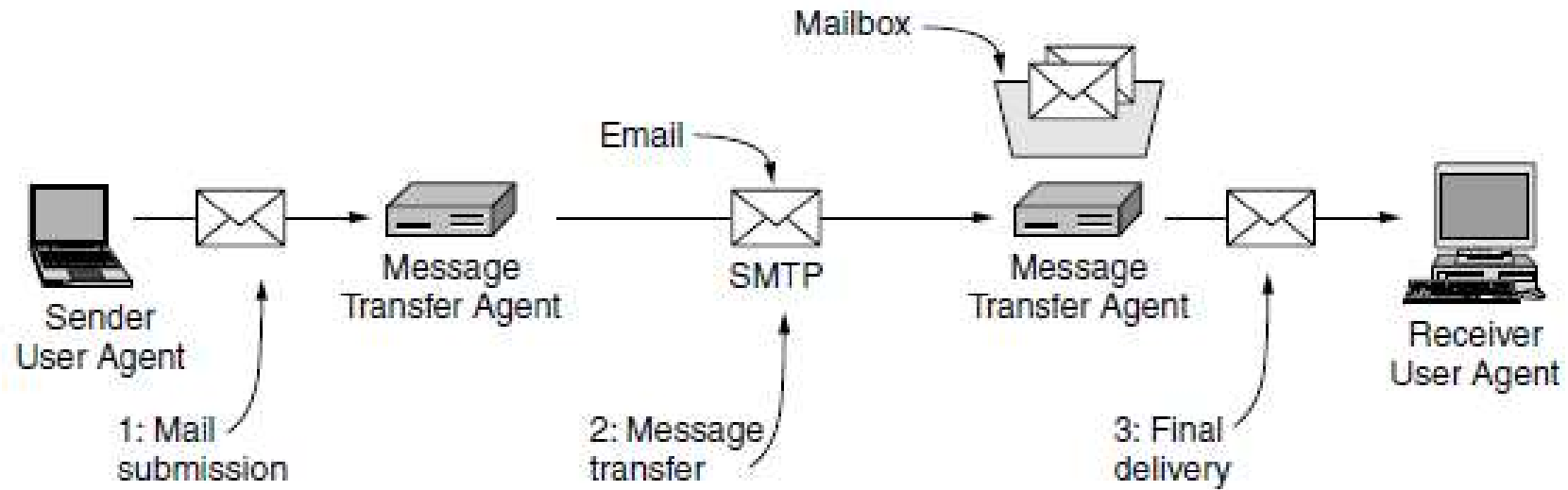
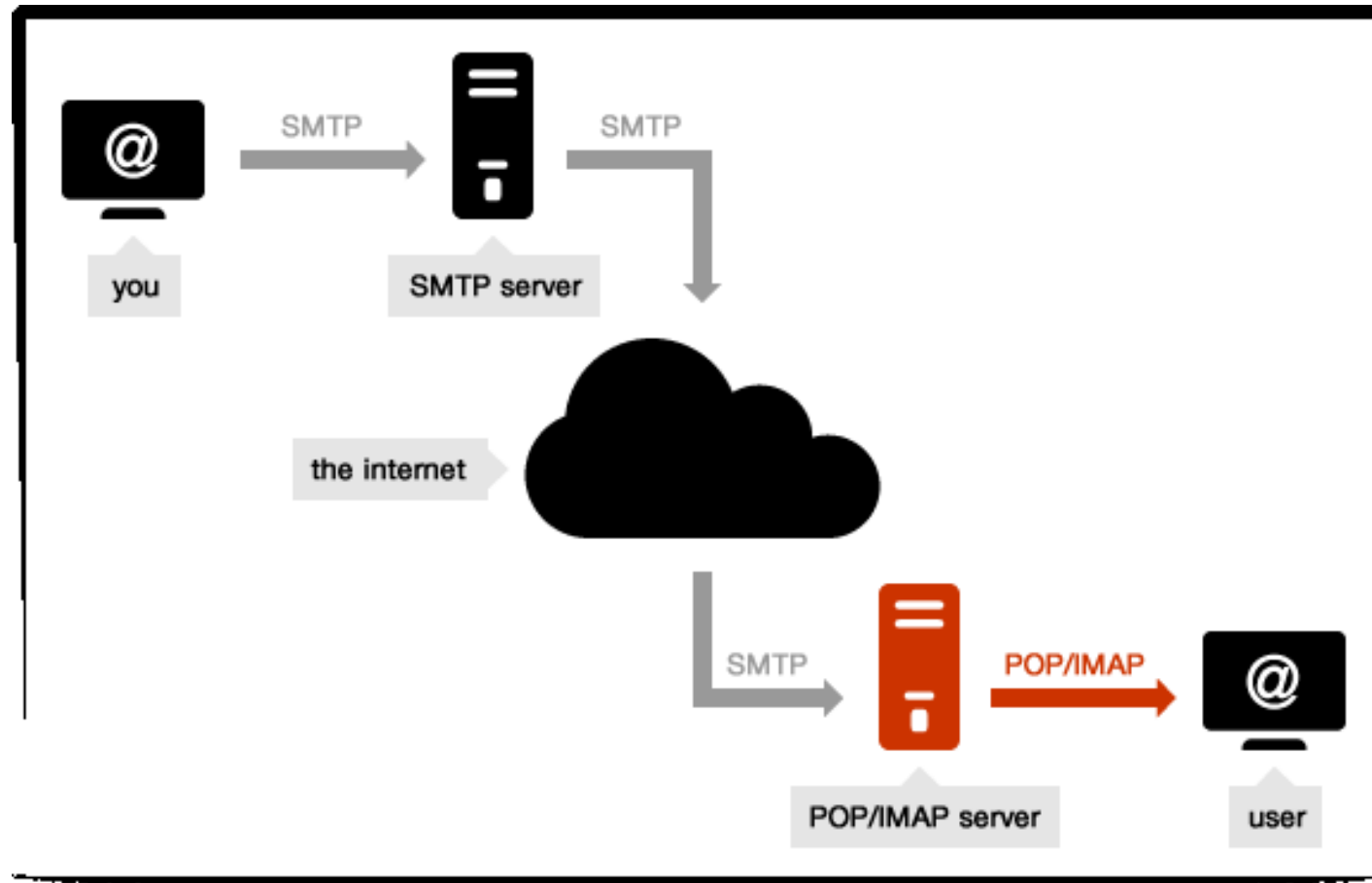


Figure Architecture of the email system.

6. E-mail

- Email consists of two kinds of subsystems
 1. **Mail User Agents (also called MUA/email client programs)**: which allow people to read and send email (Ex: Outlook)
 2. **Message Transfer Agents(also called MTA/ Email Server)** : which move the messages from the source to the destination (Ex: Gmail Server)
- Act of sending new messages into the mail system for delivery is called **Mail submission (Email Client to Email Sever)**
- The Process of transferring mail from one MTA to another (Ex : from gmail to yahoo server) is called **Message Transfer**
- **Mailboxes** store the email that is received for a user

6. E-mail (Working all Protocols)



6.1. SMTP (Simple Mail Transfer Protocol)

- Message transfer from originator to the recipient mailbox is done with SMTP
- It uses TCP well known port 25
- SMTP server accepts incoming connections, subject to some security checks, and accepts messages for delivery
- If a message cannot be delivered, an error report containing the first part of the undeliverable message is returned to the sender
- Email is submitted by a mail client (**MUA, mail user agent**) to a mail server (**MSA, mail submission agent**) using SMTP on TCP port 587
- **MSA** delivers the mail to its mail transfer agent **MTA**

6.1.1. Features of SMTP

- SMTP supports sending of email only It cannot retrieve (deliver to user) messages from a remote server on demand
- SMTP provides system for sending message to same (or different) servers (gmail **to** gmail / gmail **to** yahoo)
- SMTP provide a mail exchange between users on same (or different) server
- SMTP supports:
 1. Sending a message to one or more recipients
 2. Sending message that includes text, voice, video or graphics
 3. Sending message to users on other network

6.2. POP (Post Office Protocol)

- Post Office Protocol (POP) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection
- POP has been developed through several versions, with version 3 (POP3) being the last standard
- E-mails are downloaded from the server's mailbox to your computer
- No copy of Email will be kept in mailbox after downloading the email
- E-mails are available when you are not connected

6.2.1. POP Working

- Working of POP servers is as following steps:
 1. Connect to server
 2. Retrieve all mail
 3. Store locally as new mail
 4. Delete mail from server*
 5. Disconnect

** Deletion of mail is default setting , However user can change the settings to keep the copy of email in mail box*

6.2.2.Features of POP

- POP is a much simpler protocol, making implementation easier
- POP mail moves the message from the email server onto your local computer, although there is usually an option to leave the messages on the email server as well
- POP treats the mailbox as one store, and has no concept of folders
- POP protocol requires the currently connected client to be the only client connected to the mailbox
- When POP retrieves a message, it receives all parts of it

6.2.3. Advantages of POP

- Advantages are:
 1. Mail stored locally, i.e. always accessible, even without internet connection
 2. Internet connection needed only for sending and receiving mail
 3. Saves server storage space
 4. Option to leave copy of mail on server

6.3. IMAP (Internet Message Access Protocol)

- Protocols that is used for final delivery is **IMAP**
- **IMAP** is an Internet standard protocol used by e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection
- IMAP provides mechanisms for storing messages received by SMTP in a mailbox
- IMAP server stores messages received by each user until the user connects to download and read them using an email clients

** Now a days IMAP replaced POP in all E-mail services*

6.3.1. IMAP Working

- Working of IMAP servers is as following steps:
 1. Connect to server
 2. Fetch user requested content and cache it locally, e.g. list of new mail, message summaries, or content of explicitly selected emails
 3. Process user edits, *e.g. marking email as read, deleting email etc.*
 4. Disconnect

6.3.2 Features of IMAP

- Connected and disconnected modes of operation (Faster Operation)
- Multiple clients simultaneously connected to the same mailbox
- Access to message parts and partial fetch of messages (No need for complete message to be displayed only **subject / user name** can be retrieved)
- Provides message state information (**Message states are** : read / unread / replied / forwarded)
- Provides multiple mailboxes on the server (create new mail boxes and copy form one to another)
- Provides mechanisms for server-side searches

6.3.3. IMAP Advantage

Advantages

1. Mail stored on remote server, i.e. accessible from multiple different locations
2. Internet connection needed to access mail
3. Faster overview as only headers are downloaded until content is explicitly requested
4. Mail is automatically backed up if server is managed properly
5. Saves local storage space
6. Option to store mail locally

Chapter 9

Network Management

&

Security

Prepared By R.G.B

Visit For Notes: <http://sites.google.com/site/rohitgbal>

Email: rohitgbal@gmail.com

Contents

1. Network Management
2. SNMP
3. Security
4. Cryptography
 1. Symmetric (DES)
 2. Asymmetric (RSA)
5. Key Exchange
 1. Diffie-Hallman
 2. Kerberos
6. Firewall
 1. Packet Filter Firewall
 2. Proxy Firewall
7. IPSec
 1. Transport Mode
 2. Tunnel Mode
8. VPN

1. Network Management

- **Network Management** is defined as **monitoring, testing, configuring,** and **troubleshooting** network components to meet a set of requirements defined by an organization/user
- Network Management system can be divided into five broad categories:
 1. Configuration Management
 2. Fault Management
 3. Performance Management
 4. Security Management
 5. Accounting Management

1.1 Configuration Management

- Configuration management system must know, at any time, the status of each entity (*hardware/software/user*) and its relation to other entities
- Configuration management can be subdivided into two parts
 1. **Reconfiguration**, which means adjusting the network components and features, can be a daily occurrence in a large network. There are three types of reconfiguration: **hardware reconfiguration, software reconfiguration, and user-account reconfiguration**
 2. **Documentation**, The original network configuration and each subsequent change must be **recorded** properly. This means that there must be documentation for **hardware, software, and user accounts**

1.2. Fault Management

- Proper operation of the network depends on the proper operation of each component individually and in relation to each other
- **Fault management** handles this issue whether individual component or relation between component is working properly or not.
- Fault management system has two subsystems:
 1. **Reactive fault management system** is responsible for detecting, isolating, correcting, and recording faults. It handles short-term solutions to faults
 2. **Proactive fault management** tries to prevent faults from occurring. Although this is not always possible, some types of failures can be predicted and prevented

1.3. Performance Management

- **Performance management**, which is closely related to fault management, tries to monitor and control the network to ensure that it is running as efficiently as possible
- Performance management tries to quantify performance by using some measurable quantity such as
 1. Capacity : he performance management system must ensure that it is not used above this capacity
 2. Traffic : Traffic can be measured in two ways: **internally and externally**. **Internal traffic** is measured by the number of packets (or bytes) traveling inside the network. **External traffic** is measured by the exchange of packets (or bytes) outside the network
 3. Throughput : Performance management monitors the throughput to make sure that it is not reduced to unacceptable levels
 4. Response Time : Response time is normally measured from the time a user requests a service to the time the service is granted

1.4. Security Management

- **Security management** is responsible for controlling access to the network based on the predefined policy
- Security management is done with help of Cryptography, Digital signature, IPSec, VPN

1.5. Accounting Management

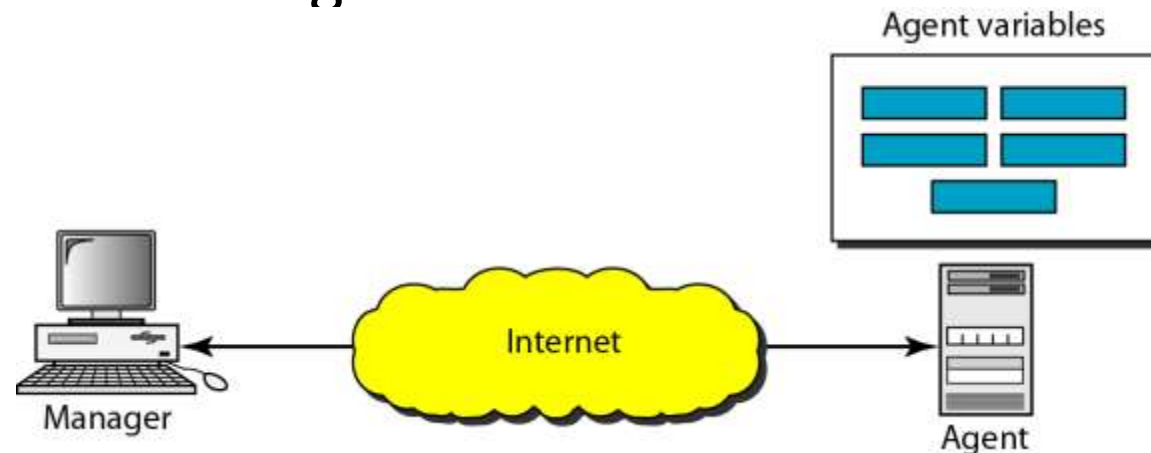
- Accounting management is the control of users access to network resources through charges
- Under accounting management, individual users, departments, divisions, or even projects are charged for the services they receive from the network
- Organizations use an accounting management system for the following reasons:
 1. It prevents users from monopolizing limited network resources
 2. It prevents users from using the system inefficiently
 3. Network managers can do short- and long-term planning based on the demand for network use

2. SNMP

- **Simple Network Management Protocol (SNMP)** is a framework for managing devices in network
- It provides a set of fundamental operations for **monitoring** and **maintaining** network
- SNMP uses the concept of **manager** and **agent**
- SNMP is an application-level protocol in which a few manager stations control a set of agents
- **Manager**, usually a host, **controls** and **monitors** a set of **agents**, usually routers

2.1. SNMP Concepts

- Management is achieved through simple interaction between a **manager** and an **agent**
- **Agent** keeps performance information in a database
- **Manager** has access to the values in the database
- The manager can fetch and compare the values of these two variables to see if the router is congested or not



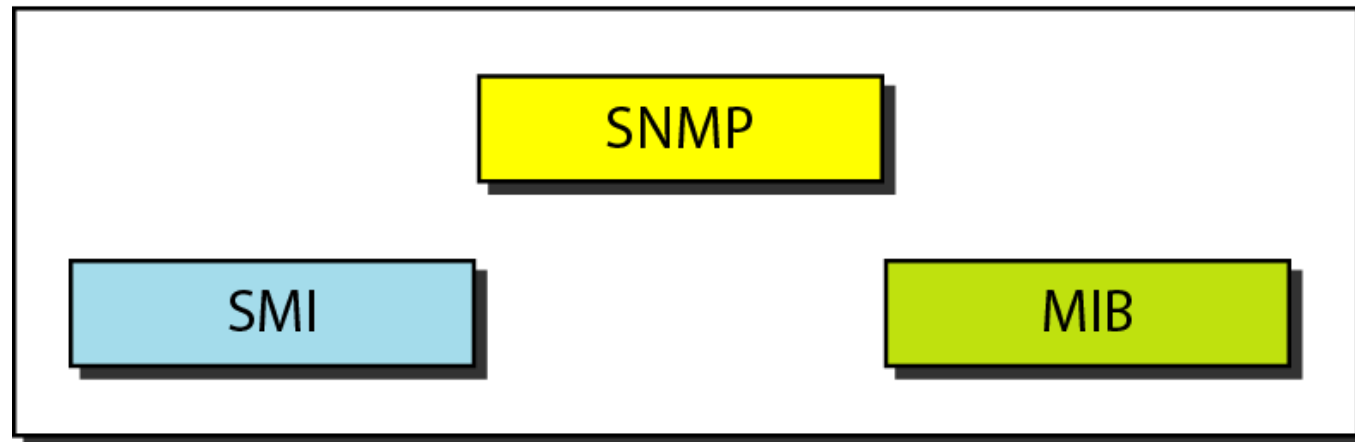
2.1. SNMP Concepts

- Management with SNMP is based on three basic ideas:
 1. A manager checks an agent by requesting information that reflects the behaviour of the agent.
 2. A manager forces an agent to perform a task by resetting values in the agent database.
 3. An agent contributes to the management process by warning the manager of an unusual situation
- **SNMP managed network** consists of three key components:
 1. Managed device → Device which is managed by **SNMP also called network elements**
 2. Agent → software which runs on managed devices
 3. Network management system (NMS) → software which runs on the manager

2.2. SNMP Components

- For management tasks SNMP uses two other protocols:
 1. Structure of Management Information (SMI)
 2. Management Information Base (MIB)
- Management on the Internet is done through the cooperation of the three protocols **SNMP**, **SMI**, and **MIB**

Management



2.2.1. Role of SNMP

- SNMP has some very specific roles in network management. They are:
 1. Defines the format of the packet to be sent from a manager to an agent and vice versa
 2. Interprets the result and creates statistics
 3. The packets exchanged contain the object (variable) names and their status (values)
 4. SNMP is responsible for reading and changing these values

2.2.2. Role of SMI

- SMI functions are:
 1. To name objects
 2. To define the type of data that can be stored in an object
 3. To show how to encode data for transmission over the network
- SMI does not define the number of objects an entity should manage or name the objects to be managed or define the association between the objects and their values

2.2.3. Role of MIB

- MIB creates
 1. A set of objects defined for each entity similar to a database
 2. MIB creates a collection of named objects, their types
 3. Creates objects relationships to each other in an entity to be managed
- MIB must define the number of objects, name them according to the rules defined by SMI, and associate a type to each named object

3. Security

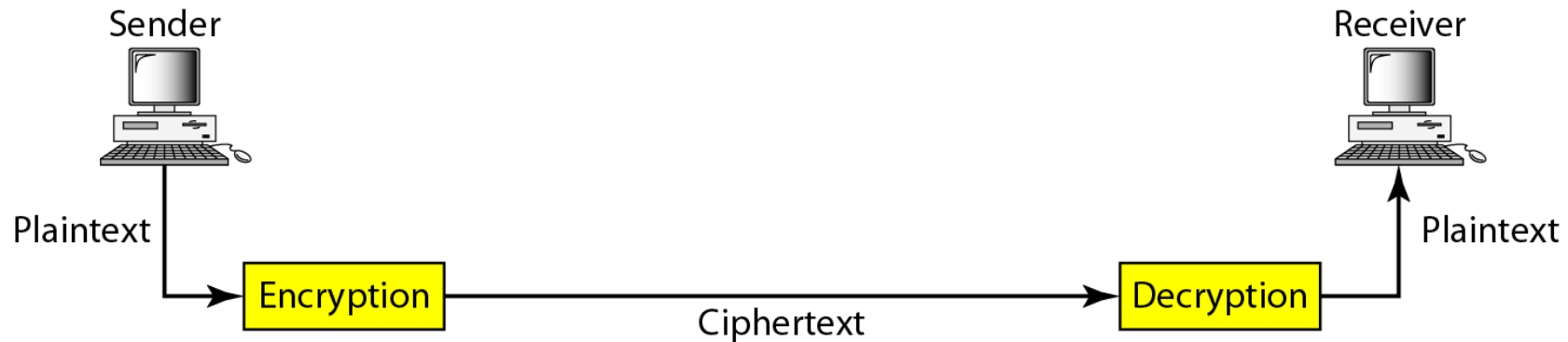
- Security is need for unauthorised access of the data in communication
- Security in network is provided by help of cryptography, IP security, Firewall (All topics are discussed in sections 4,5,6,7,8)
- Computer and network security requirements:
 1. **Confidentiality:** Requires that data only be accessible by authorized parties.
 2. **Integrity:** Requires that data can be modified only by authorized users. Modification includes writing, changing, changing status, deleting and creating.
 3. **Availability:** Requires that data are available to authorized parties.
 4. **Authenticity:** Requires that host or service be able to verify the identity of a user

4. Cryptography

- **Cryptography**, a word with Greek origins, cryptos means “*secret*” and graphein means “*writing*”
- Cryptography refers to the science and art of transforming messages to make them secure and immune to attacks
- Terms used:
 - **Plain-text** : Messages which are in readable format (Original Message)
 - **Cipher-Text** : Messages which are not in readable format (Scrambled Message)
 - **Encryption** : Converting plain-text to cipher-text (like locking)
 - **Decryption** : Converting cipher-text to plain-text (like unlocking)
 - **Cipher** : Encryption and decryption algorithms are commonly called cipher
 - **Key** : Key is used to encryption and decryption algorithm to convert messages to different format (like a password)

4. Cryptography

- Before message is sent by the sender to the network , the message the user entered (plain-text) will be encrypted (converting plain-text to cipher-text) and after receiving the cipher-text will be decrypted (converting cipher-text to plain-text) and used by receiver

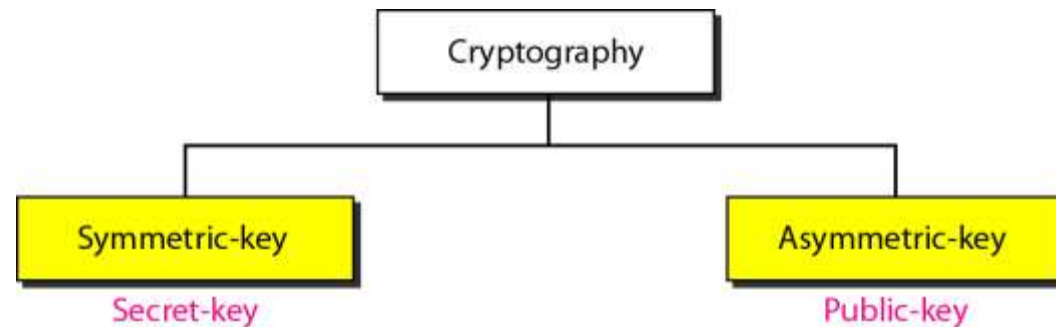


4.1. Cryptography - Characters (*Alice, Bob, and Eve*)

- Three characters in an information exchange scenario
- Alice is the person who needs to send secure data
- Bob is the recipient of the data
- Eve is the person who somehow disturbs the communication between Alice and Bob by intercepting messages to uncover the data or by sending her own disguised messages
- *These three names represent computers or processes that actually send or receive data, or intercept or change data in coming sections*

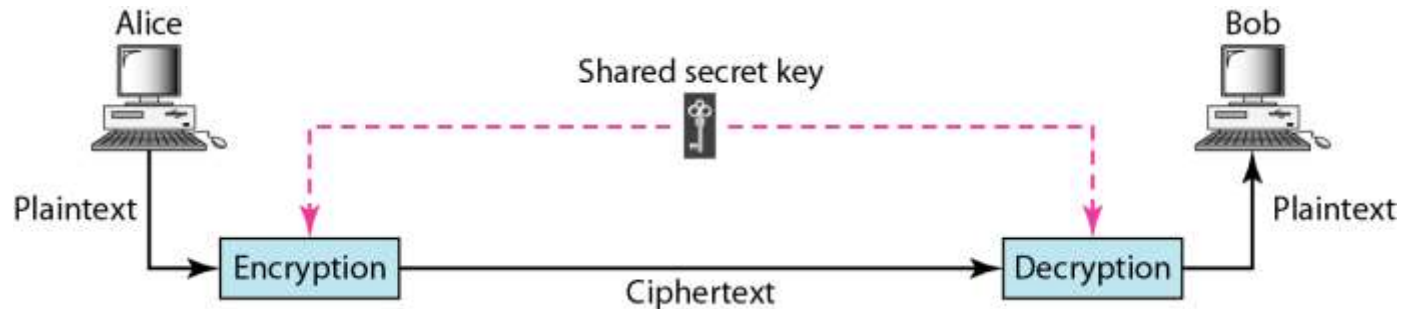
4.2. Cryptography Categories

- Cryptographic ciphers (algorithms) are divided into two groups:
 1. Symmetric key cryptography
 - Also called secret-key cryptography
 - Same key for sender (Encryption) and receiver (Decryption)
 2. Asymmetric cryptography
 - Also called public-key cryptography
 - Different key for Sender (Encryption) and receiver (Decryption)



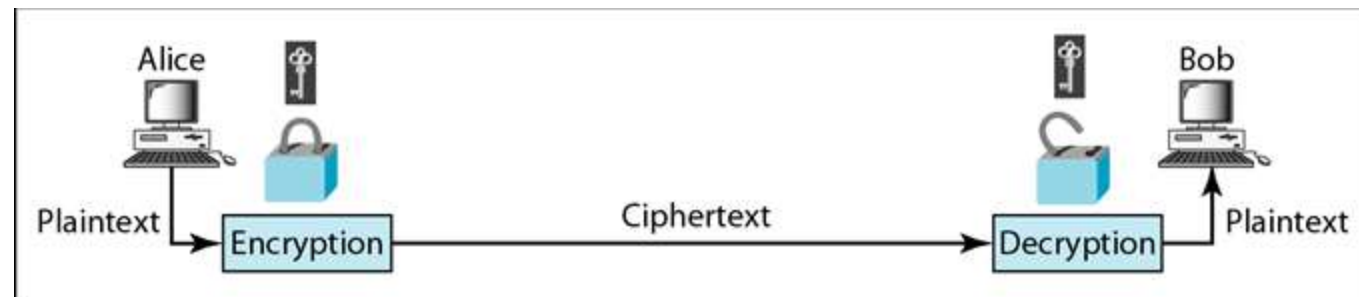
4.2.1. Symmetric key Cryptography

- It is also called **secret-key** cryptography
- In symmetric-key cryptography, the same key is used by both parties
- The sender uses this key and an encryption algorithm to encrypt data
- The receiver uses the same key and the corresponding decryption algorithm to decrypt the data
- The key is shared



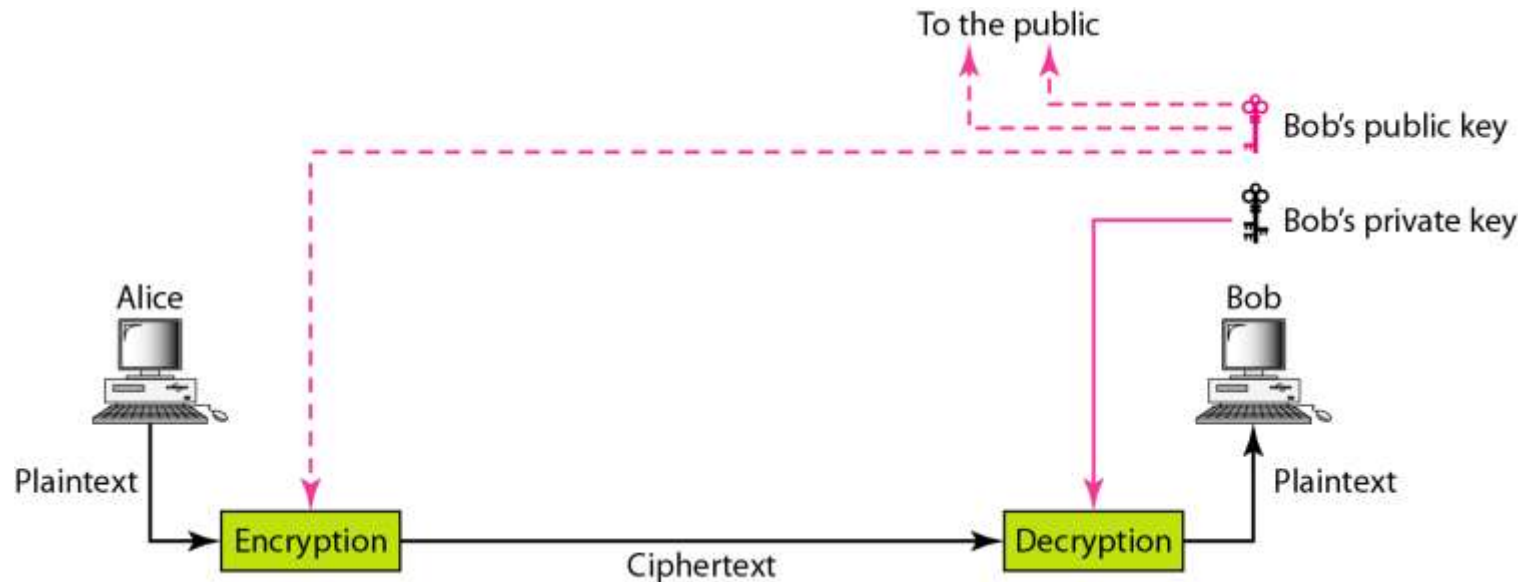
4.2.1. Symmetric key Cryptography

- **Key Exchange** : If Alice wanted to send data to bob using symmetric key Alice will first send the key used for encryption (Shared secret key) to the Bob
- Alice will encrypt the data using encryption algorithm + shared key
- Bob will decrypt the data using decryption algorithm + shared key



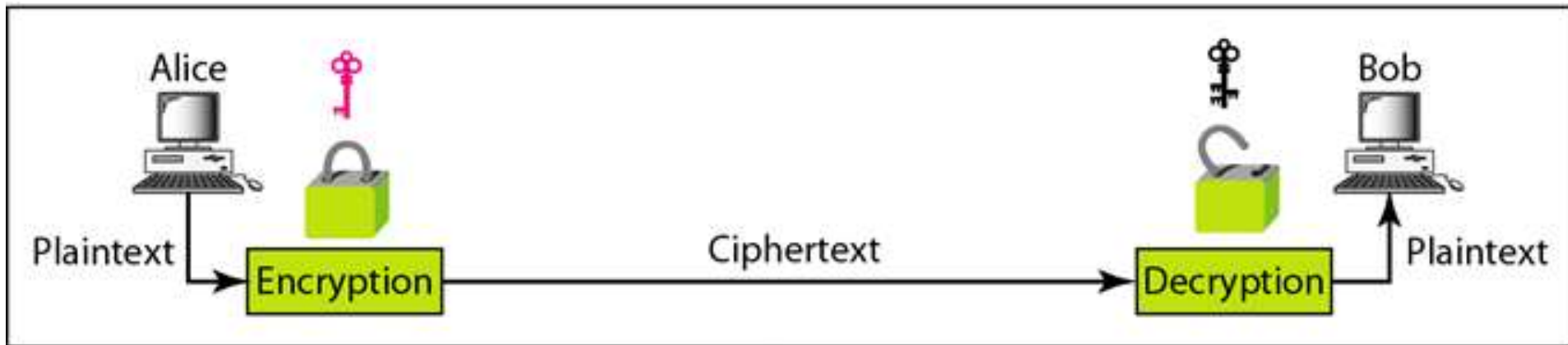
4.2.2. Asymmetric Cryptography

- In asymmetric or public-key cryptography, there are two keys
 1. **Private key:** is kept by the receiver (only Bob)
 2. **Public key:** is announced to the public (Every one who wanted to communicate with Bob)



4.2.2. Asymmetric Cryptography

- Imagine Alice wants to send a message to Bob, Alice uses the public key to encrypt the message , When the message is received by Bob, the private key is used to decrypt the message
- In public-key encryption/decryption, the **public key** that is used for **encryption** and the **private key** that is used for **decryption**

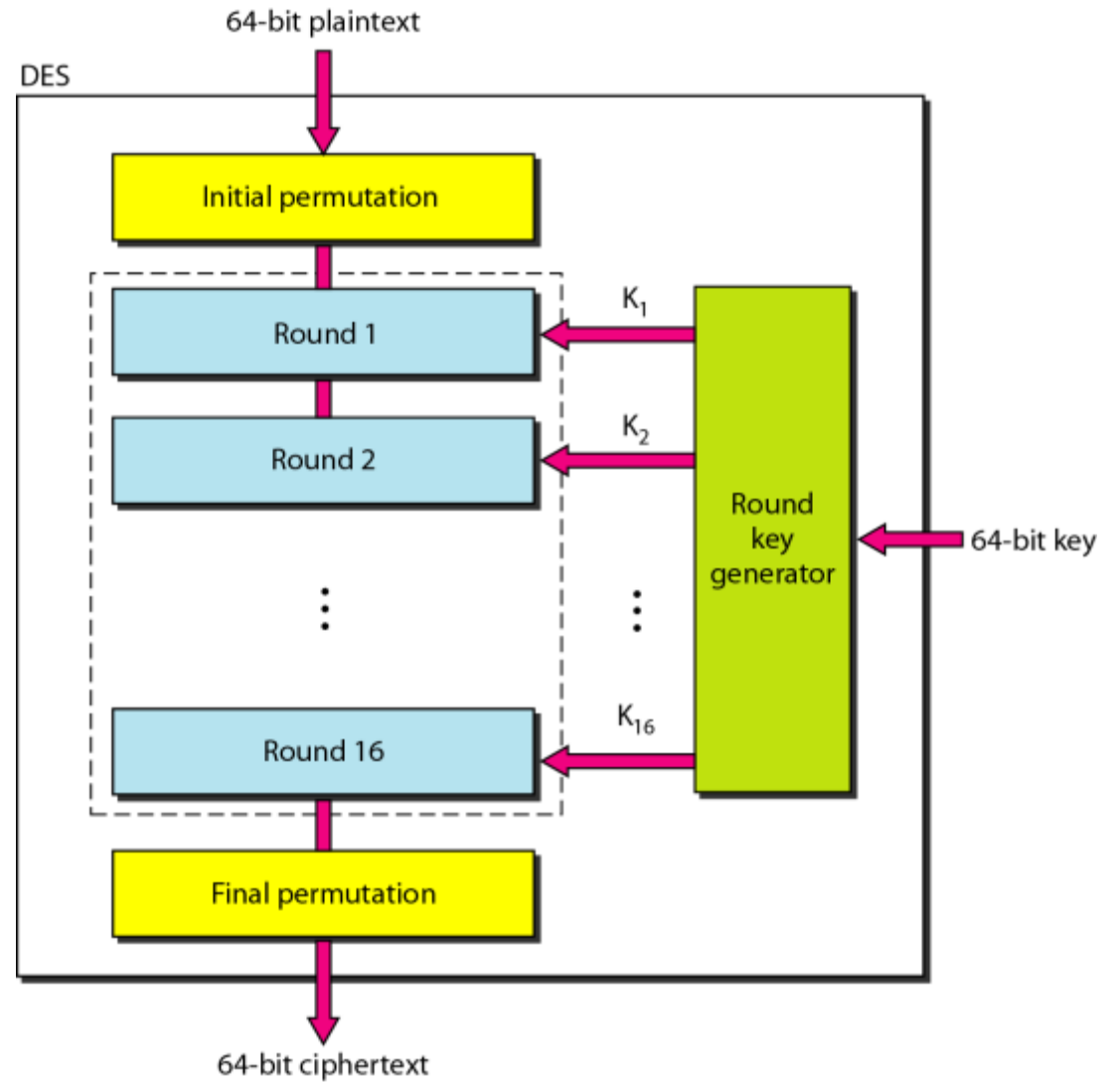


4.3. DES (Data Encryption Standard)

- It is symmetric Key algorithm
- The algorithm encrypts a **64-bit plaintext** block using a **64-bit key**
- DES has two transposition blocks (P-boxes) and 16 complex round ciphers (they are repeated)
- Although the 16 iteration round ciphers are conceptually the same, each uses a different key derived from the original key.

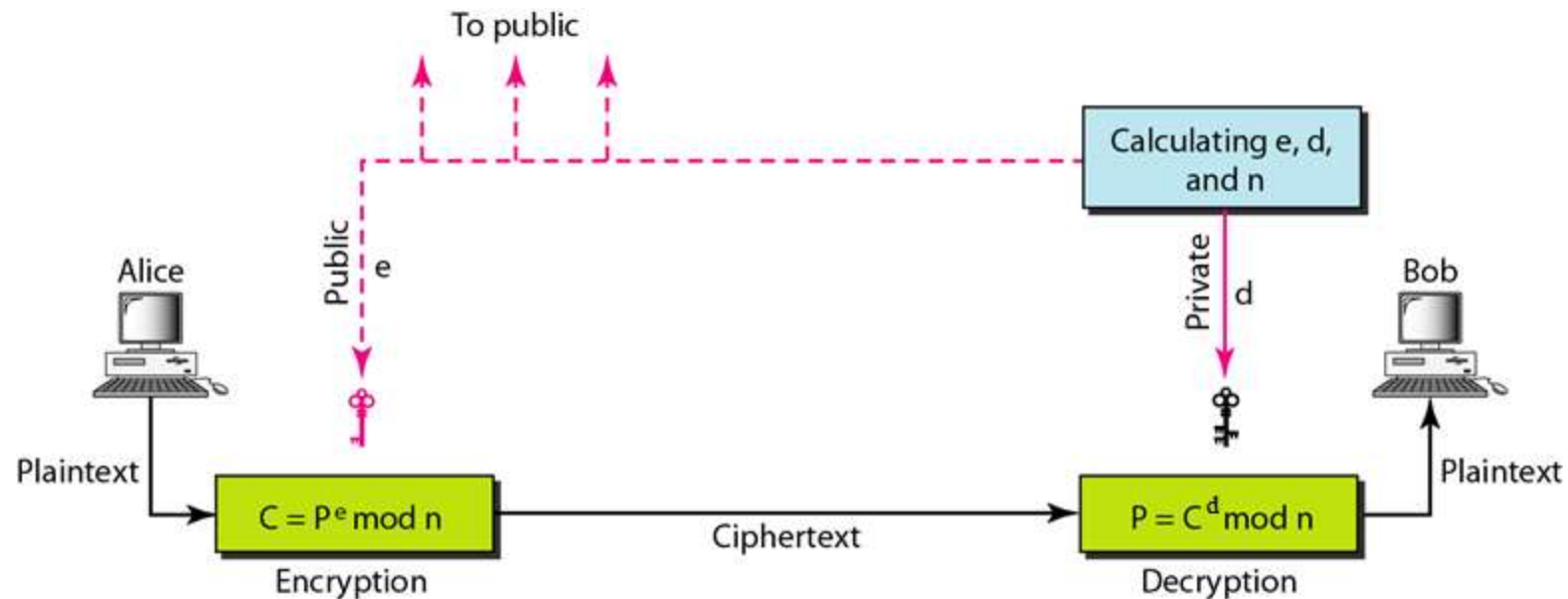
4.3. DES (Data Encryption Standard)

1. The initial and final permutations are keyless straight permutations that are the inverse of each other
2. The permutation takes a 64-bit input and permutes them according to predefined values.
3. Each round of DES is a complex round cipher, as shown in Figure
4. The structure of the encryption round ciphers is different from that of the decryption one



4.4. RSA (Rivest, Shamir, Adleman)

- It is Asymmetric Key algorithm
- Uses two numbers, e and d, as the public and private keys
- RSA method is based on some principles from number theory



4.4. RSA (Rivest, Shamir, Adleman)

Selecting Keys for encryption and Decryption

1. Choose two large primes, p and q (typically 1024 bits).
 2. Compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$.
 3. Choose a number relatively prime to z and call it d .
 4. Find e such that $e \times d = 1 \pmod{z}$.
- e and n are announced public (Bob's public key)
 - d and n are kept in private (Bob's private key)

4.4. RSA (Rivest, Shamir, Adleman)

In sender (Alice)

- Encryption is done with following method

$$C = P^e \text{ mod } n$$

- where C is cipher text, P is plain text e & n are the public key

In Receiver (Bob)

- Encryption is done with following method

$$P = C^d \text{ mod } n$$

- where C is cipher text, P is plain text d & n are the private key

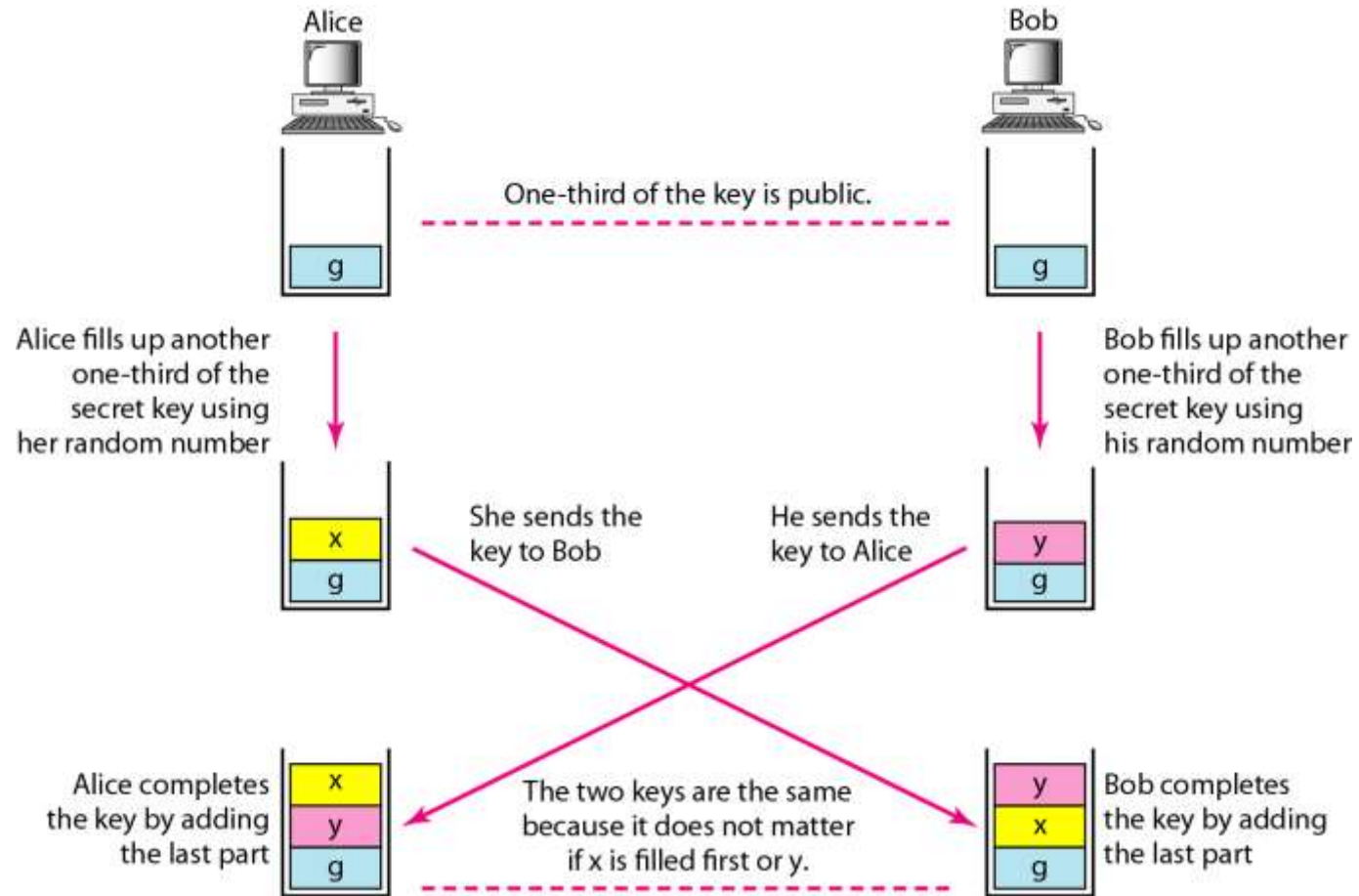
5. Key Exchange

- Key exchange is necessary for symmetric algorithm where copy of same key is used for encryption and decryption
- Sharing of key is necessary between sender(Alice) and receiver(Bob)
- Process of informing the information about key to receiver by sender is **KEY EXCHANGE**

5.1. Diffie- Hallman Key

- **Diffie-Hellman** cryptosystem, two parties create a symmetric session key to exchange data without having to remember or store the key for future use
- Before establishing a symmetric key, the two parties need to choose two numbers p and g
- p - large prime number on the order of 300 decimal digits (1024 bits)
- g - second number is a random number.
- ***These two numbers need not be confidential. They can be sent through the Internet; they can be public***

5.1. Diffie-Hallman Key



5.1. Diffie- Hallman Key

Steps

1. Alice chooses a large random number x and calculates $R1 = g^x \text{ mod } p$
2. Bob chooses another large random number y and calculates $R2 = g^y \text{ mod } p$
3. Alice sends $R1$ to Bob. Note that Alice does not send the value of x ; she sends only $R1$
4. Bob sends $R2$ to Alice. Again, Note that Bob does not send the value of y ,
5. he sends only $R2$.
6. Alice calculates $K = R2^x \text{ mod } p$
7. Bob also calculates $K = R1^y \text{ mod } p$

The symmetric key for the session is $K = g^{xy} \text{ mod } p$

5.1.1. Example Diffie- Hallman Key Exchange

- *Let us give a trivial example to make the procedure clear. Our example uses small numbers, but note that in a real situation, the numbers are very large. Assume $g = 7$ and $p = 23$. The steps are as follows:*
- *1. Alice chooses $x = 3$ and calculates $R_1 = 7^3 \bmod 23 = 21$.*
- *2. Bob chooses $y = 6$ and calculates $R_2 = 7^6 \bmod 23 = 4$.*
- *3. Alice sends the number 21 to Bob.*
- *4. Bob sends the number 4 to Alice.*
- *5. Alice calculates the symmetric key $K = 4^3 \bmod 23 = 18$.*
- *6. Bob calculates the symmetric key $K = 21^6 \bmod 23 = 18$.*
- *The value of K is the same for both Alice and Bob;
 $g^{xy} \bmod p = 7^{18} \bmod 23 = 18$.*

5.2. Kerberos

- Kerberos is an authentication protocol
- It is also used for providing Shared secret key
- Kerberos is not used for person-to-person authentication.

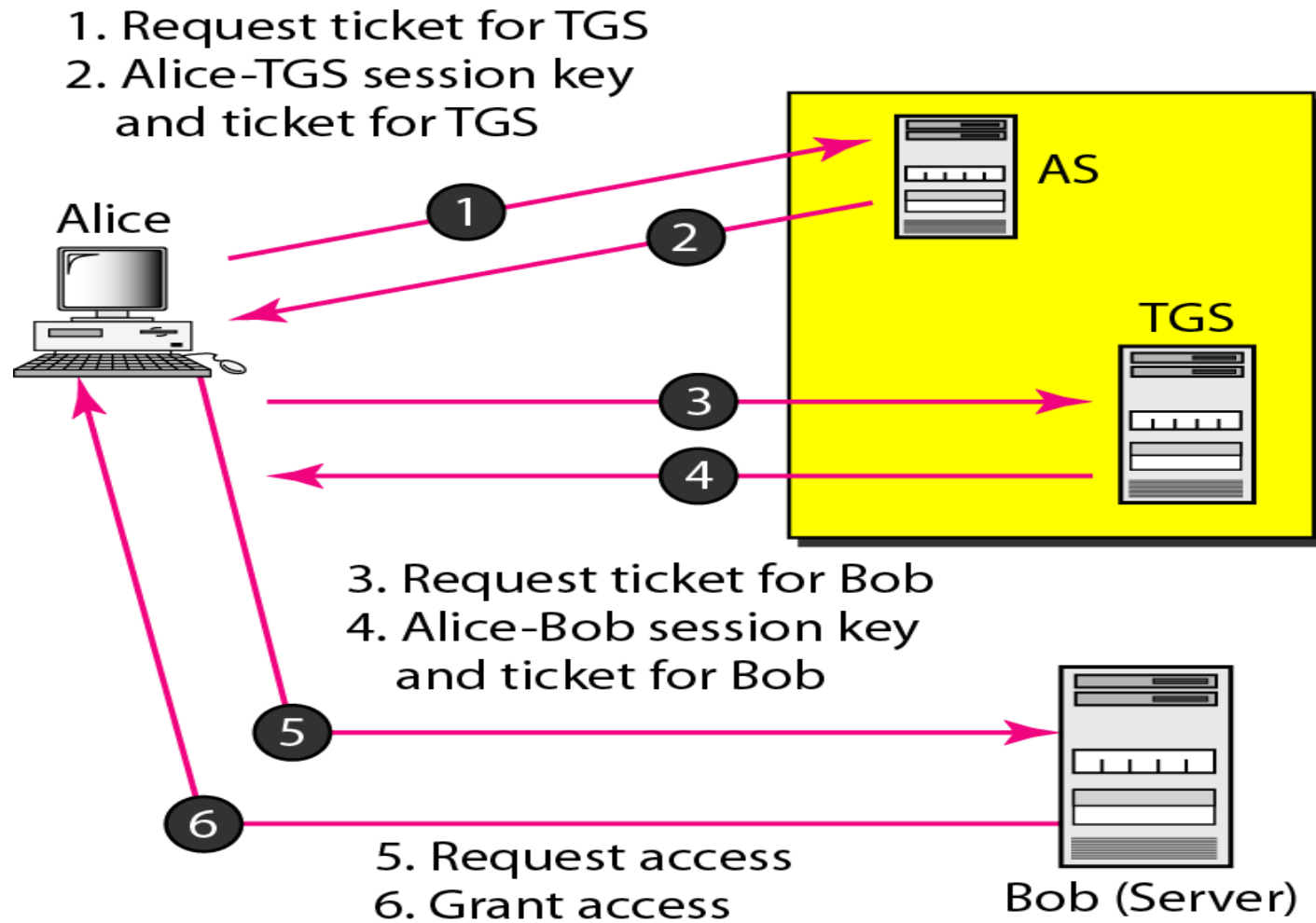
Servers

- Three servers are involved in the Kerberos protocol
 1. Authentication server(AS)
 2. Ticket-granting server (TGS)
 3. Real (data) server that provides services to others
- In our examples and figures Bob is the real server and Alice is the user requesting service.

5.2. Kerberos

- **Authentication Server (AS)** : AS is the KDC in Kerberos protocol. Each user registers with AS and is granted a user identity and a password. AS has a database with these identities and the corresponding passwords
- **Ticket-Granting Server (TGS)** : TGS issues a ticket for the real server (Bob). It also provides the session key (K_{AB}) between Alice and Bob
- **Real Server** : The real server (Bob) provides services for the user (Alice)

5.2. Kerberos



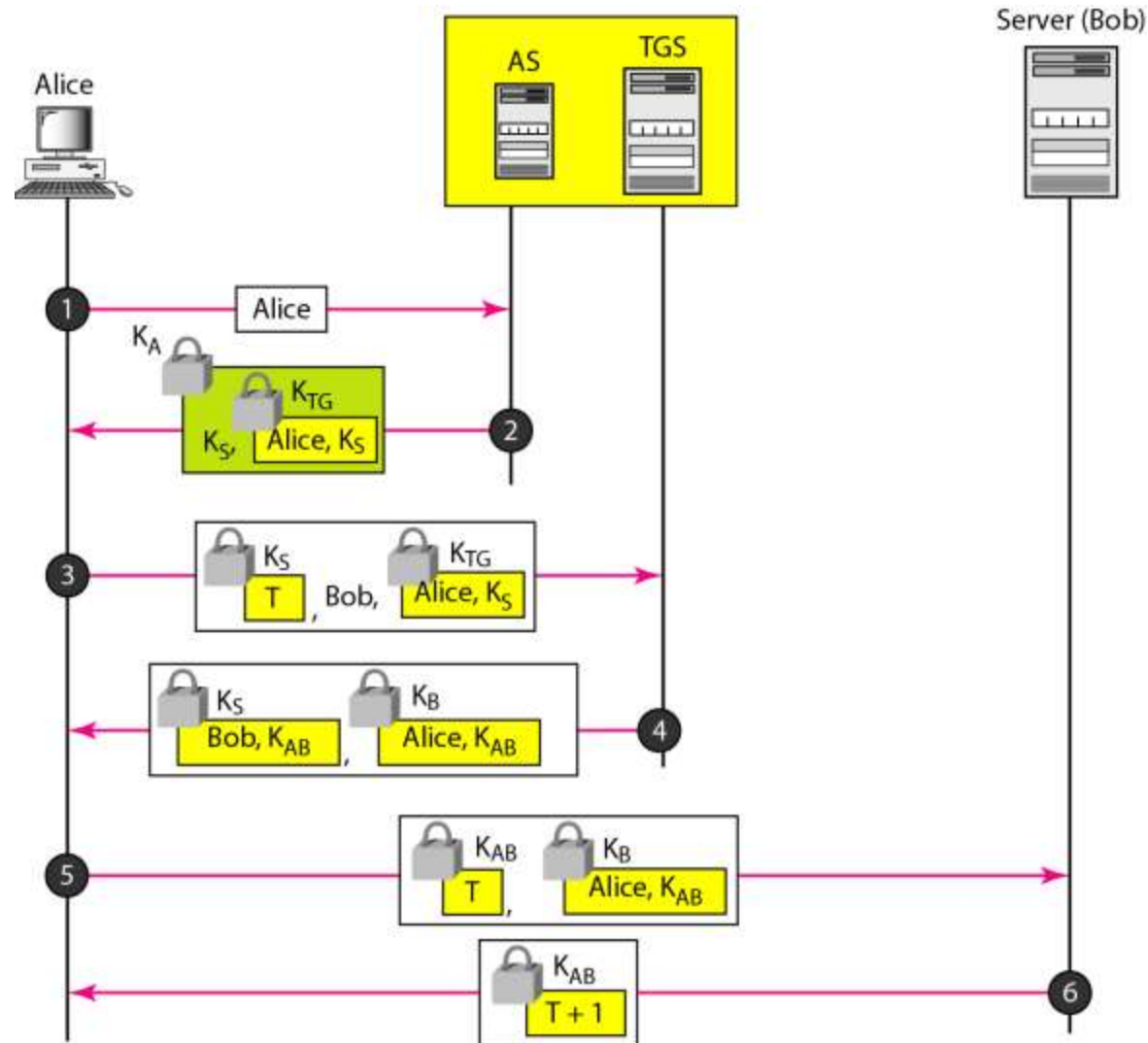
5.2.1. Kerberos Procedure

1. Alice sends her request to AS in plaintext, using her registered identity
2. AS sends a message encrypted with Alice's symmetric key K_A - The message contains **two items: session key K_S** that is used by Alice to contact TGS and a **ticket** for TGS that is encrypted with the TGS symmetric key K_{TG}
3. Alice now sends **three items** to TGS. first is the **ticket** received from AS. The second is the **name of the real server (Bob)**, the third is a **timestamp** which is encrypted by K_S . The timestamp prevents a replay by Eve

5.2.1. Kerberos Procedure

4. TGS sends two tickets, each containing the session key between Alice and Bob K_{AB} . The ticket for Alice is encrypted with K_S ; the ticket for Bob is encrypted with Bob's key K_B
5. Alice sends Bob's ticket with the timestamp encrypted by K_{AB}
6. Bob confirms the receipt by adding 1 to the timestamp. The message is encrypted with K_{AB} and sent to Alice

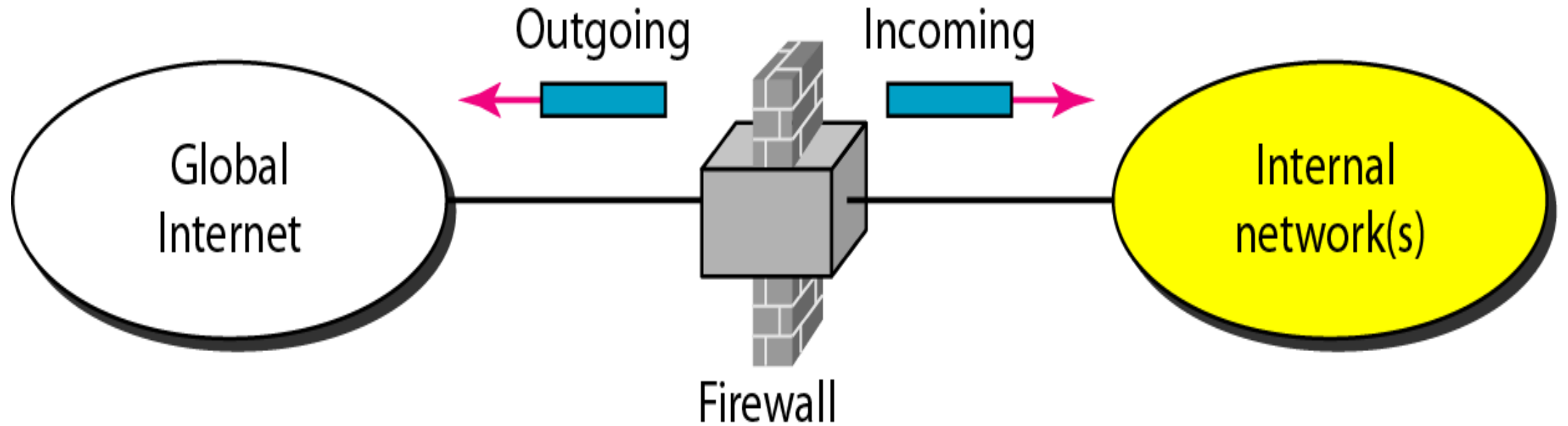
5.2.1. Kerberos Procedure



6. Firewall

- A **firewall** is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet
- Firewall is designed to **forward** some packets and **filter** (not forward) others
- A firewall is a network security system designed to prevent unauthorized access to or from a private network
- Firewalls can be implemented in both hardware and software, or a combination of both
- Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected
- All messages entering or leaving the LAN pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria

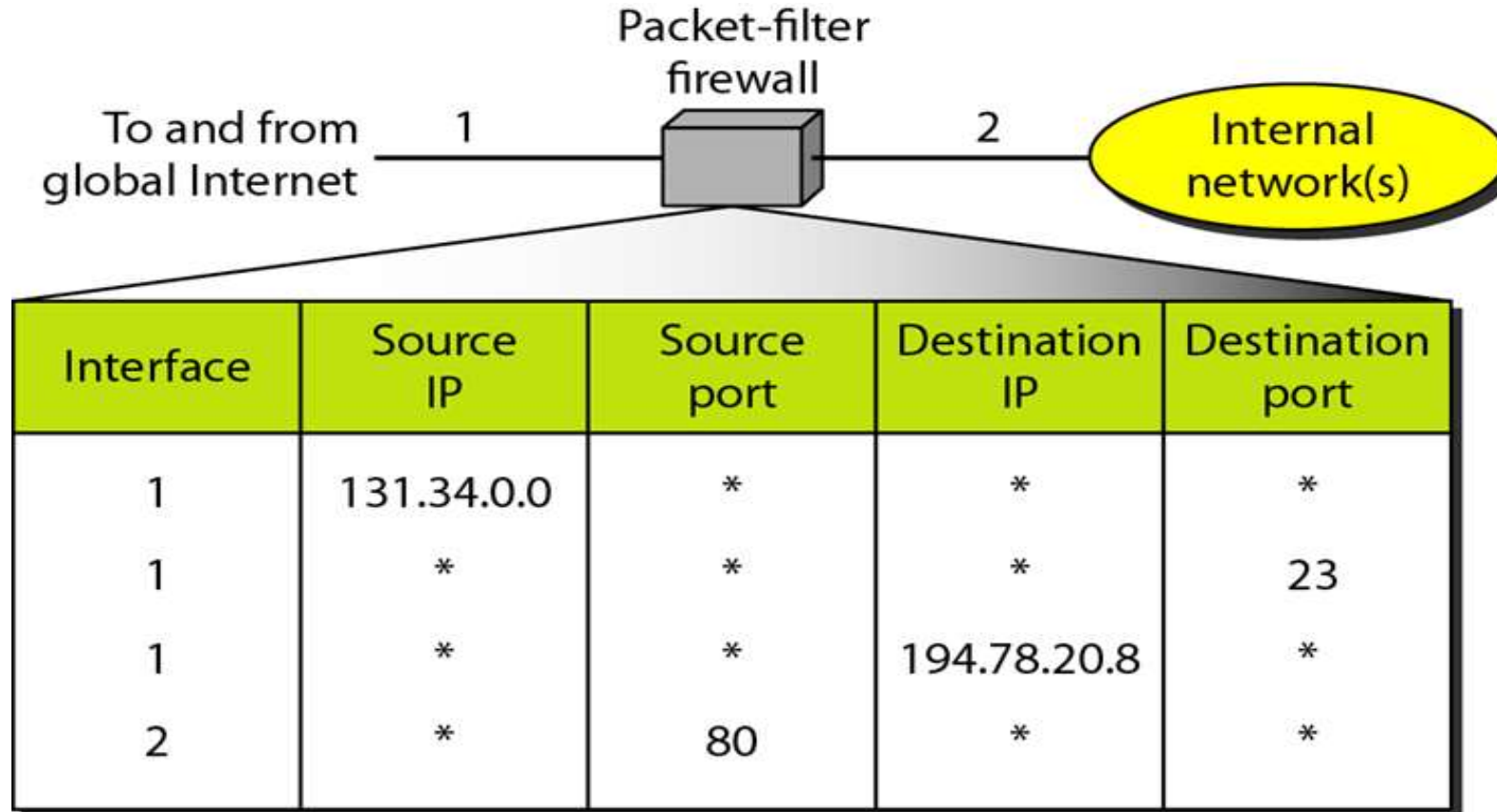
6. Firewall



6.1. Packet Filter Firewall

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

6.1. Packet Filter Firewall

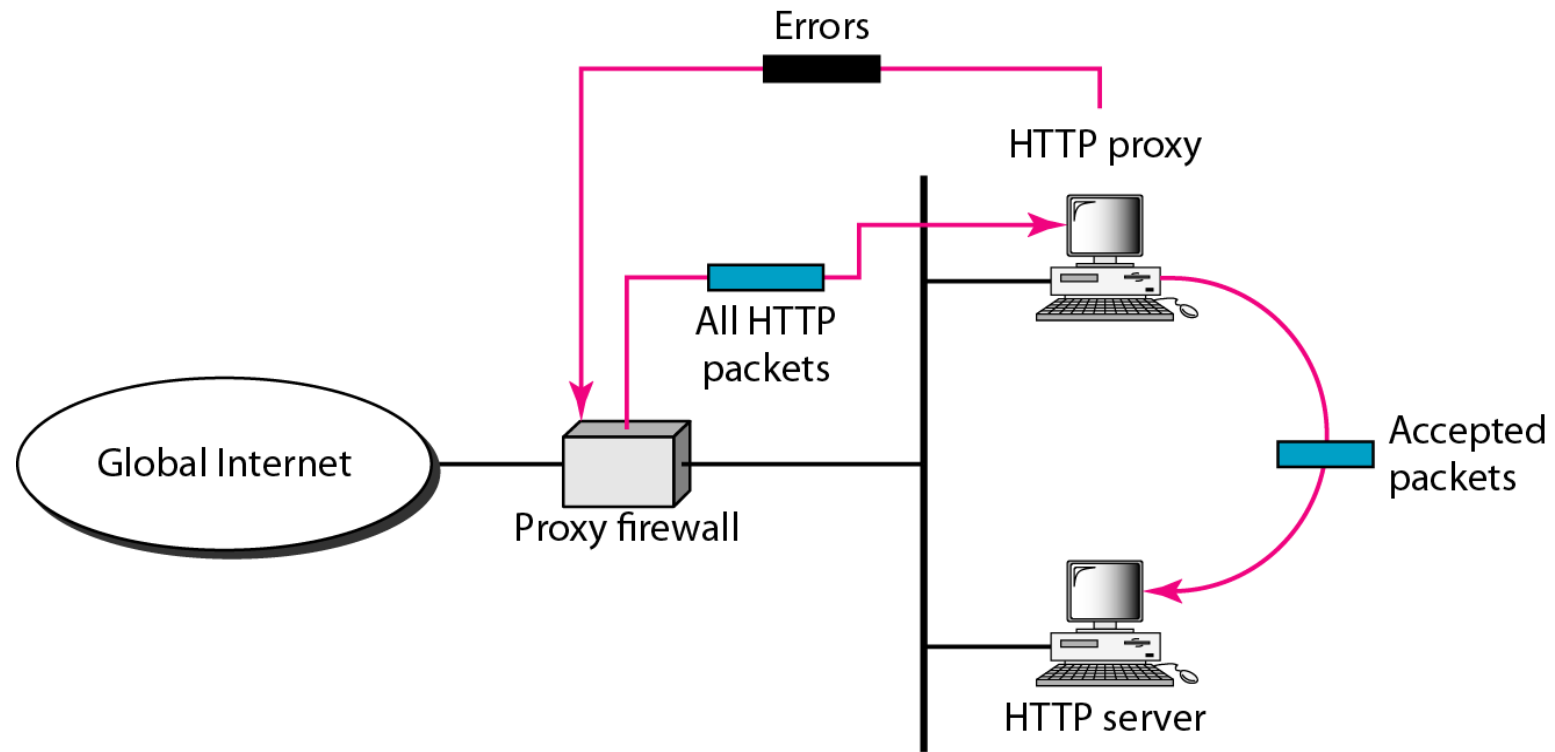


* means any network

6.2. Proxy Firewall

- If we need to filter a message based on the information available in the message itself (at the application layer)
- If application level data (like text, URL, websites, links) is to be filtered then proxy firewall is best solution

6.2. Proxy Firewall



6.1. Types of Firewall (Hardware)

- Hardware firewalls is dedicated device which can be configured according to the need of large organization

Features

- They are specialized devices
- Hardware firewalls tend to be expensive
- Complicated
- Difficult to upgrade,
- Difficult to configure

6.2. Types of Firewall-Software

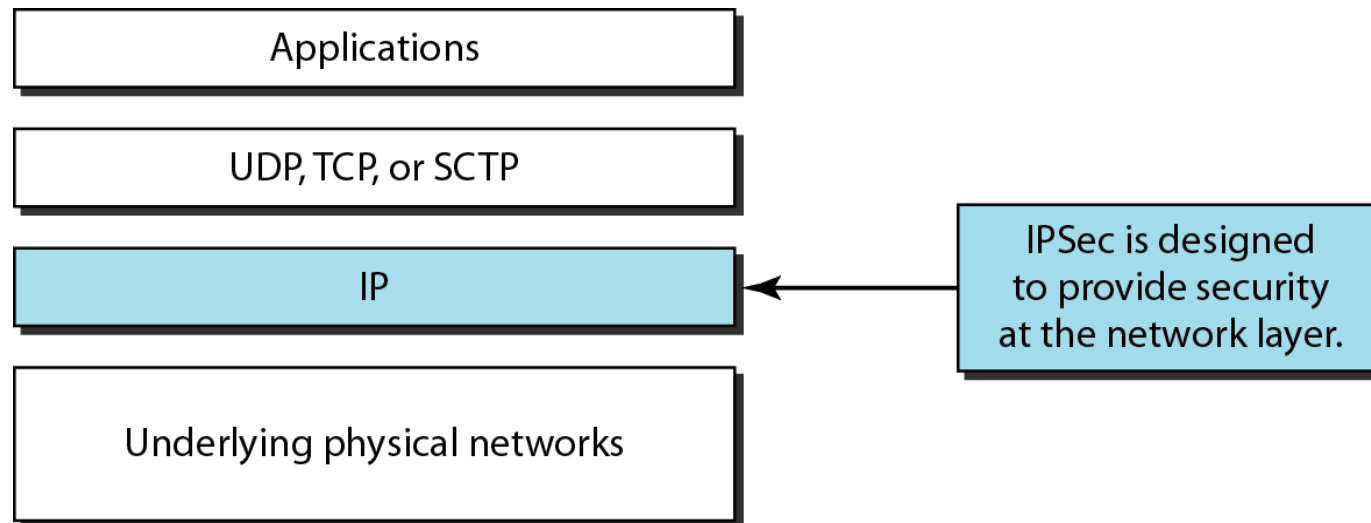
- Hardware firewall can be configured in PC. It runs as a program in the PC and configuration can be done

Features

- They are not specialized devices (Only special Programs in PC)
- Less expensive
- Easy to upgrade
- Easy to configure
- Less Complicated

7. IPSec (Internet Protocol Security)

- IPSecurity (IPSec) is a collection of protocols designed to provide **security** for a packet at the **network level**
- IPSec helps to create **authenticated and confidential** packets for the Network layer

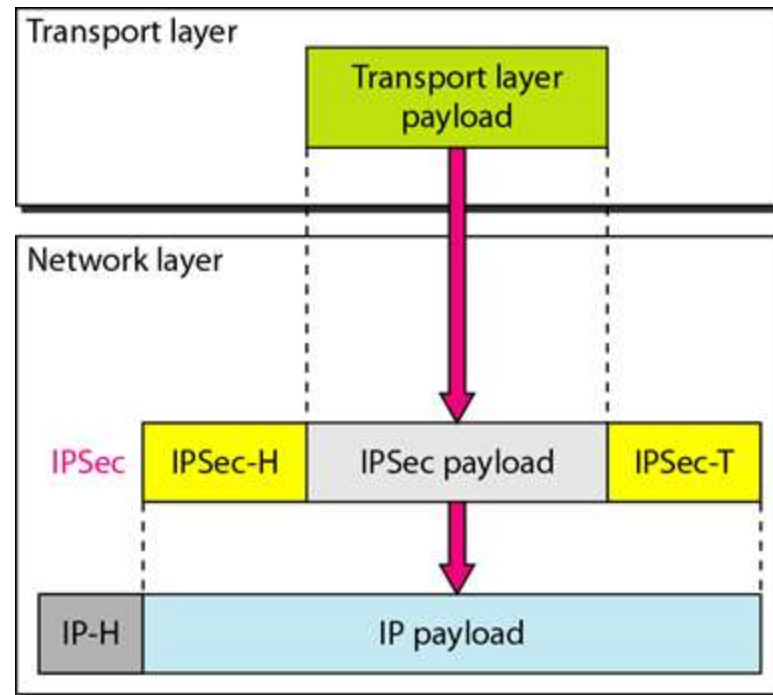


7. IPSec (Internet Protocol Security)

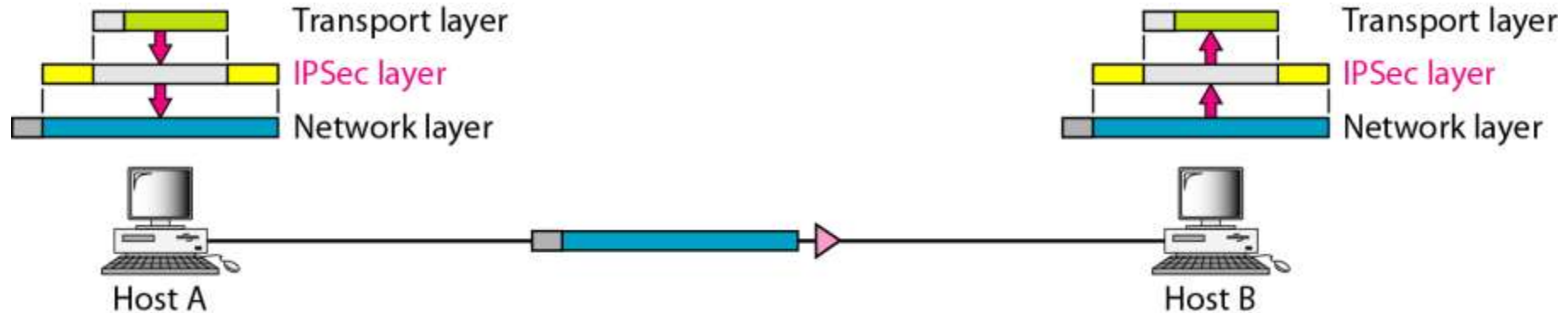
- Features are :
 1. Data confidentiality
 2. Data integrity
 3. Data origin authentication
 4. Anti-replay
- Provides 2 Protocols
 1. Authentication Header (AH) Protocol
 2. Encapsulating Security Payload (ESP) Protocol
- IPSec have two modes of operation
 1. Transport mode
 2. Tunnel Mode

7.1. Transport Mode

- IPSec in the transport mode does not protect the IP header; it only protects the information coming from the transport layer



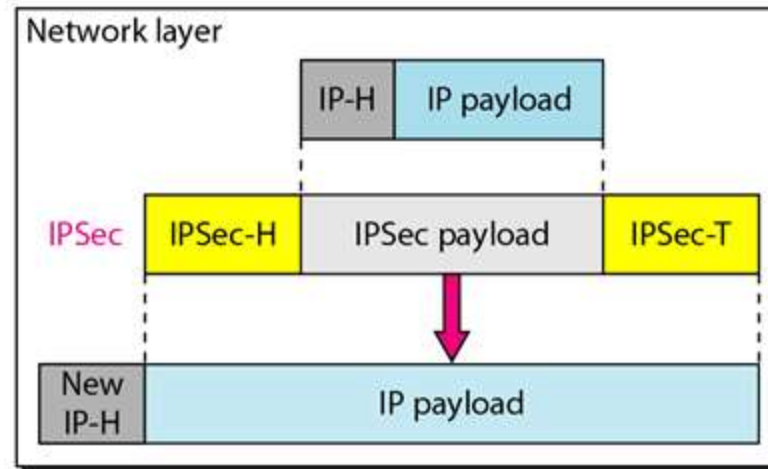
7.1. Transport Mode



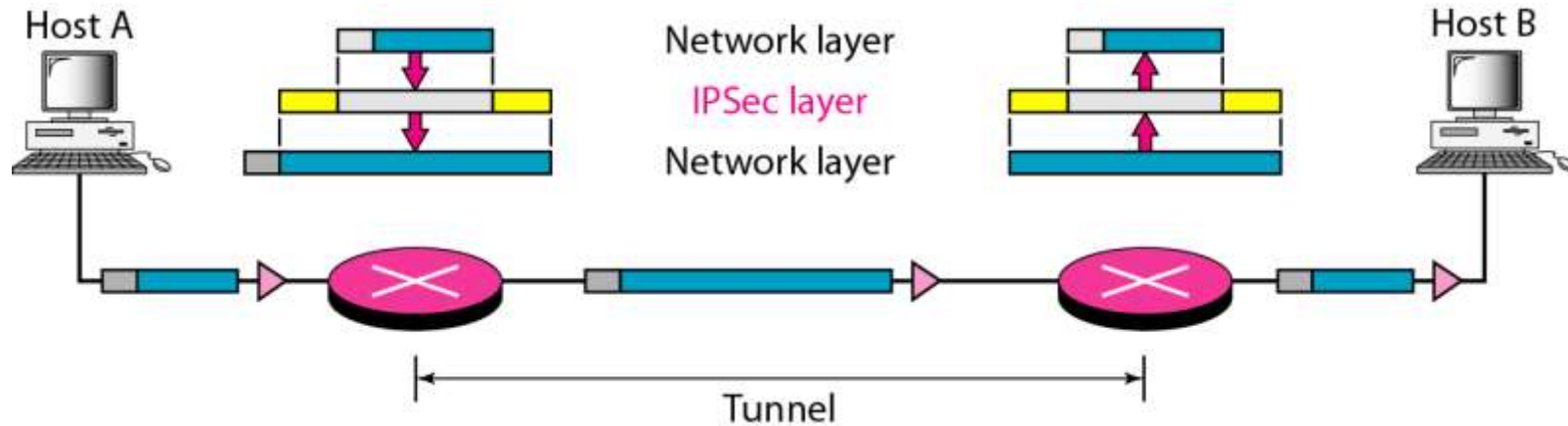
- The transport mode is normally used when we need host-to-host (end-to-end) protection of data
- Sending host : Encrypt the data from transport layer and convert to IP Packet in network layer
- Receiving host : Decrypt the IP packet from network layer and deliver it to the transport layer

7.2. Tunnel Mode

- IPSec protects the entire IP packet
- It takes an IP packet, including the header, applies IPSec security methods to the entire packet



7.2. Tunnel Mode



- The tunnel mode is normally used between two routers, between a host and a router, or between a router
- In this method whole packet goes through an imaginary tunnel

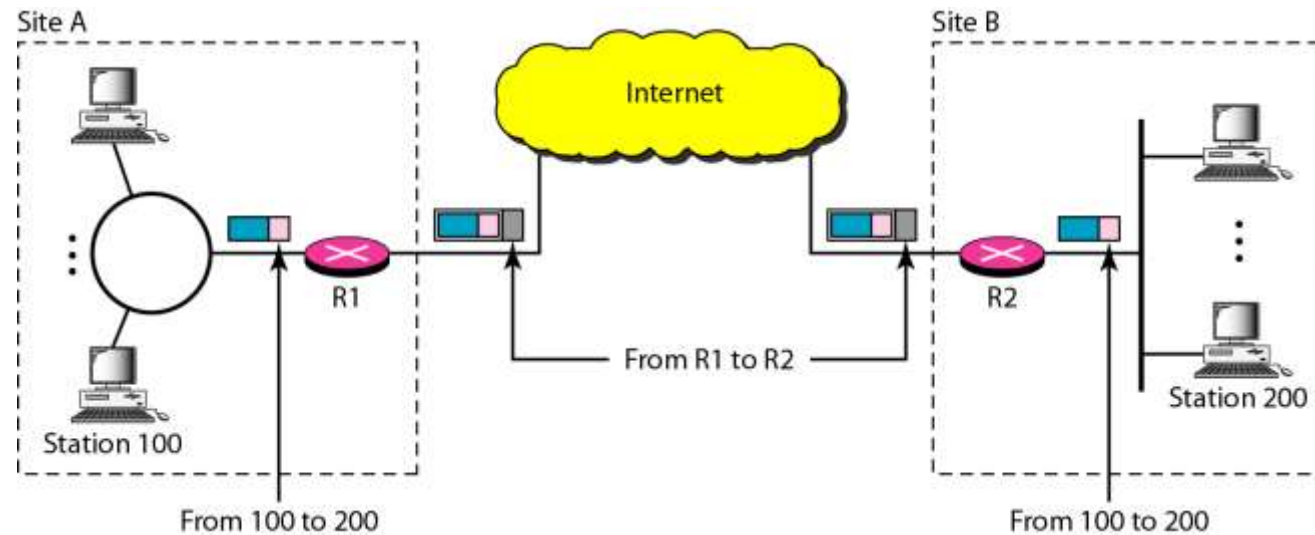
8. VPN (Virtual Private Network)

- Virtual private network (VPN) is a technology that provide privacy in communication through internet for both intra/inter organization communication
- Using Private dedicated (Private WAN)line between 2 end is very costly , VPN through Internet (Public WAN) with help of VPN provide privacy
- VPN technology uses IPSec in the tunnel mode to provide authentication, integrity, and privacy

8. VPN (Virtual Private Network)

- VPN creates a network that is private but virtual It is private because it guarantees privacy inside the organization
- It is virtual because it does not use real private WANs; the network is physically public but virtually private
- **Tunnelling** : To guarantee privacy and other security measures for an organization, VPN can use the IPSec in the tunnel mode
- Outsiders cannot decipher the contents of the packet or the source and destination addresses

8. VPN (Virtual Private Network)



- Multiple Encapsulation in Datagram
- Two or more Encapsulation is done in above figure
- First Encapsulation from 100 to 200
- Second Encapsulation from R1 to R2