Computer Networks

Basic Concepts

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Basic Concepts

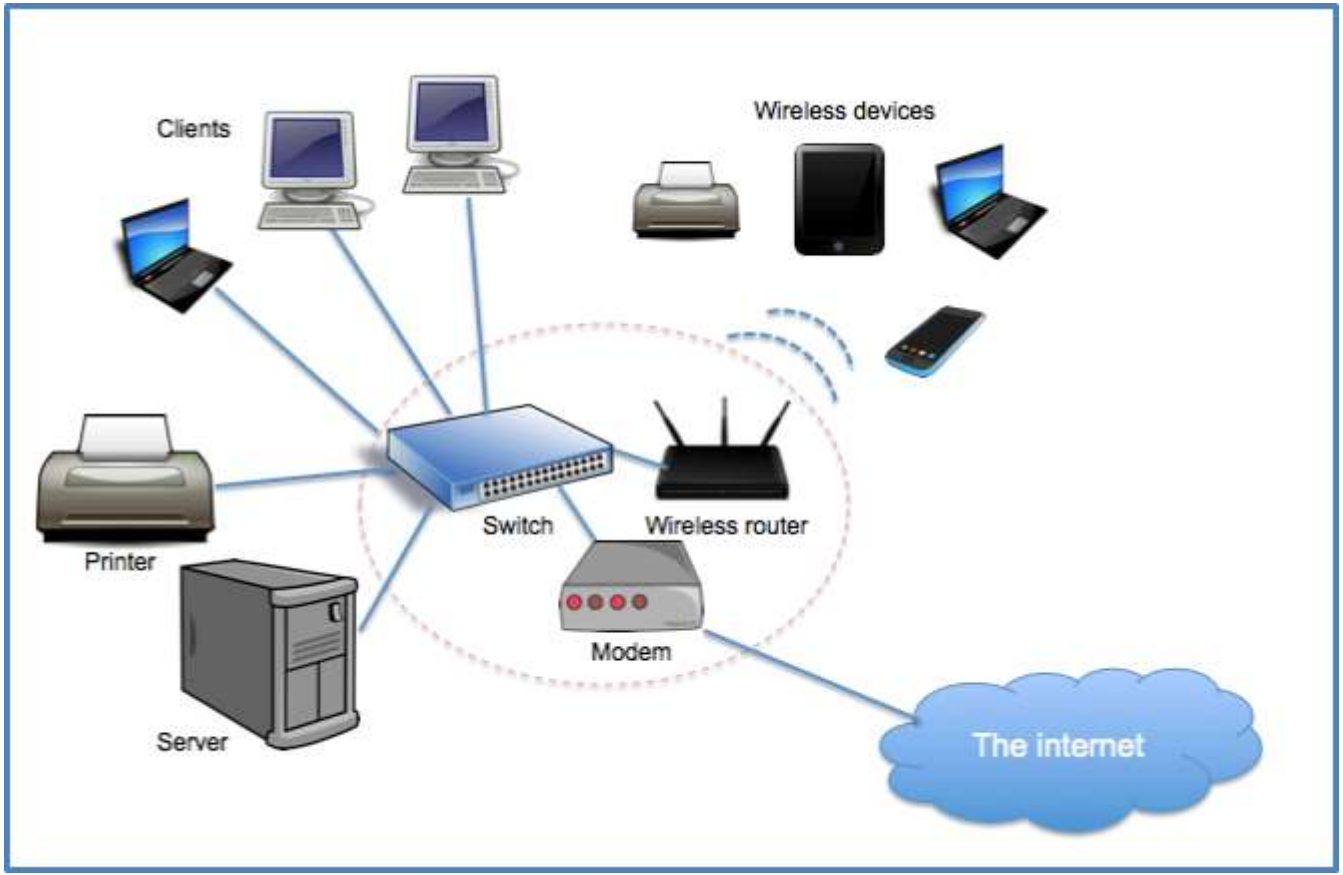
Computer Networks: MCA, I Year/II-Sem.

Outline

- What is a Network
- Internet
- Uses of computer Networks
- Data Communication System
- Data Flow

What is Network

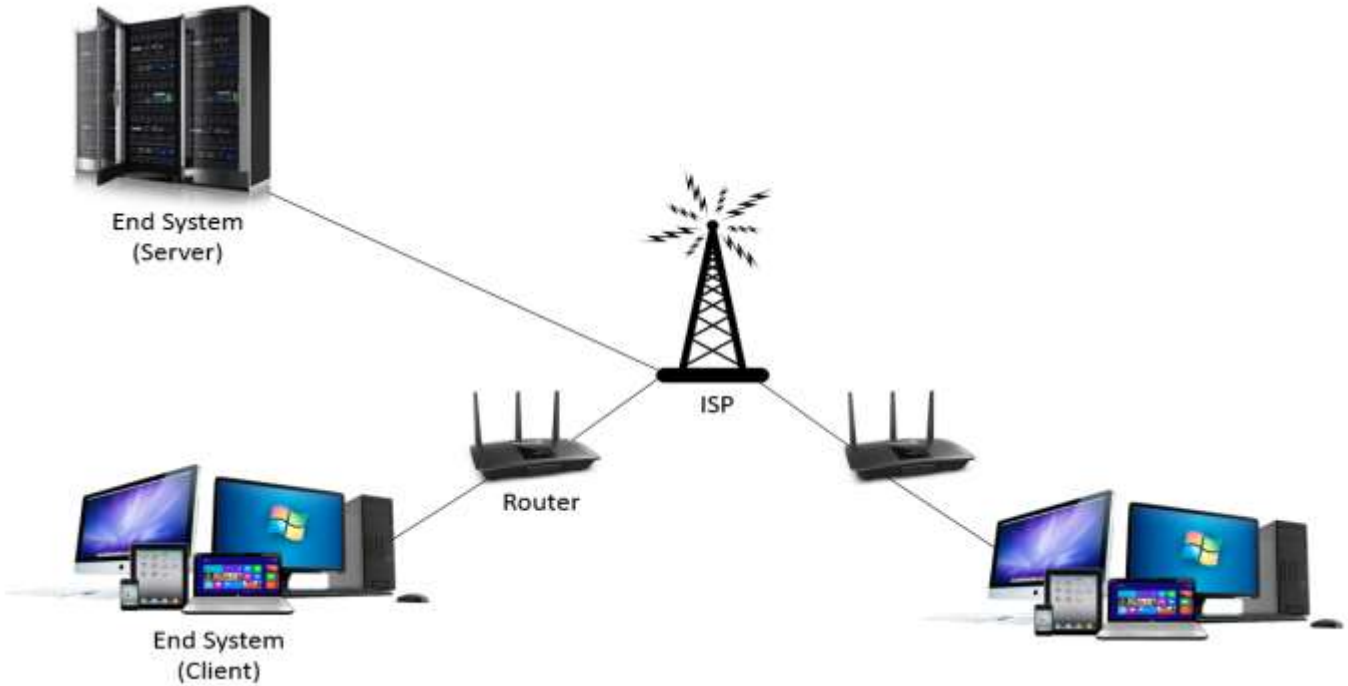
- A network is a set of devices (often referred to as nodes) connected by communication links
- A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network
- “Computer network” to mean a collection of autonomous computers interconnected by a single technology
- Two computers are said to be interconnected if they are able to exchange information


Clients
Wireless devices
Printer
Switch
Wireless router
Modem
Server
The internet

Introduction about Internet

• The Internet is a vast network that connects computers all over the world. Through the Internet, people can share information and communicate from anywhere with an Internet connection

• The Internet consists of technologies developed by different individuals and organizations. Important figures include Robert W. Taylor, who led the development of the ARPANET (an early prototype of the Internet), and Vinton Cerf and Robert Kahn, who developed the Transmission Control Protocol/Internet Protocol (TCP/IP) technologies


End System
(Server)
ISP
Router
End System
(Client)

Uses of Computer Networks

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

Data Communication System

1 Message:

The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2 Sender:

The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. Receiver:

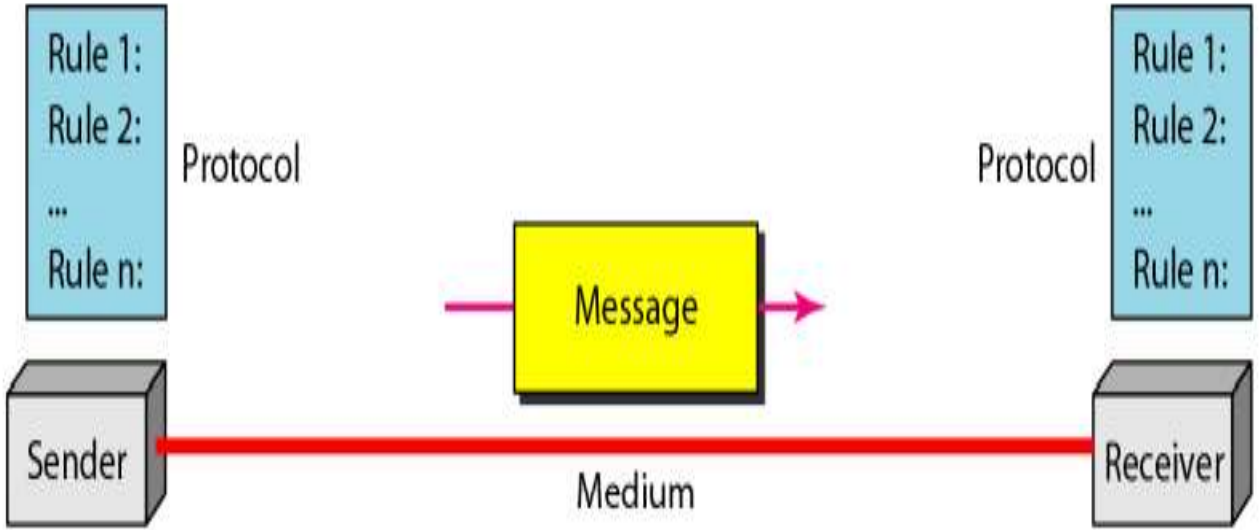
The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. Transmission medium:

The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

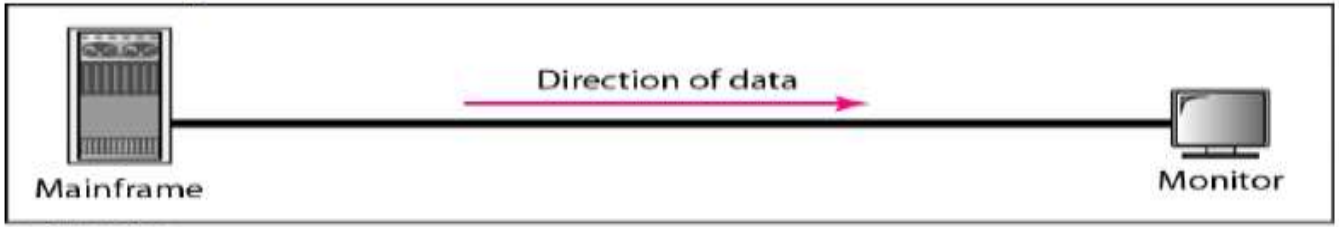
5. Protocol:

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

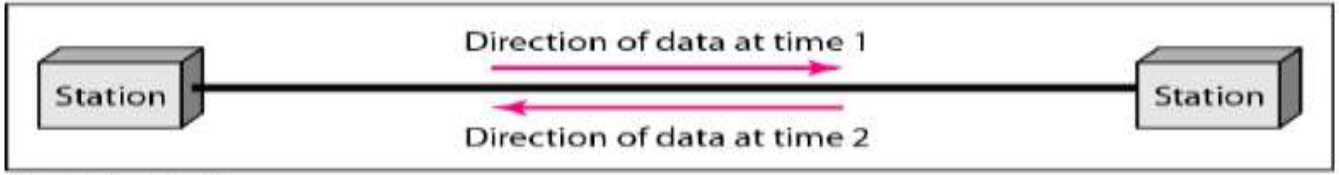

Rule 1:
Rule 2:
...
Rule n:
Protocol
Message
Protocol
Rule 1:
Rule 2:
...
Rule n:
Sender
Medium
Receiver

Data Flow

- Communication between two devices can be simplex, half-duplex, or full-duplex
- Simplex In simplex mode, the communication is unidirectional, as on a oneway street. Only one of the two devices on a link can transmit; the other can only receive (Figure a). Keyboards and traditional monitors are examples of simplex devices
- Half-Duplex In half-duplex mode, each station can both transmit and receive, but not at the same time
- When one device is sending, the other can only receive, and vice versa (Figure b) Walkie-talkies and CB (citizens band) radios are both halfduplex systems



a. Simplex



b. Half-duplex

c. Full-duplex

- Full-Duplex In full-duplex, both stations can transmit and receive simultaneously (Figure c).
- One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.
- The full-duplex mode is used when communication in both directions is required all the time

Computer Networks

Network Topologies

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Network Topologies

Computer Networks: MCA, I Year/II-Sem.

Outline

- What is a Topology
- Bus Topology
- Ring Topology
- Star Topology
- Mesh Topology
- Hybrid Topology

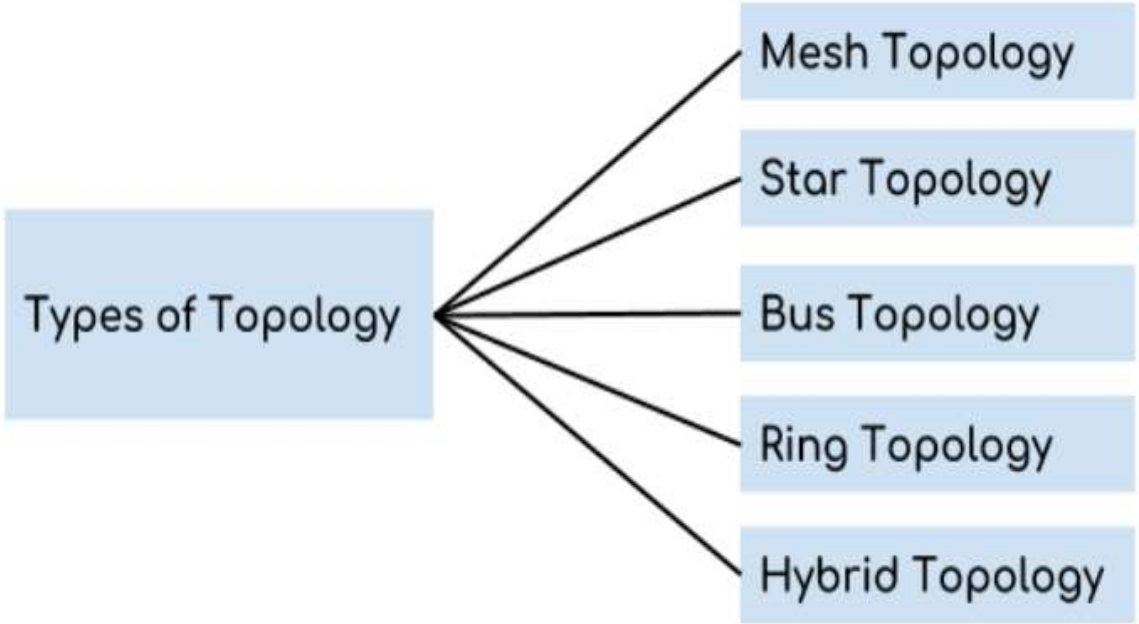
What is Topology

• The term physical topology refers to the way in which a network is laid out physically

• Two or more devices connect to a link; two or more links form a topology

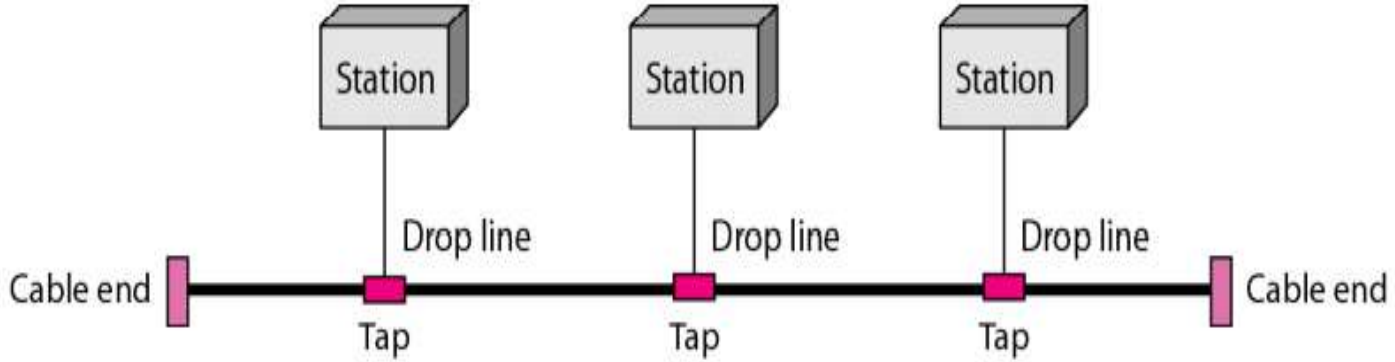
• The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another

• There are four basic topologies possible: mesh, star, bus, and ring


Types of Topology
Mesh Topology
Star Topology
Bus Topology
Ring Topology
Hybrid Topology

Bus Topology

• A line topology, a bus topology is a network setup in which each computer and network device are connected to a single cable or backbone



Advantages of bus topology

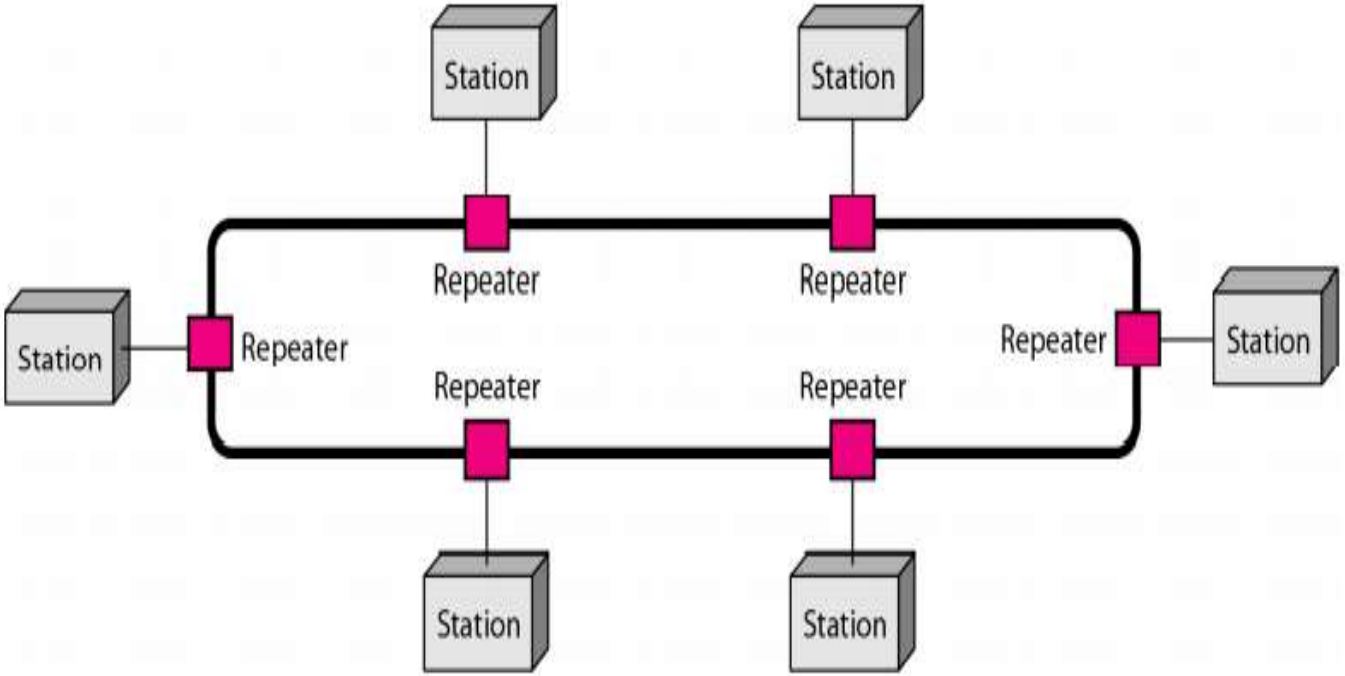
- It works well when you have a small network
- It's the easiest network topology for connecting computers or peripherals in a linear fashion
- It requires less cable length than a star topology

Disadvantages of bus topology

- It can be difficult to identify the problems if the whole network goes down
- It can be hard to troubleshoot individual device issues
- Bus topology is not great for large networks

Ring Topology

- A ring topology is a network configuration in which device connections create a circular data path
- In a ring network, packets of data travel from one device to the next until they reach their destination
- Most ring topologies allow packets to travel only in one direction, called a unidirectional ring network
- Others permit data to move in either direction, called bidirectional.


Station
Station
Repeater
Repeater
Station
Repeater
Repeater
Repeater
Repeater
Station
Station
Station

Advantages of Ring topology

- All data flows in one direction, reducing the chance of packet collisions.
- A network server is not needed to control network connectivity between each workstation
- Data can transfer between workstations at high speeds

Disadvantages of Ring topology

- The major disadvantage of a ring topology is that if any individual connection in the ring is broken, the entire network is affected

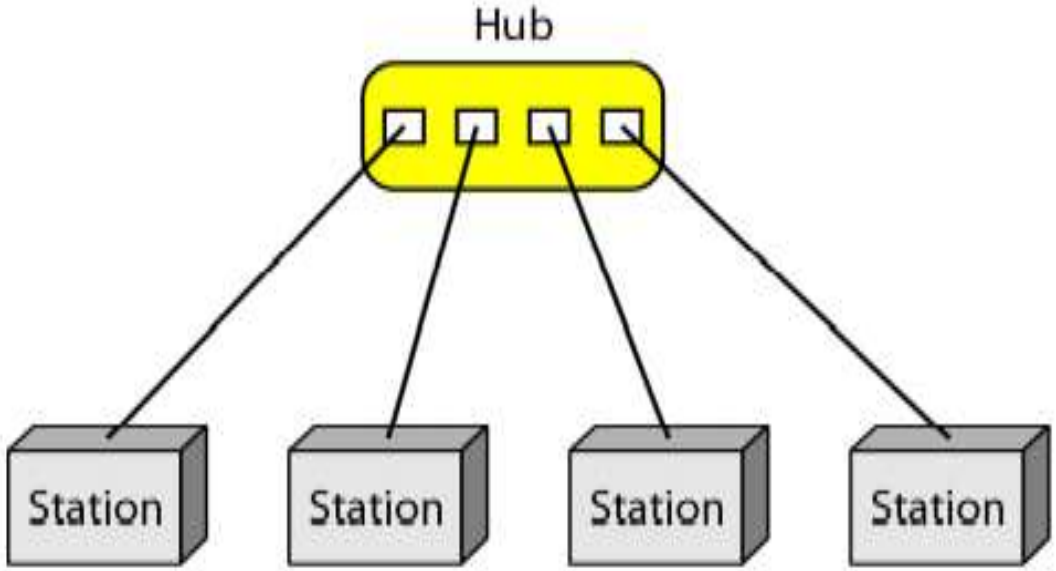
Star Topology

• A star network, star topology is one of the most common network setups

• In this configuration, every node connects to a central network device, like a hub, switch, or computer (Server)

• The central network device acts as a server and the peripheral devices act as clients

• Depending on the type of network card used in each computer of the star topology, a coaxial cable or a RJ-45 network cable is used to connect computers together


Hub
Station
Station
Station
Station

Advantages of Star topology

• Centralized management of the network, through the use of the central computer, hub, or switch

• Easy to add another computer to the network

• If one computer on the network fails, the rest of the network continues to function normally

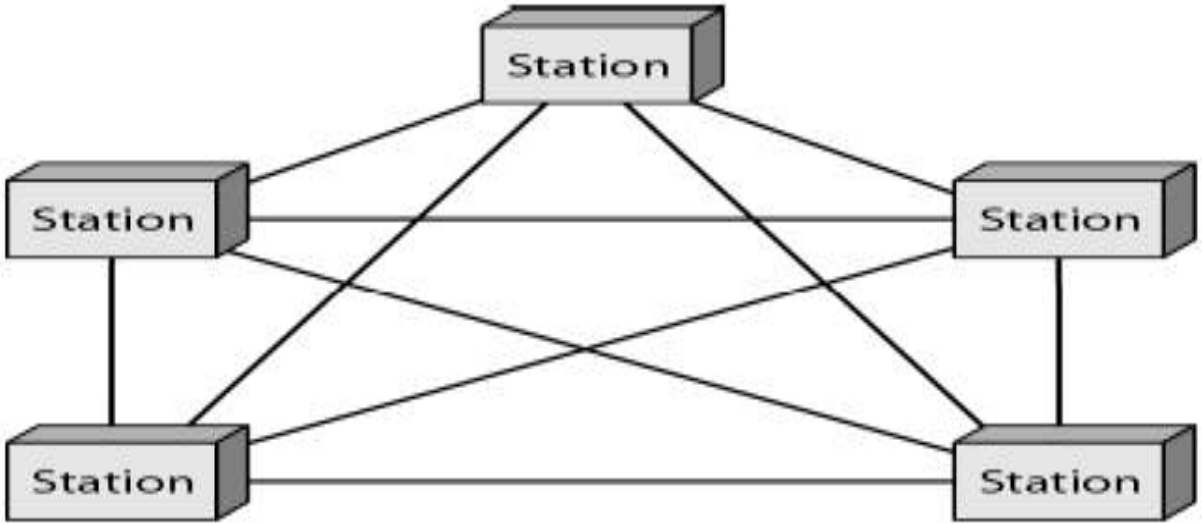
Disadvantages of Star topology

• Can have a higher cost to implement, especially when using a switch or router as the central network device

• If the central computer, hub, or switch fails, the entire network goes down and all computers are disconnected from the network

Mesh Topology

- A mesh topology is the one where every node is connected to every other node in the network.
- A mesh topology can be a full mesh topology or a partially connected mesh topology.
- In a full mesh topology, every computer in the network has a connection to each of the other computers in that network.
- In a partially connected mesh topology, at least two of the computers in the network have connections to multiple other computers in that network.
- It is an inexpensive way to implement redundancy in a network. In the event that one of the primary computers or connections in the network fails, the rest of the network continues to operate normally.


Station
Station
Station
Station
Station

Advantages of bus topology

• Can handle high amounts of traffic, because multiple devices can transmit data simultaneously

• A failure of one device does not cause a break in the network or transmission of data

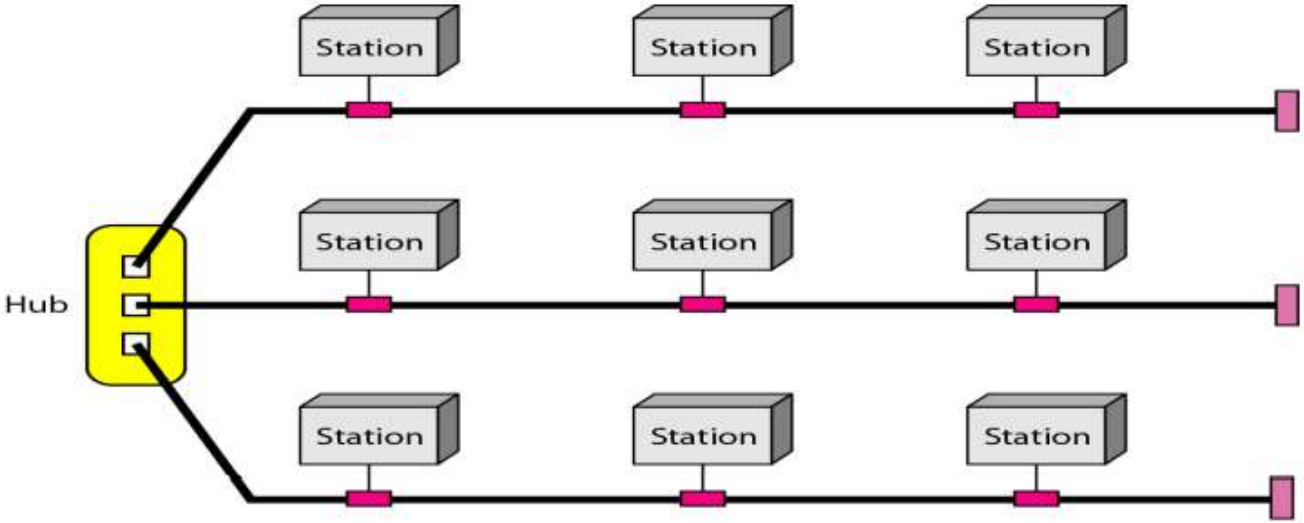
Disadvantages of bus topology

• The cost to implement is higher than other network topologies, making it a less desirable option

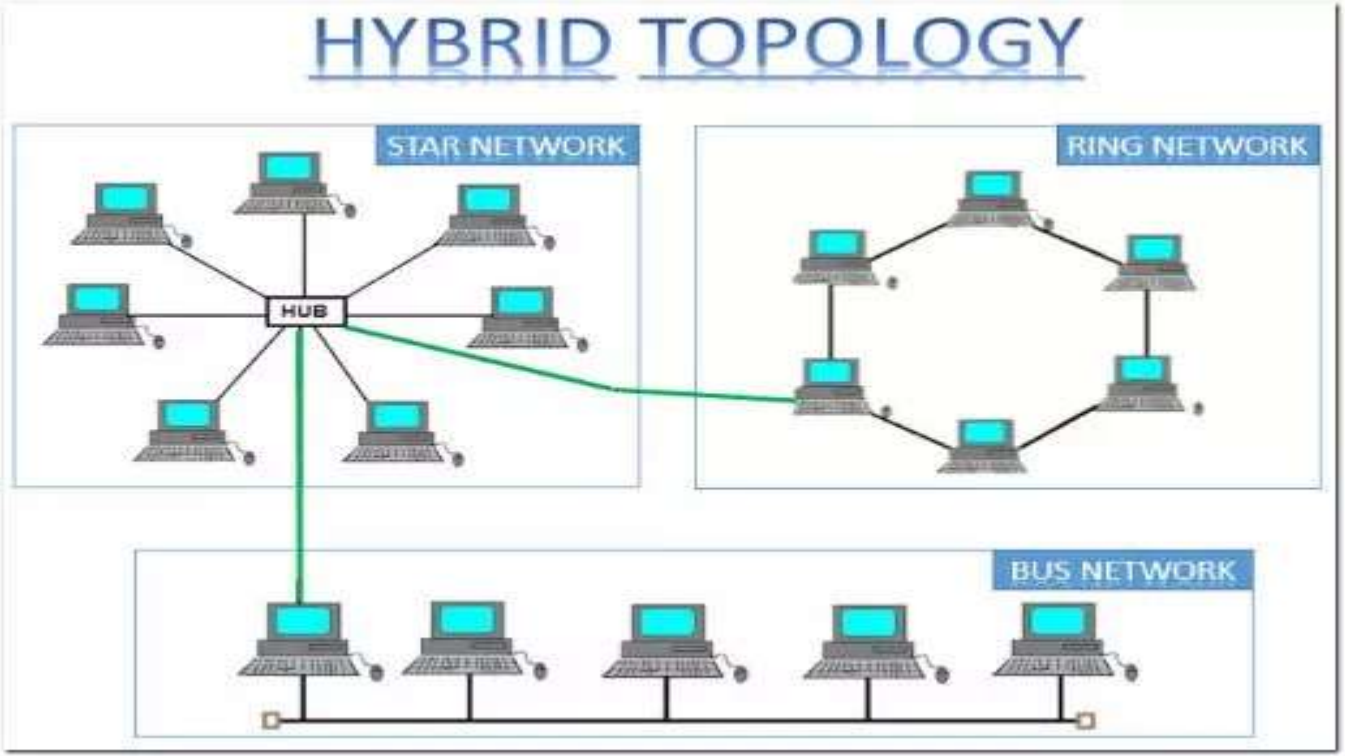
• Building and maintaining the topology is difficult and time consuming

Hybrid Topology

Hybrid Topology A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology



HYBRID TOPOLOGY



Computer Networks

Types of Networks
and
Protocol Layering Scenario

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Network Topologies

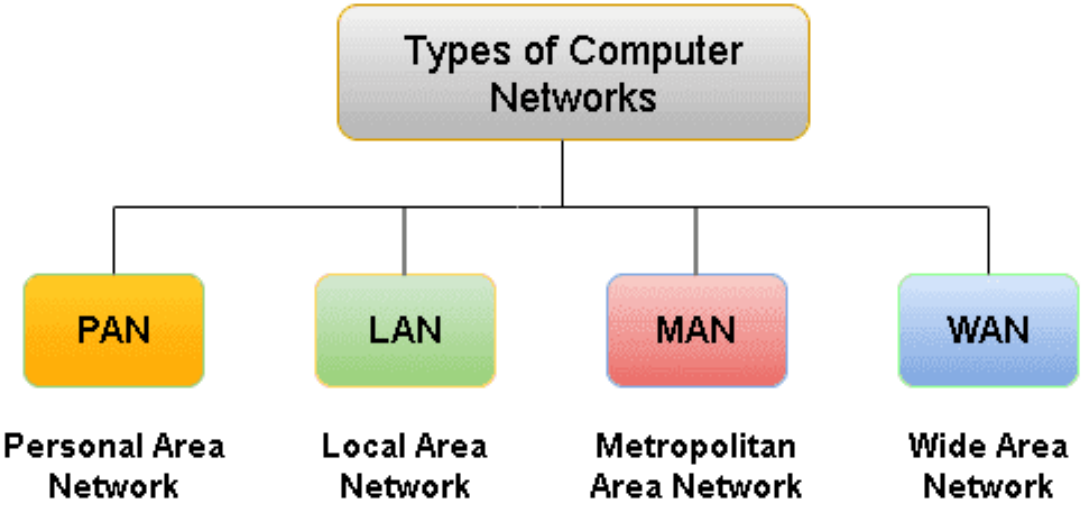
Computer Networks: MCA, I Year/II-Sem.

Outline

- Types of Networks
- LAN
- MAN
- WAN
- Protocol
- Single Layer Protocol
- Three Layer Protocol

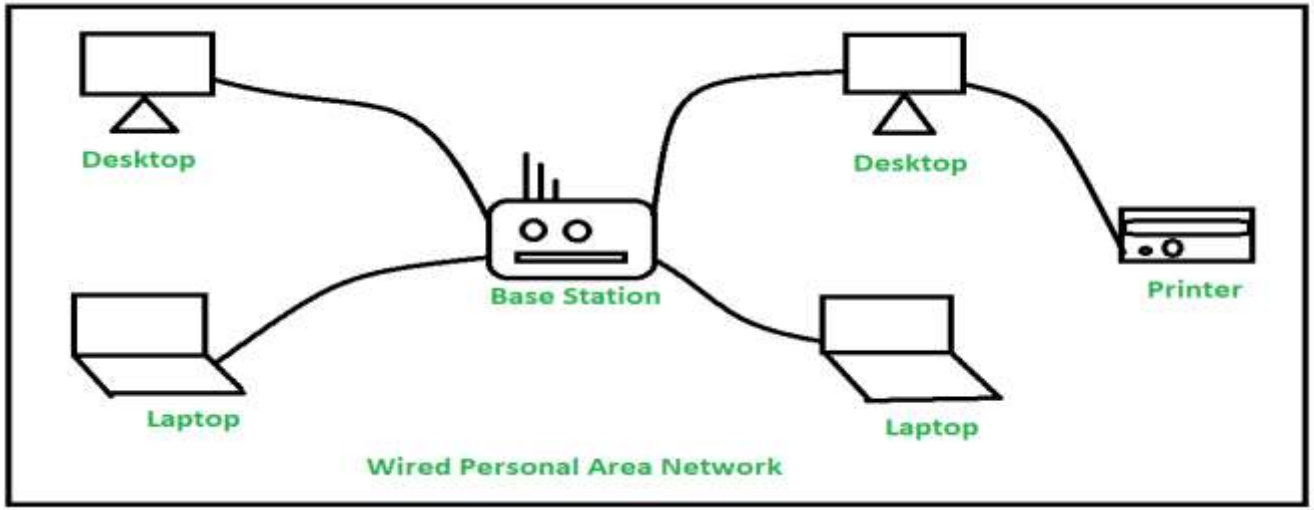
Network Types

- The types of network are classified based upon the size, the area it covers and its physical architecture
- The three primary network categories are LAN, WAN and MAN
- Each network differs in their characteristics such as distance, transmission speed, cables and cost


Types of Computer Networks
PAN
LAN
MAN
WAN
Personal Area Network
Local Area Network
Metropolitan Area Network
Wide Area Network

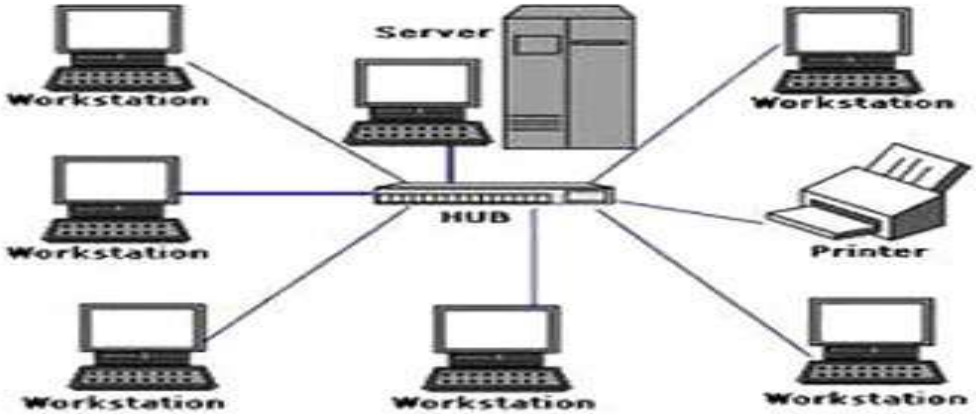
PAN

• PAN (Personal Area Network) Network organized by the individual user for its personal use



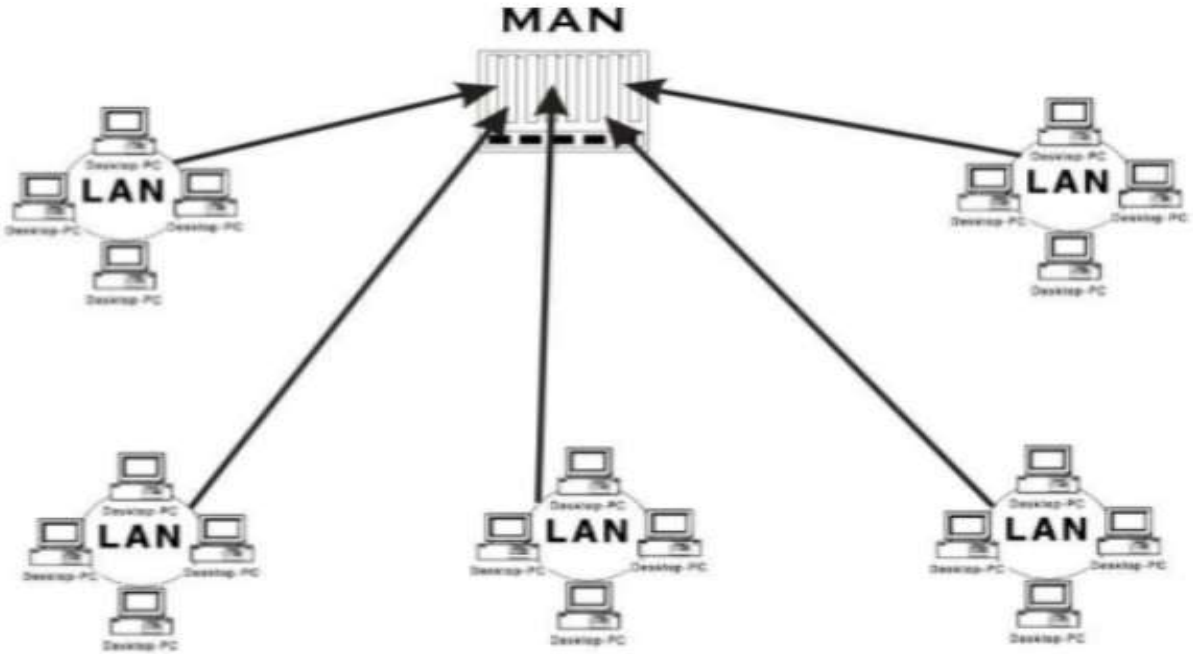
LAN

- Group of interconnected computers within a small area. (room, building, campus)
- Two or more pc's can from a LAN to share files, folders, printers, applications and other devices.
- Coaxial or CAT 5 cables are normally used for connections.
- Due to short distances, errors and noise are minimum.
- Data transfer rate is 10 to 100 mbps.
- Example: A computer lab in a College or School


Server
Workstation
Workstation
Workstation
HUB
Workstation
Workstation
Printer
Workstation

MAN

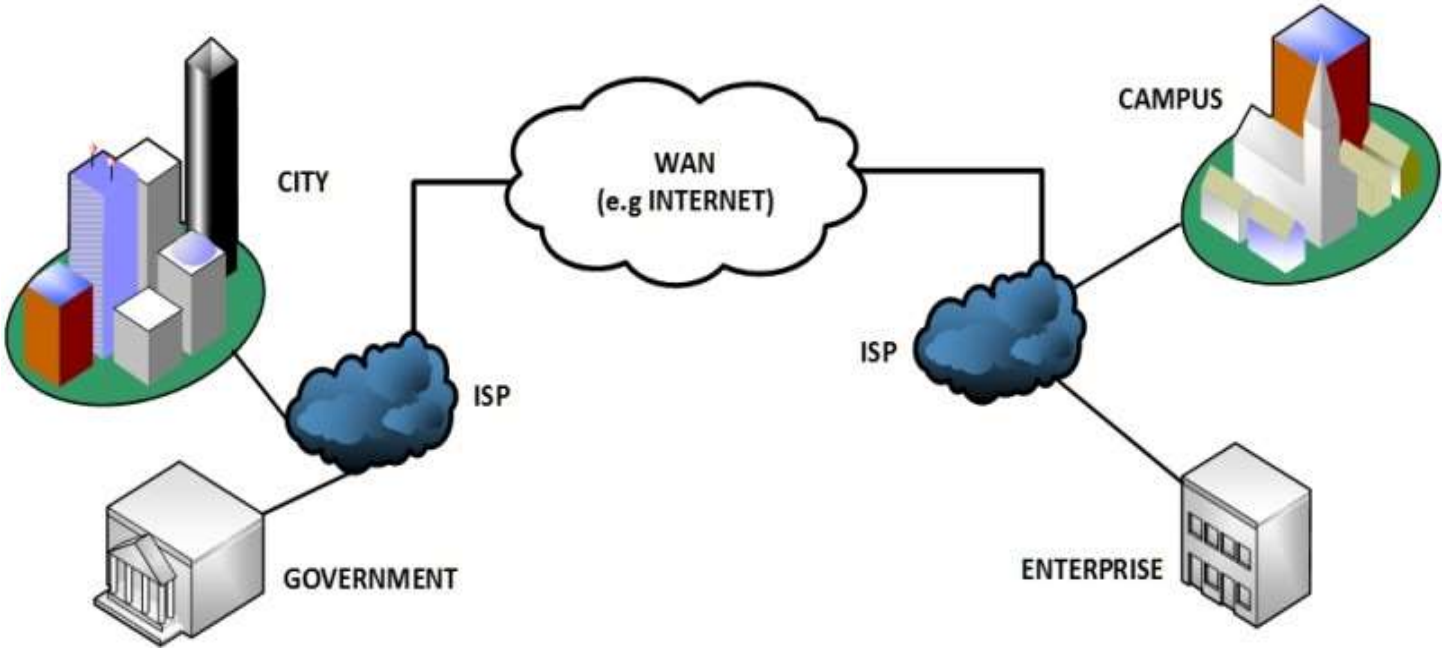
- Design to extend over a large area. Connecting number of LAN's to form larger network, so that resources can be shared
- Networks can be up to 5 to 50 km
- Owned by organization or individual
- Data transfer rate is low compare to LAN
- Example: Organization with different branches located in the city


MAN
LAN
LAN
LAN
LAN
LAN

WAN

- Are country and worldwide network
- Contains multiple LAN's and MAN's
- Distinguished in terms of geographical range
- Uses satellites and microwave relays
- Data transfer rate depends upon the ISP provider and varies over the location
- Best example is the internet

WIDE AREA NETWORK (WAN)



Protocol Layering

• A protocol the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively

• When communication is simple, we may need only one simple protocol

• When the communication is complex, we need a protocol at each layer, or protocol layering

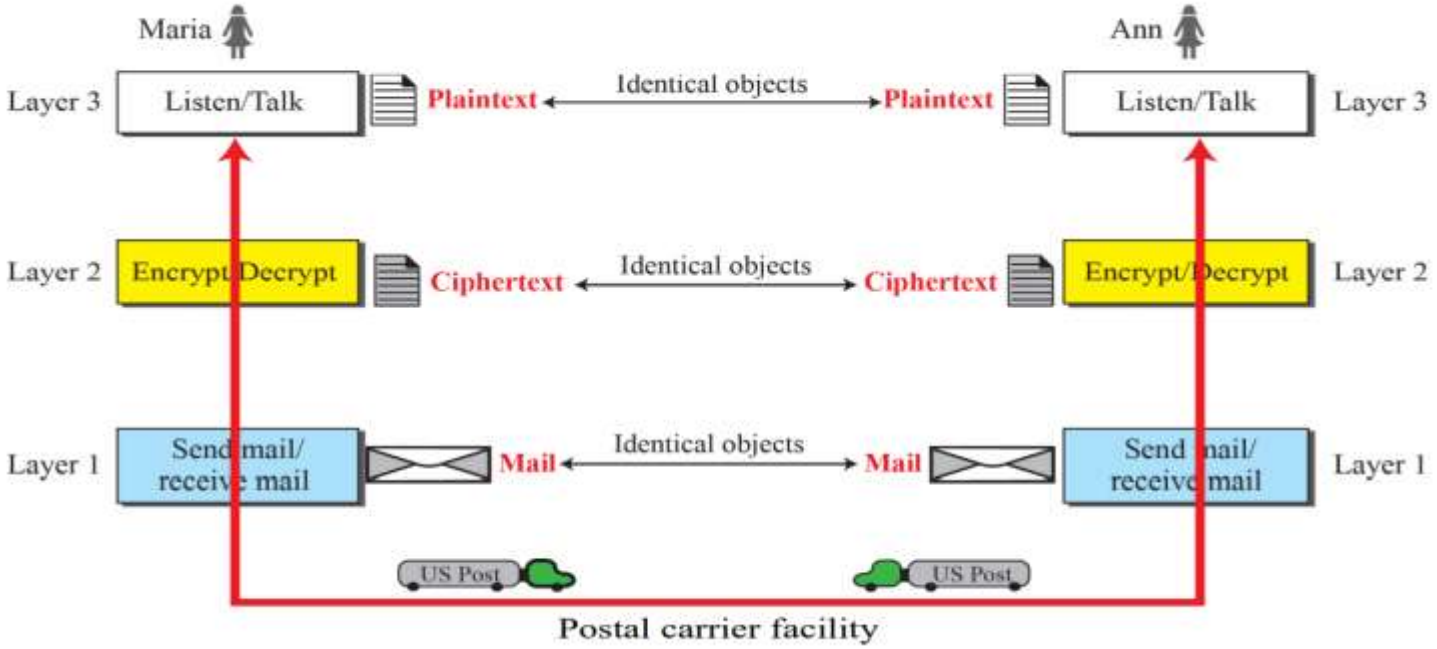
Two simple scenarios to better understand the need for protocol layering

1) communication is so simple that it can occur in only one layer

2) the communication between Maria and Ann takes place in three layers

Single Layer-Protocol

Three Layer-Protocol



• The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction.

• The second principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical

• We can think about logical connection between each layer layer-to-layer communication Maria and Ann can think that there is a logical (imaginary) connection at each layer through which they can send the object created from that layer

Computer Networks

The OSI Model

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : The OSI Model

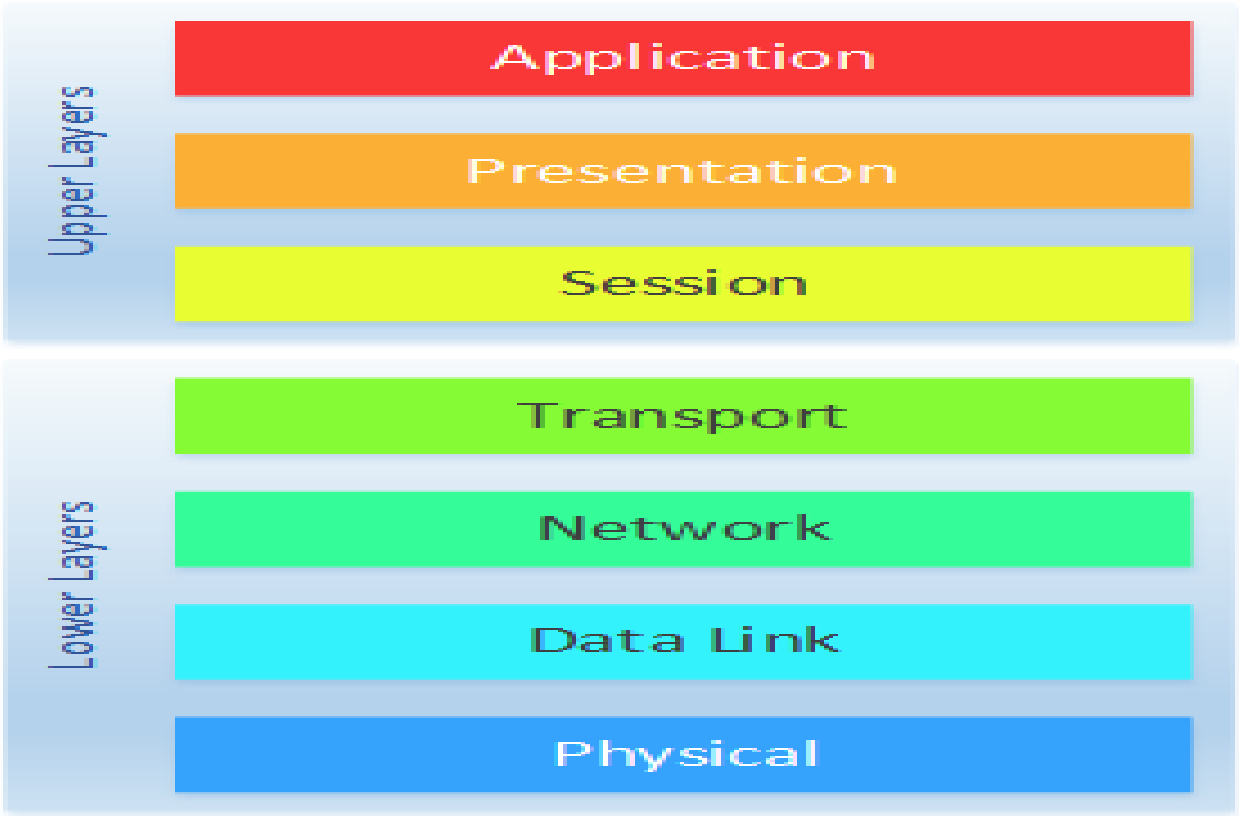
Computer Networks: MCA, I Year/II-Sem.

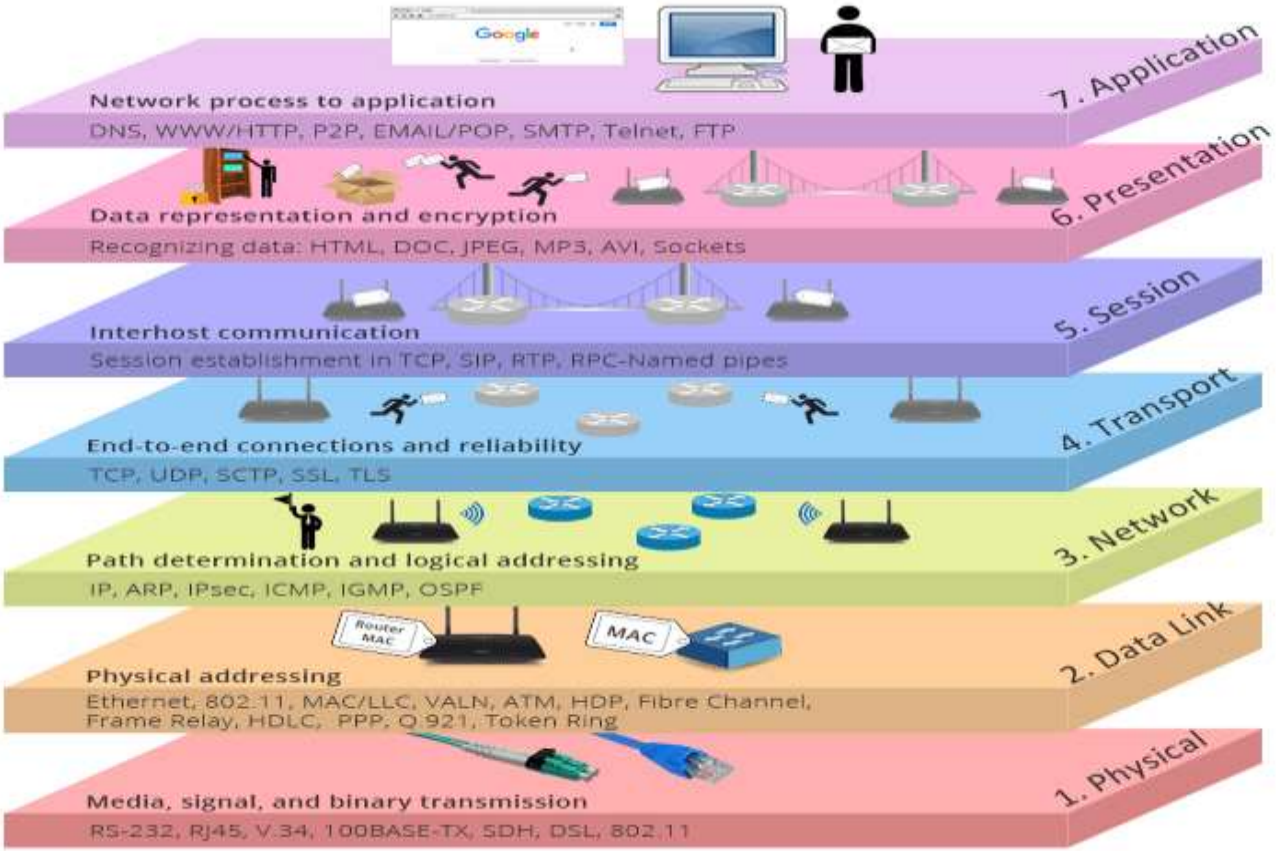
Outline

- Introduction of OSI
- OSI Model Representation
- Data referred in OSI Model
- OSI Layers
- Interaction between the layers in OSI Model
- Data exchange in OSI Model

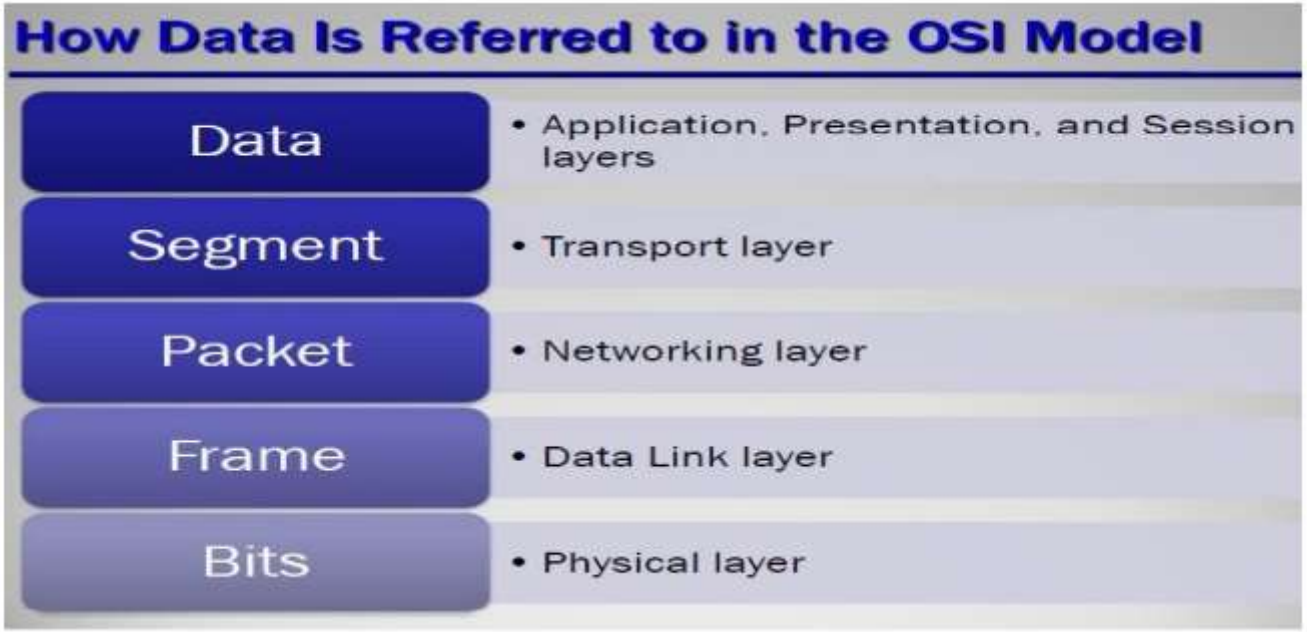
OSI

- OSI stands for Open Systems Interconnection
- Created by International Standards Organization (ISO)
- Was created as a framework and reference model to explain how different networking technologies work together and interact
- Each layer has specific functions it is responsible for
- All layers work together in the correct order to move data around a network


Upper Layers
Application
Presentation
Session
Lower Layers
Transport
Network
Data Link
Physical



Data Referred in OSI Model



Physical Layer

- Deals with all aspects of physically moving data from one computer to the next
- Converts data from the upper layers into 1s and 0s for transmission over media
- Defines how data is encoded onto the media to transmit the data
- Defined on this layer: Cable standards, wireless standards, and fiber optic standards.
- Copper wiring, fiber optic cable, radio frequencies, anything that can be used to transmit data is defined on the Physical layer of the OSI Model
- Device example: Hub

Data Link Layer

- Data Link Layer responsible for moving frames from node to node or computer to computer
- Can move frames from one adjacent computer to another, cannot move frames across routers
- Requires MAC address or physical address
- Protocols defined include Ethernet Protocol and Point-to-Point Protocol (PPP)
- Two sub-layers: Logical Link Control (LLC) and the Media Access Control (MAC)

Network Layer

- Responsible for moving packets (data) from one end of the network to the other, called end-to-end communications
- Requires logical addresses such as IP addresses
- Device example: Router
- Routing is the ability of various network devices and their related software to move data packets from source to destination

Transport Layer

- Takes data from higher levels of OSI Model and breaks it into segments that can be sent to lower-level layers for data transmission
- Conversely, reassembles data segments into data that higher-level protocols and applications can use
- Also puts segments in correct order (called sequencing) so they can be reassembled in correct order at destination

• Concerned with the reliability of the transport of sent data

• May use a connection-oriented protocol such as TCP to ensure destination received segments

• May use a connectionless protocol such as UDP to send segments without assurance of delivery Uses port addressing

Session Layer

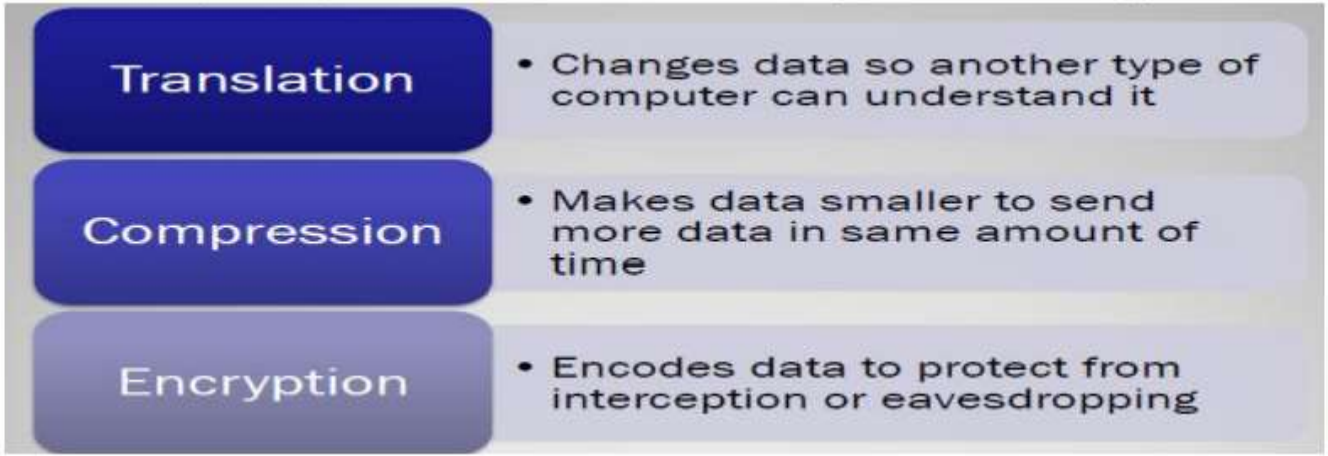
- Responsible for managing the dialog between networked devices
- Establishes, manages, and terminates connections
- Provides duplex, half-duplex, or simplex communications between devices
- Provides procedures for establishing checkpoints, adjournment, termination, and restart or recovery procedures

Presentation Layer

Concerned with how data is presented to the network

Handles three primary tasks:

–Translation , –Compression , –Encryption

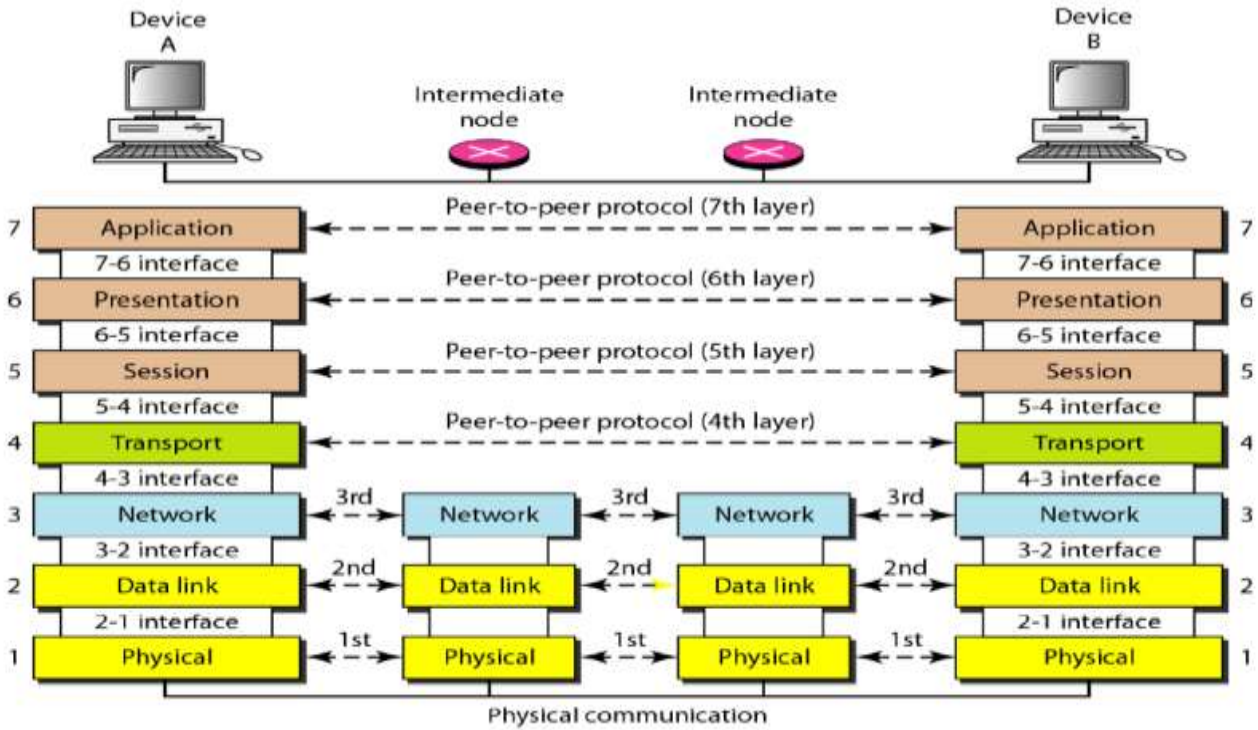


Application Layer

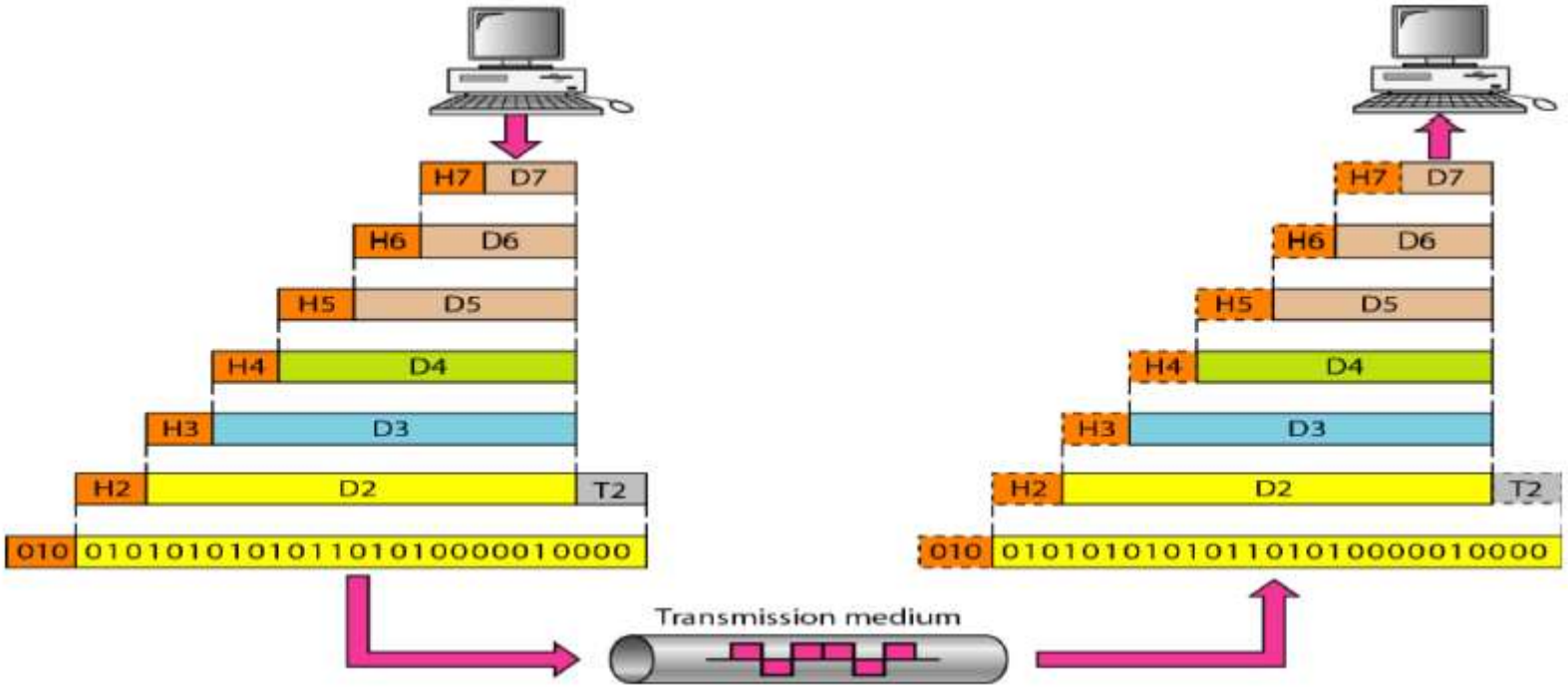
• Contains all services or protocols needed by application software or operating system to communicate on the network

• Examples o –Firefox web browser uses HTTP (Hyper-Text Transport Protocol) –E-mail program may use POP3 (Post Office Protocol version 3) to read e-mails and SMTP (Simple Mail Transport Protocol) to send e-mails

Interaction Between the layers in OSI Model



Exchanging data in OSI Model



Computer Networks

TCP/IP

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : TCP/IP

Computer Networks: MCA, I Year/II-Sem.

Outline

- Introduction of TCP/IP
- TCP/IP Network Model
- TCP/IP Layers
- TCP/IP Protocol Suit
- Comparing TCP/IP with OSI Reference Model

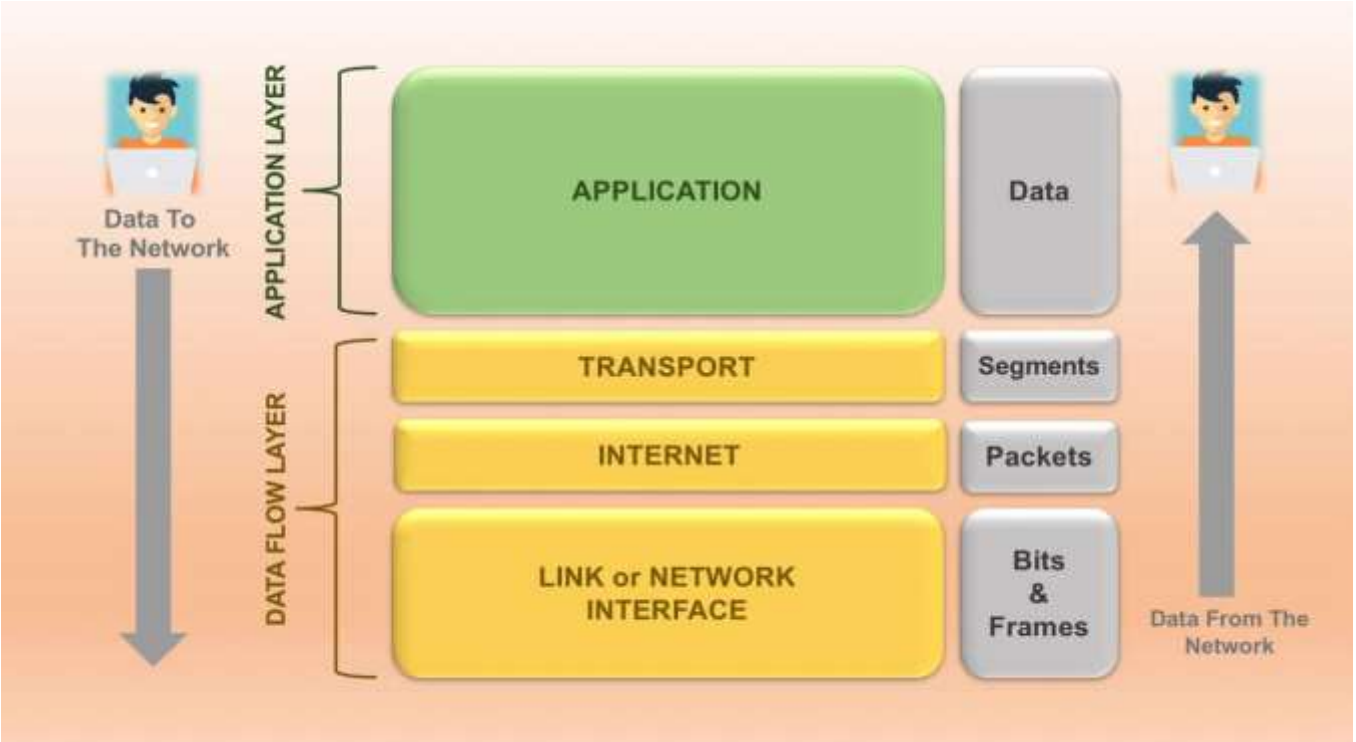
TCP/IP

•TCP/IP Reference Model is a four-layered suite of communication protocols

• It is developed by ARPANET (Advanced Research Project Agency Network)

• It is named after the two main protocols that are used in the model, namely, TCP and IP

•TCP stands for Transmission Control Protocol and IP stands for Internet Protocol


Data To
The Network
APPLICATION LAYER
DATA FLOW LAYER
APPLICATION
TRANSPORT
INTERNET
LINK or NETWORK
INTERFACE
Data
Segments
Packets
Bits
&
Frames
Data From The
Network

Application Layer

Transport Layer

Internet Layer

Network Access Layer

Application Layer

• Application layer protocols define the rules when implementing specific network applications

• Rely on the underlying layers to provide accurate and efficient data delivery

• Typical protocols: o FTP – File Transfer Protocol

• For file transfer o Telnet – Remote terminal protocol

• For remote login on any other computer on the network o SMTP – Simple Mail Transfer Protocol

• For mail transfer o HTTP – Hypertext Transfer Protocol

Transport Layer

TCP is a connection-oriented protocol

Does not mean it has a physical connection between sender and receiver

TCP provides the function to allow a connection virtually exists – also called virtual circuit

UDP provides the functions:

Dividing a chunk of data into segments

Reassembly segments into the original chunk

Provide further the functions such as reordering and data resend

Offering a reliable byte-stream delivery service

Functions the same as the Transport layer in OSI

Internet Layer

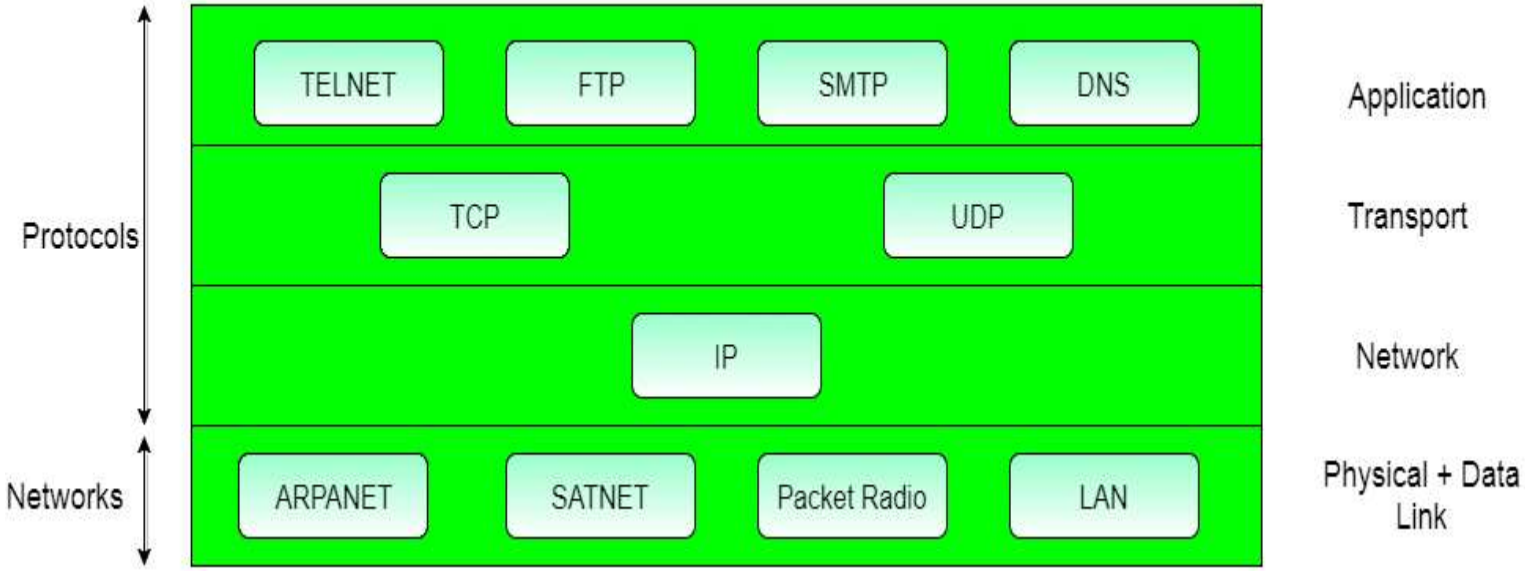
• The network layer, also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries

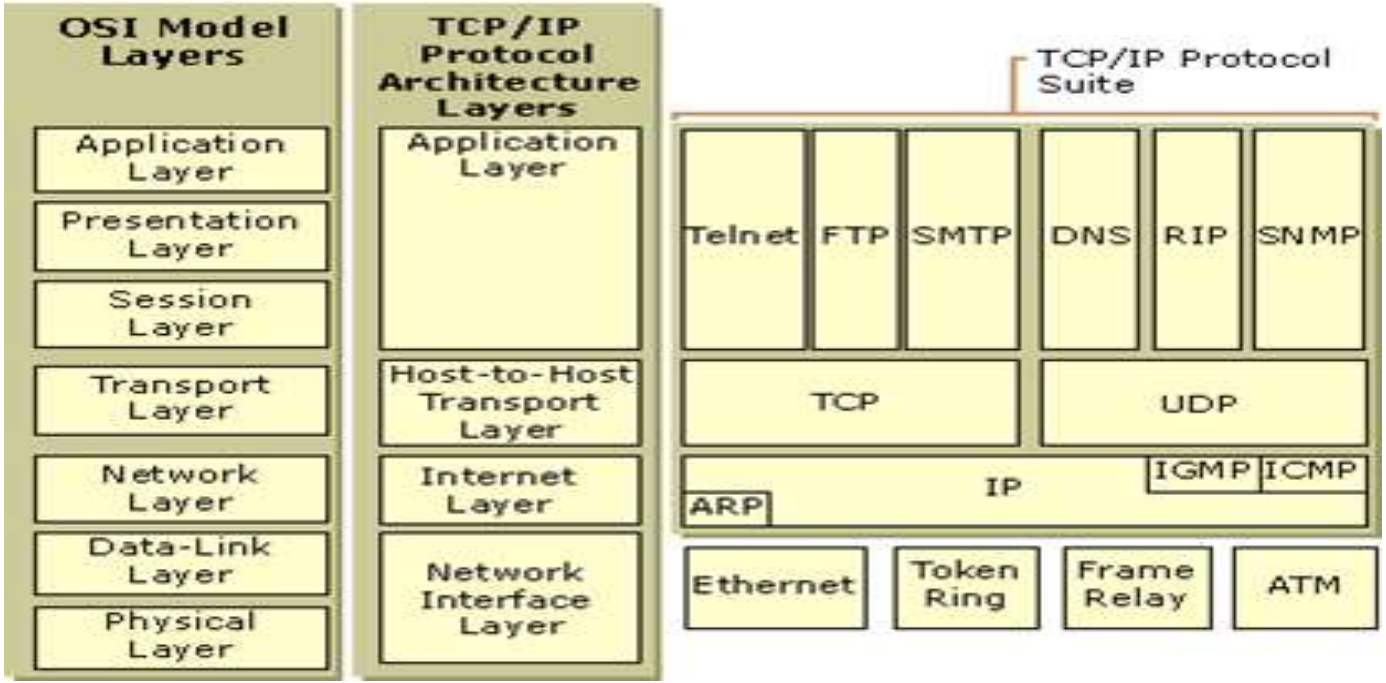
• The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting

Network Access Layer = PL+ DLL

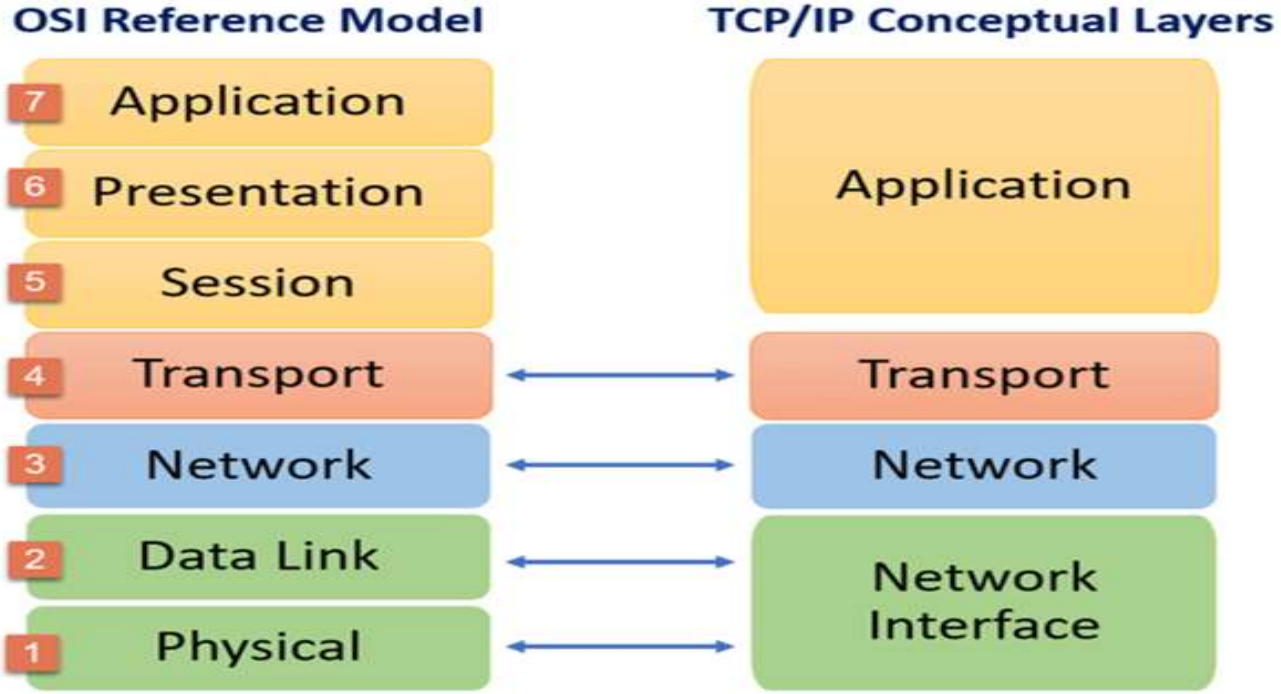
- The Host-to-network layer is the lowest layer of the TCP/IP reference model
- It combines the link layer and the physical layer of the ISO/OSI model
- At this layer, data is transferred between adjacent network nodes in a WAN or between nodes on the same LAN

TCP/IP Protocol Suite




OSI Model Layers
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data-Link Layer
Physical Layer
TCP/IP Protocol Architecture Layers
Application Layer
Host-to-Host Transport Layer
Internet Layer
Network Interface Layer
TCP/IP Protocol Suite
Telnet
FTP
SMTP
DNS
RIP
SNMP
TCP
UDP
IP
IGMP
ICMP
ARP
Ethernet
Token Ring
Frame Relay
ATM

Comparing TCP/IP with OSI



Key Differences

OSI Model	TCP/IP Model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI layers have seven layers.	TCP/IP has four layers.

In the OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are a part of the OSI model.	There is no session and presentation layer in the TCP model.
It is defined after the advent of the Internet.	It is defined before the advent of the internet.
The minimum size of the OSI header is 5 bytes.	The minimum header size is 20 bytes.

Computer Networks

Transmission Medium

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Transmission Medium

Computer Networks: MCA, I Year/II-Sem.

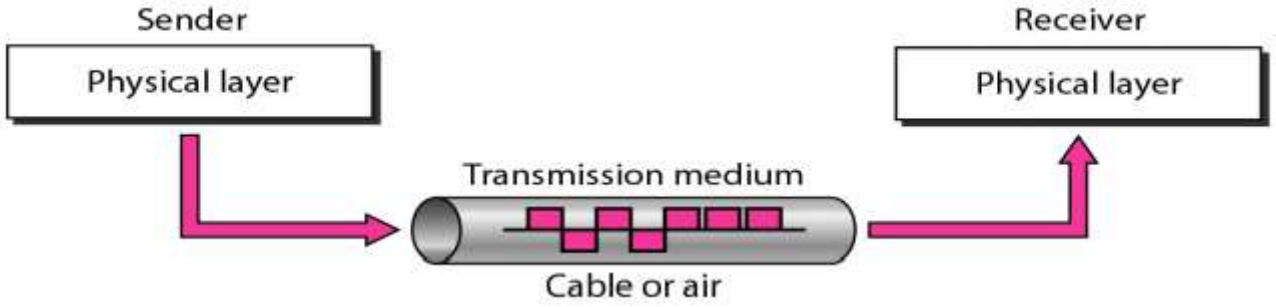
Outline

- Introduction to Transmission Medium
- Classification of Transmission Medium
- Guided Medium
- Un-Guided Medium

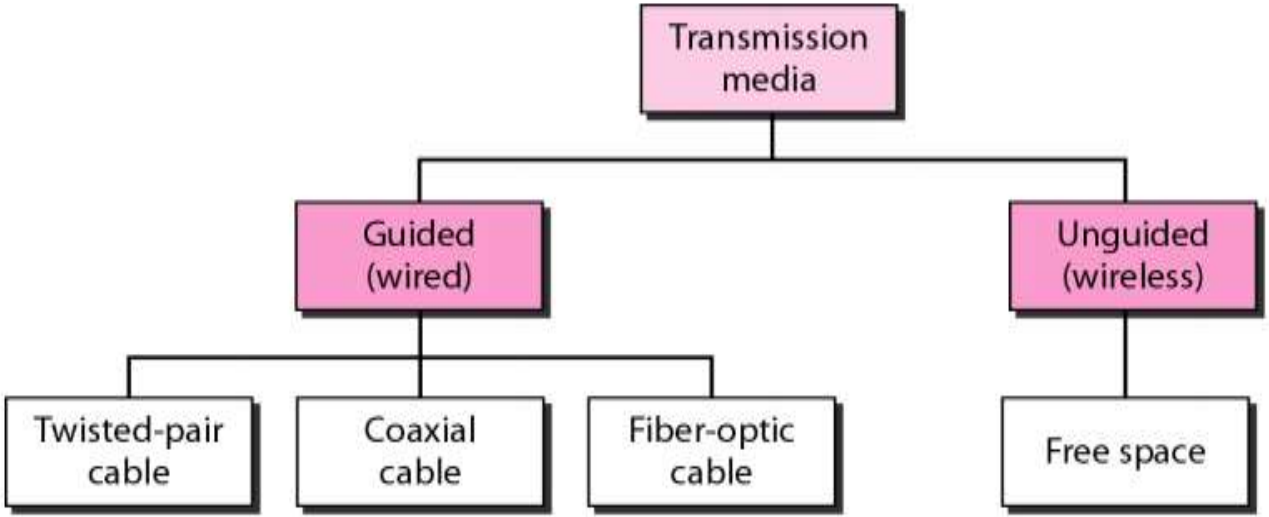
Transmission Medium

• In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver

• It is the channel through which data is sent from one place to another



Classification



Guided Media

Guided media, which are those that provide a medium from one device to another, include

- Twisted-pair cable
- Coaxial cable
- Fiber-optic cable

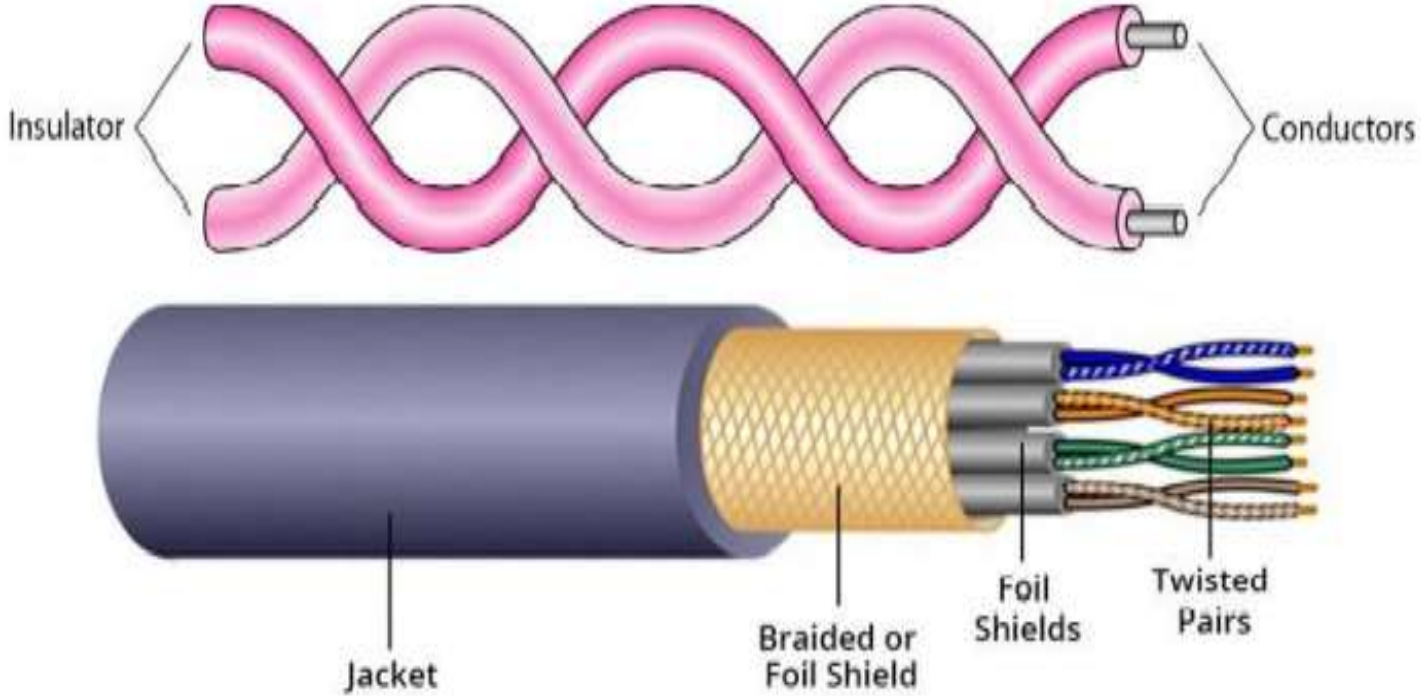
Twisted-Pair Cables

• A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.

• One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference

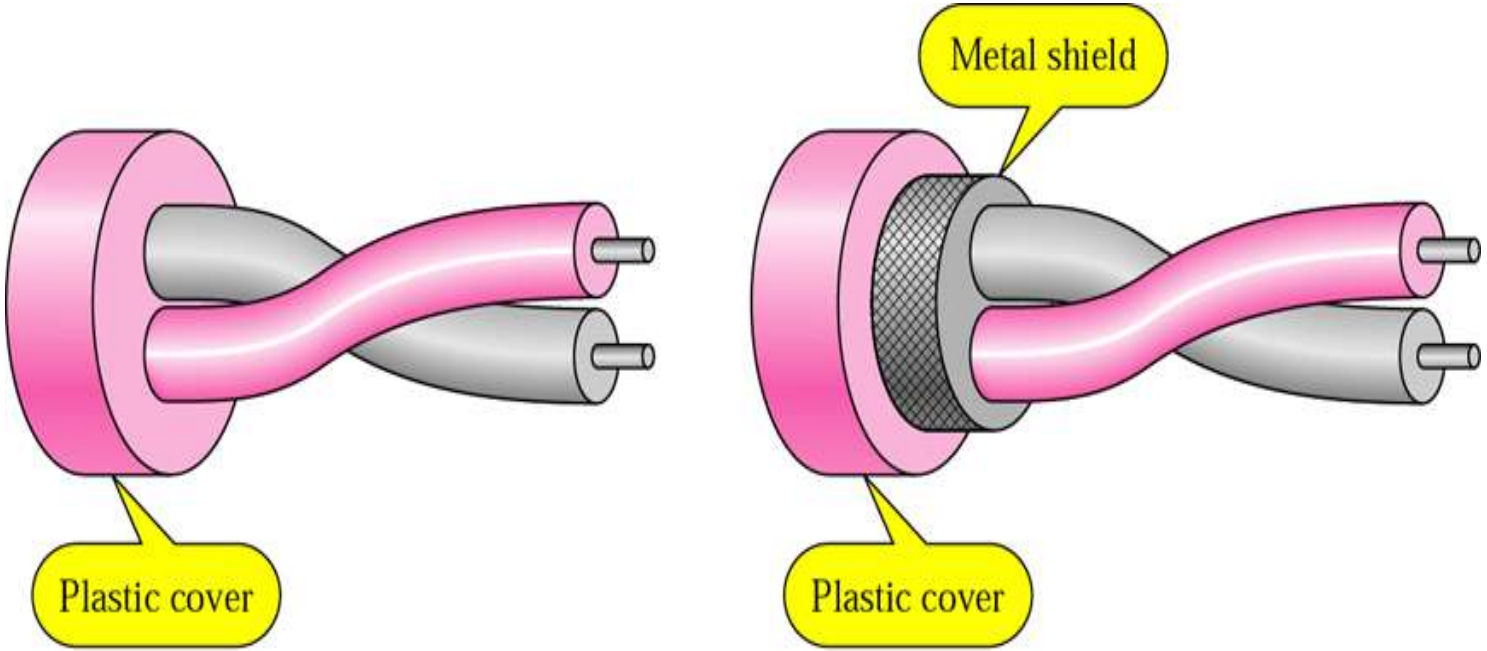
• Twisted-pair cables are used in telephone lines to provide voice and data channels.

• Local-area networks, such as l0Base-T and l00Base-T, also use twisted-pair cables.


Insulator
Conductors
Jacket
Braided or
Foil Shield
Foil
Shields
Twisted
Pairs

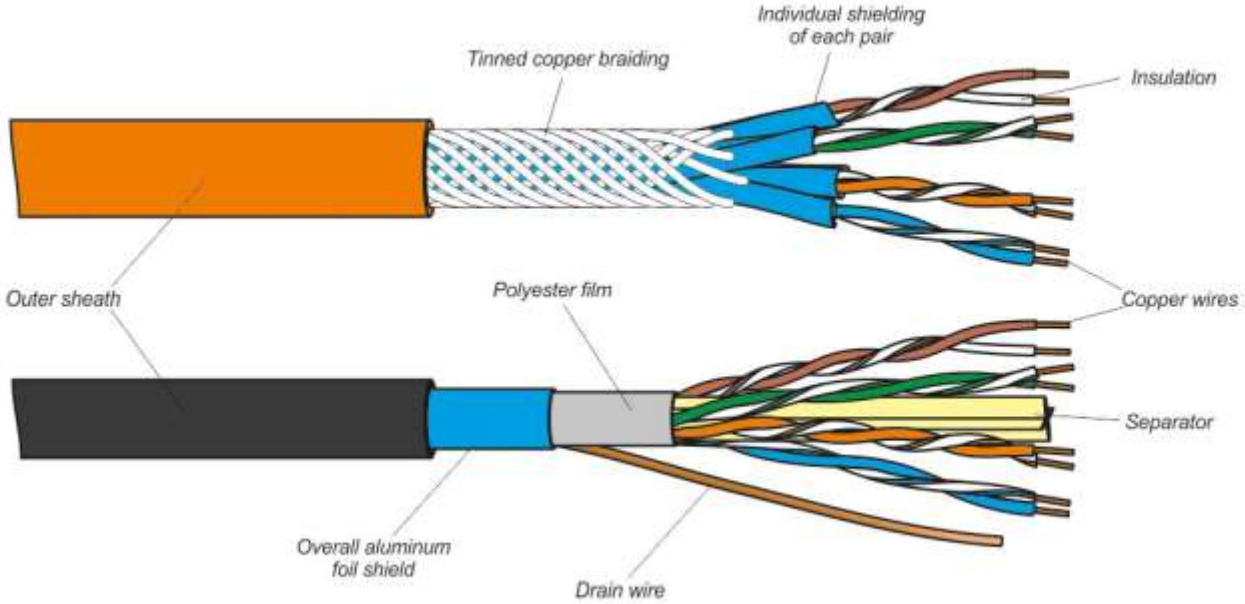
Shield and Un-Shield Twisted-Pair

- The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP)
- STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors
- Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive



a. UTP

b. STP


Individual shielding
of each pair
Tinned copper braiding
Insulation
Outer sheath
Polyester film
Copper wires
Separator
Overall aluminum
foil shield
Drain wire

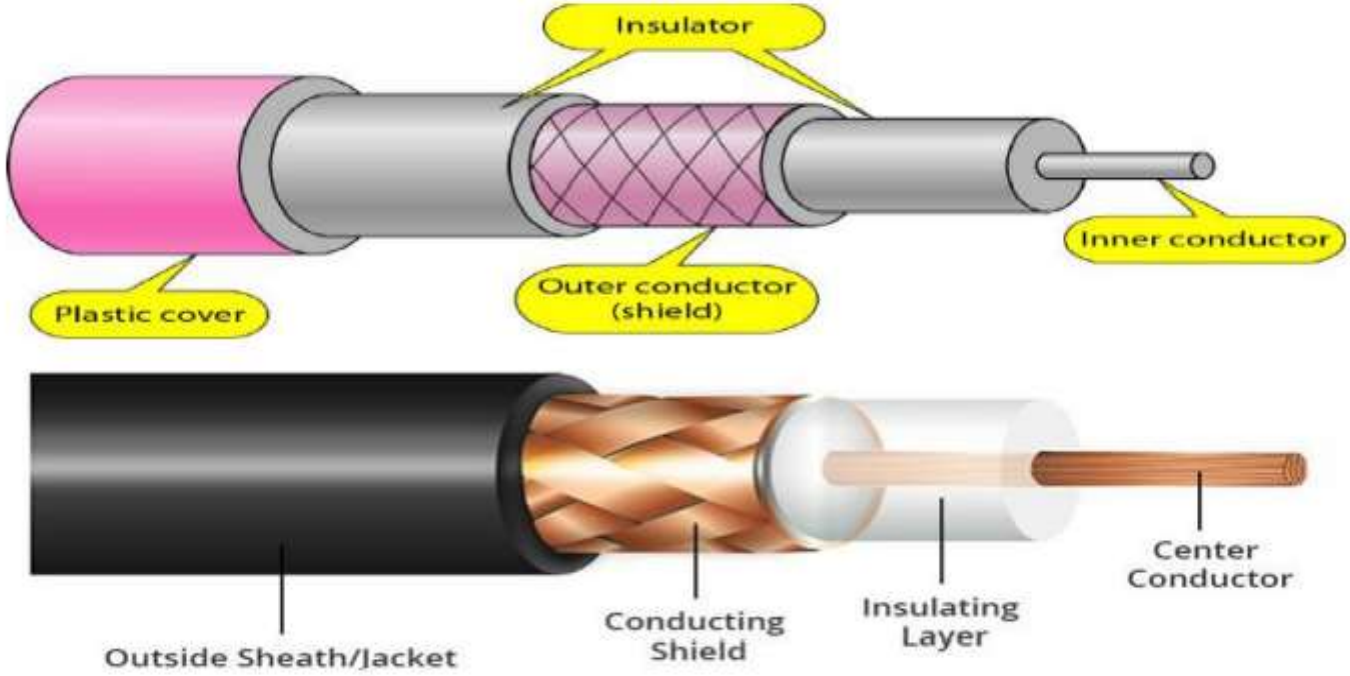
Coaxial Cable

• Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable.

• Coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.

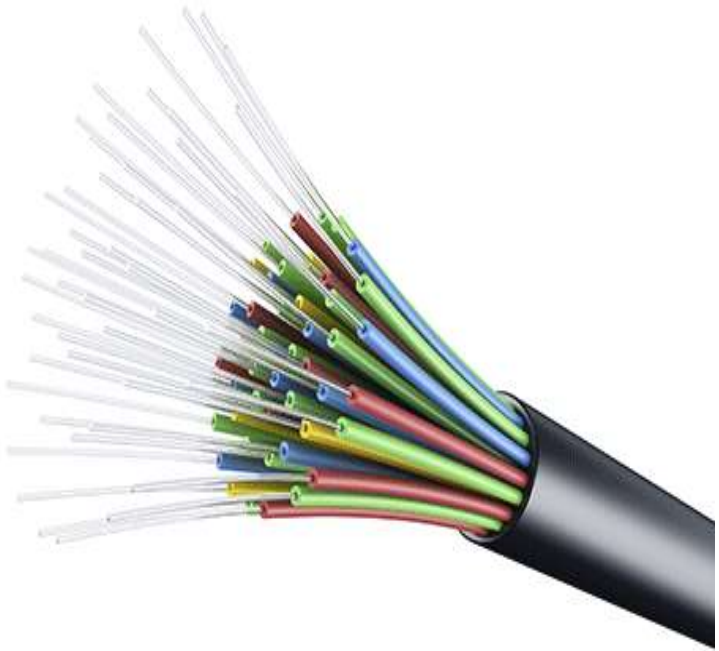
• The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.

•This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover


Insulator
Plastic cover
Outer conductor
(shield)
Inner conductor
Outside Sheath/Jacket
Conducting
Shield
Insulating
Layer
Center
Conductor

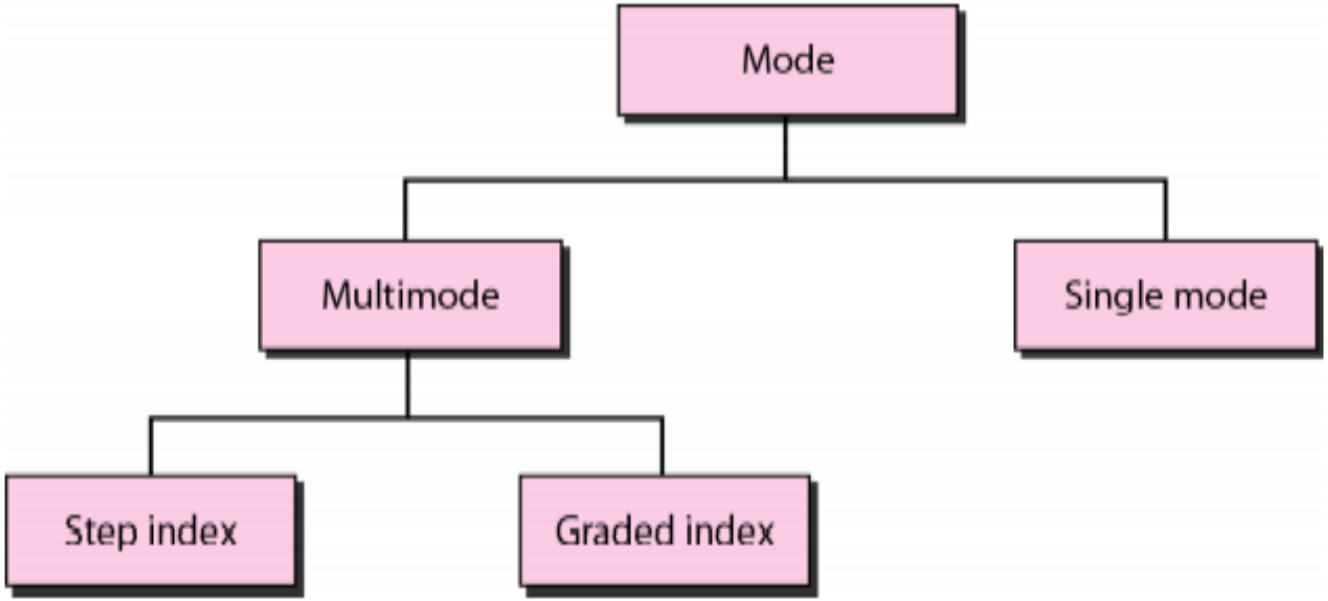
Fiber-Optic Cable

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- Light travels in a straight line as long as it is moving through a single uniform substance.
- If a ray of light traveling through one substance suddenly enters another substance(of a different density), the ray changes direction.
- Bending of light ray-Optical fibers use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.




1920 x 1380

Propagation Modes



Applications

- Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective..
- Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network
- Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable

Un-Guided Media

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.

Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation

- Radio Waves
- Microwaves
- Infrared

Radio Waves

- Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves.
- Radio waves are omni directional. When an antenna transmits radio waves, they are propagated in all directions.
- This means that the sending and receiving antennas do not have to be aligned.
- A sending antenna sends waves that can be received by any receiving antenna.
- The omni directional property has a disadvantage, too.
- The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band

The Omni directional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers.

AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

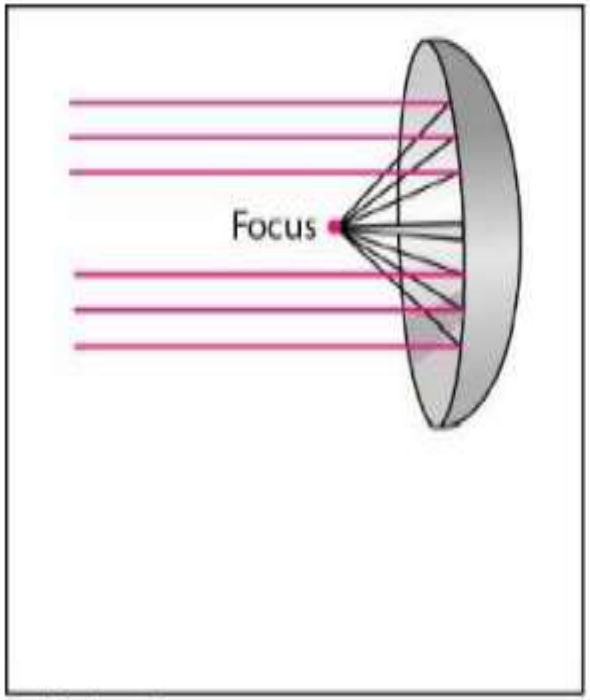
Micro Waves

• Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.

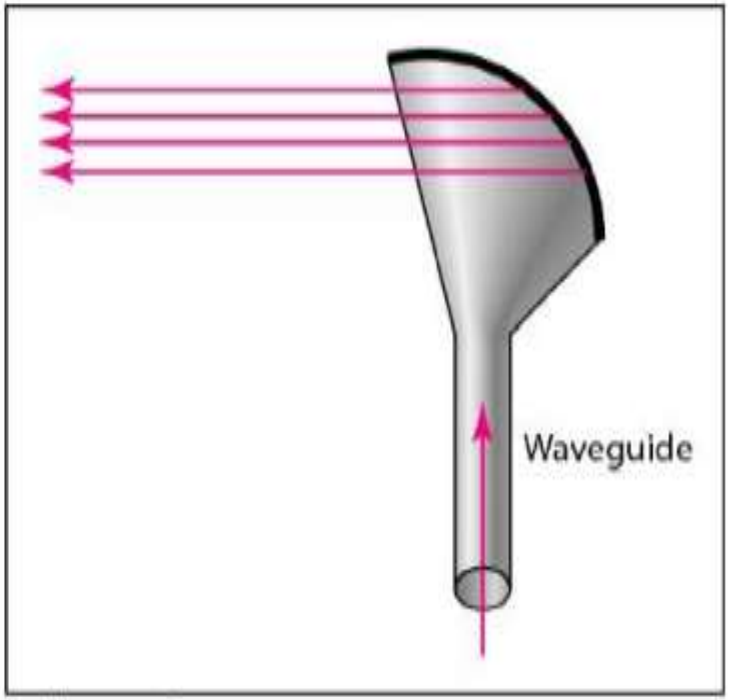
• Microwaves are unidirectional. The sending and receiving antennas need to be aligned.

• The unidirectional property has an obvious advantage.

• A pair of antennas can be aligned without interfering with another pair of aligned antennas



a. Dish antenna



b. Horn antenna

Infrared Waves

• Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication

• Infrared waves, having high frequencies, cannot penetrate walls

• This advantageous characteristic prevents interference between one system and another; a short range communication system in one room cannot be affected by another system in the next room.

Computer Networks

Transmission Medium

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Transmission Medium

Computer Networks: MCA, I Year/II-Sem.

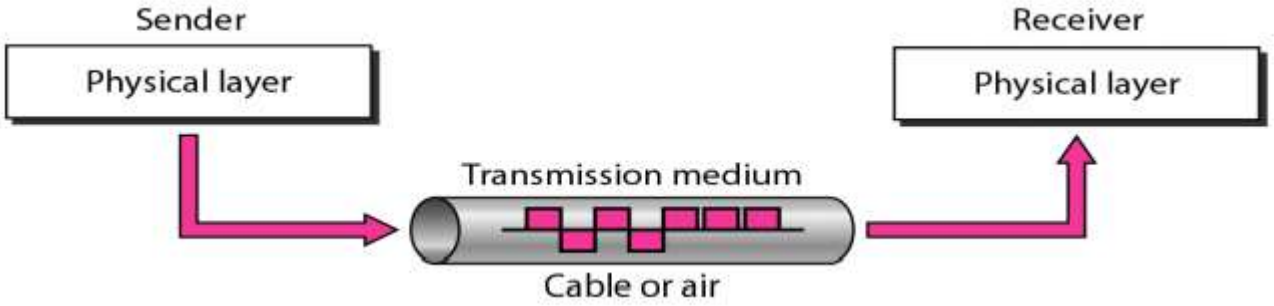
Outline

- Introduction to Transmission Medium
- Classification of Transmission Medium
- Guided Medium
- Un-Guided Medium

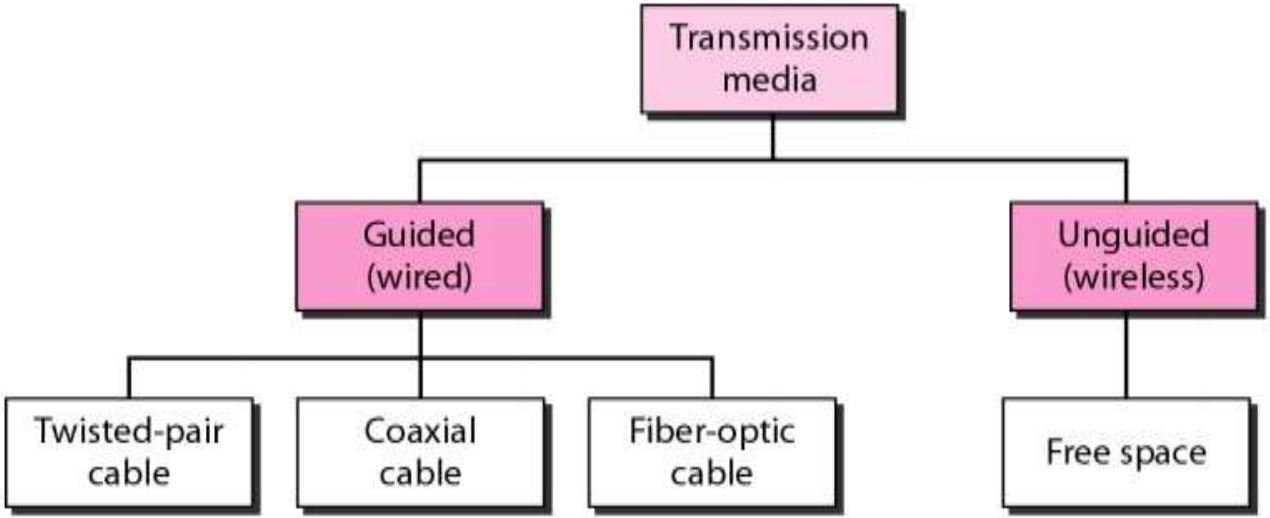
Transmission Medium

• In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver

• It is the channel through which data is sent from one place to another



Classification



Guided Media

Guided media, which are those that provide a medium from one device to another, include

- Twisted-pair cable
- Coaxial cable
- Fiber-optic cable

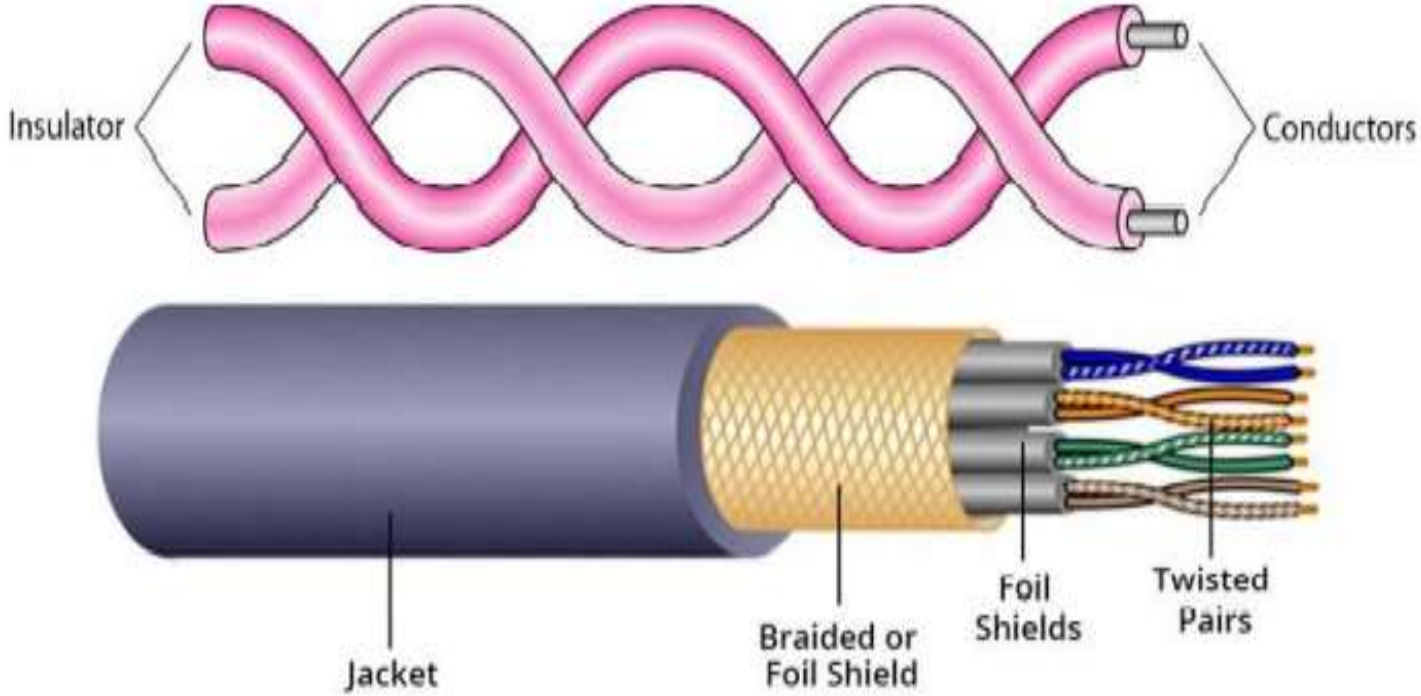
Twisted-Pair Cables

• A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.

• One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference

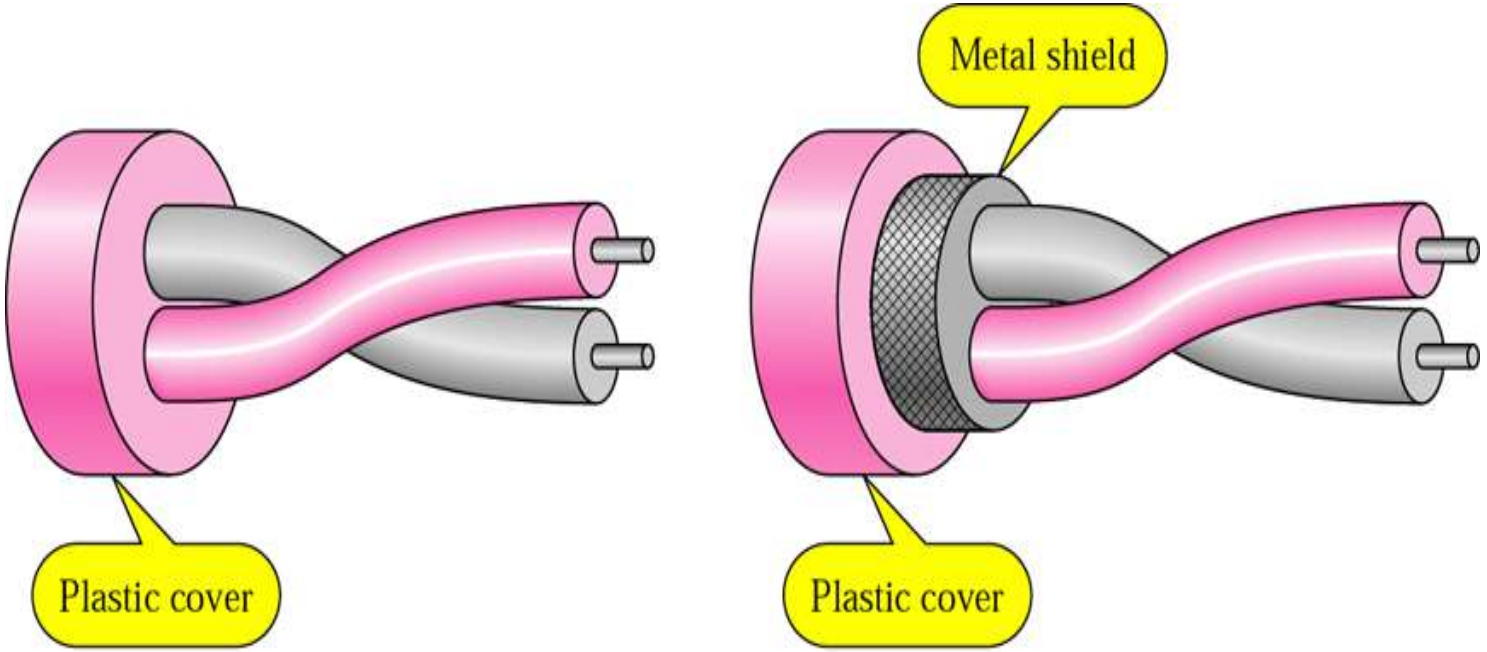
• Twisted-pair cables are used in telephone lines to provide voice and data channels.

• Local-area networks, such as l0Base-T and l00Base-T, also use twisted-pair cables.


Insulator
Conductors
Jacket
Braided or
Foil Shield
Foil
Shields
Twisted
Pairs

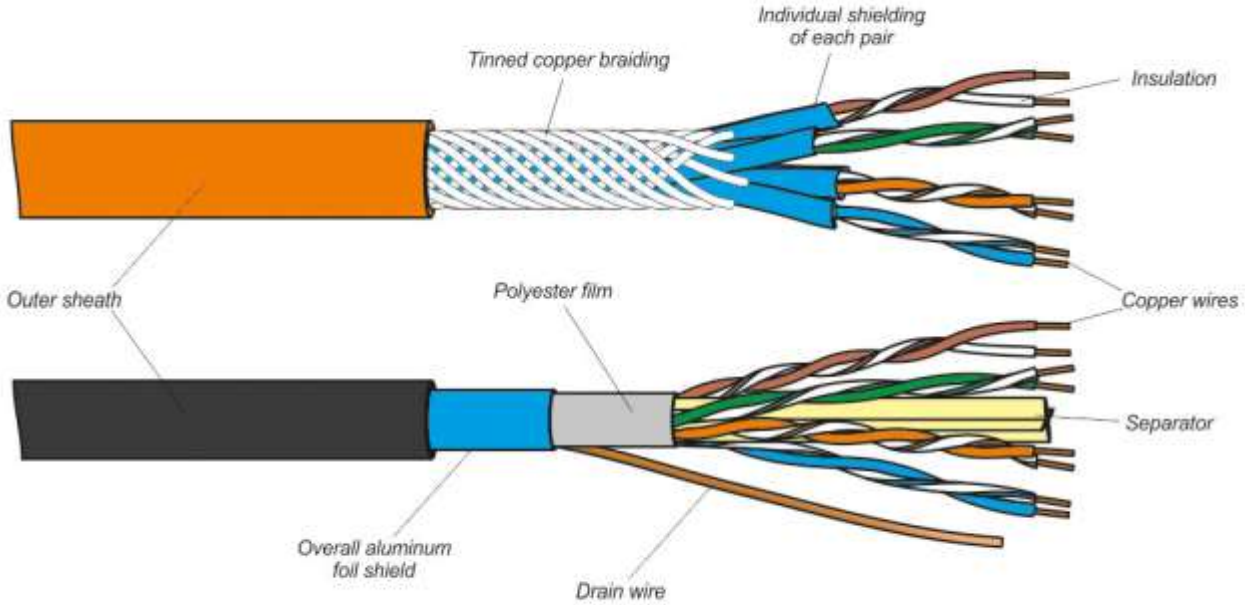
Shield and Un-Shield Twisted-Pair

- The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP)
- STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors
- Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive



a. UTP

b. STP


Individual shielding
of each pair
Tinned copper braiding
Insulation
Outer sheath
Polyester film
Copper wires
Separator
Overall aluminum
foil shield
Drain wire

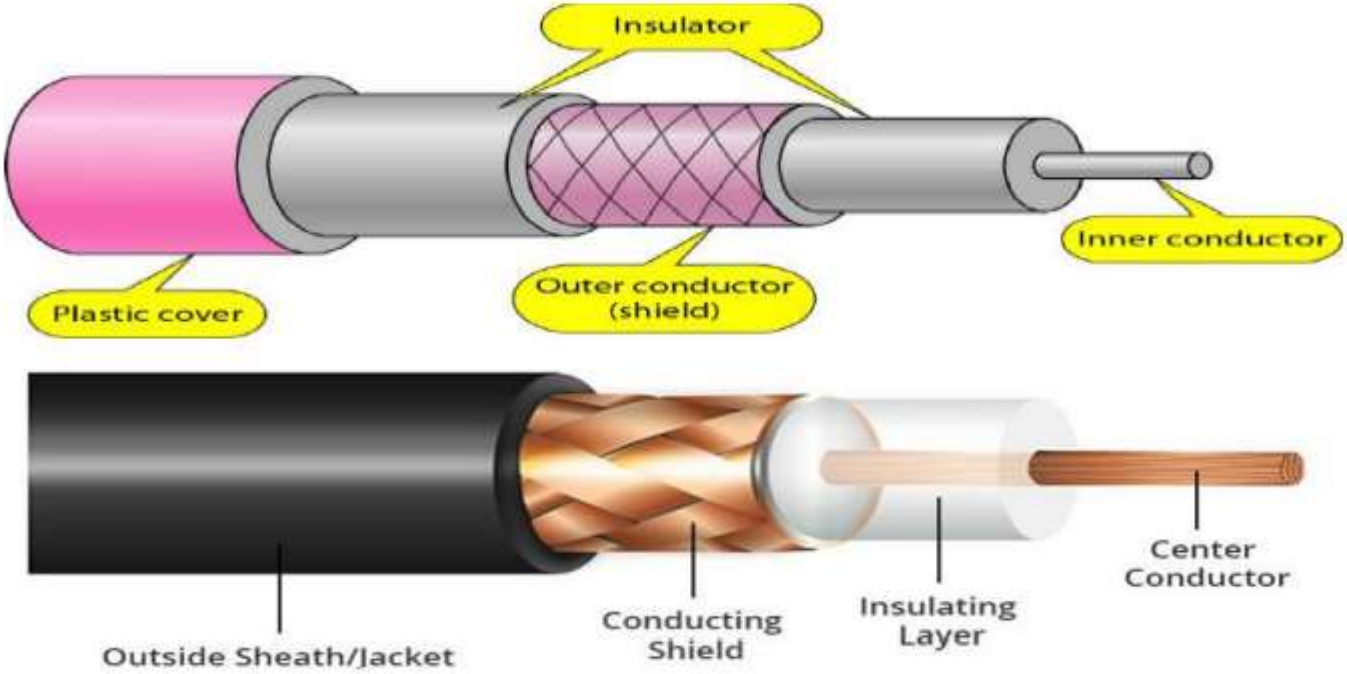
Coaxial Cable

• Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable.

• Coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.

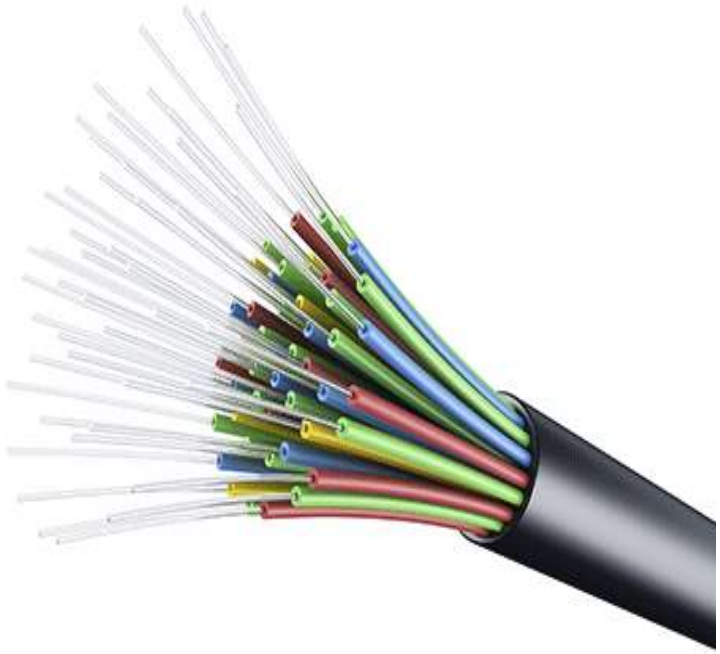
• The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.

•This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover


Insulator
Inner conductor
Plastic cover
Outer conductor
(shield)
Outside Sheath/Jacket
Conducting
Shield
Insulating
Layer
Center
Conductor

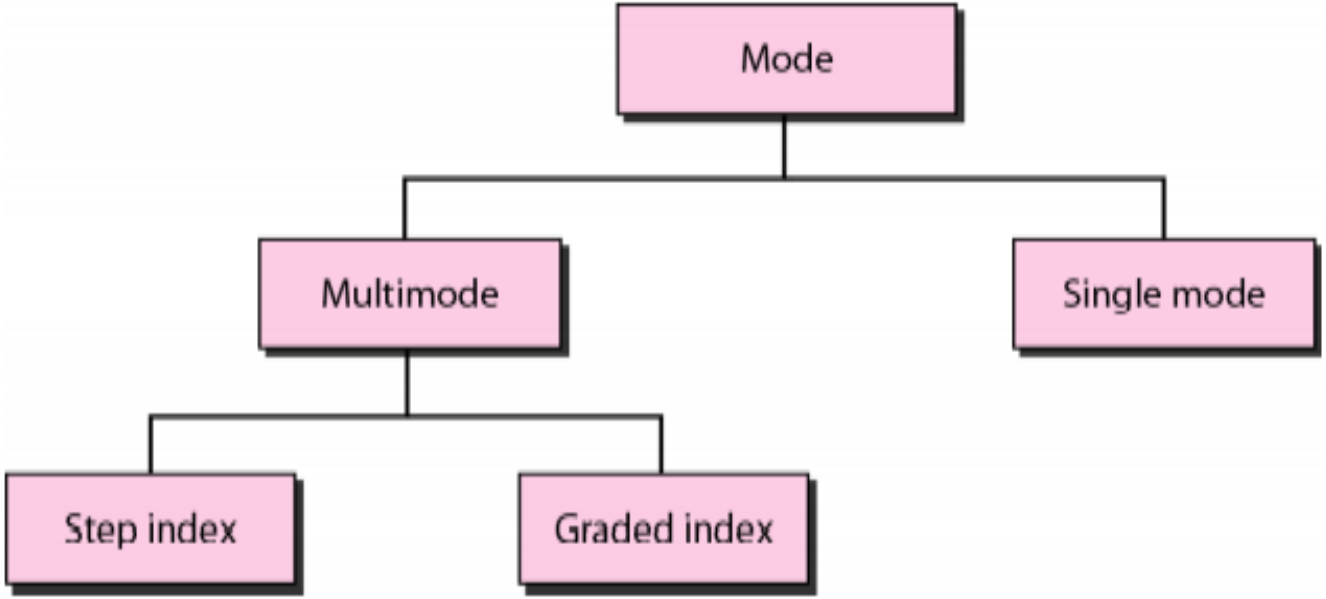
Fiber-Optic Cable

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- Light travels in a straight line as long as it is moving through a single uniform substance.
- If a ray of light traveling through one substance suddenly enters another substance(of a different density), the ray changes direction.
- Bending of light ray-Optical fibers use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.




1920 x 1380

Propagation Modes



Applications

- Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective..
- Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network
- Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable

Un-Guided Media

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.

Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation

- Radio Waves
- Microwaves
- Infrared

Radio Waves

• Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves.

• Radio waves are omni directional. When an antenna transmits radio waves, they are propagated in all directions.

• This means that the sending and receiving antennas do not have to be aligned.

• A sending antenna sends waves that can be received by any receiving antenna.

• The omni directional property has a disadvantage, too.

• The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band

The Omni directional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers.

AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

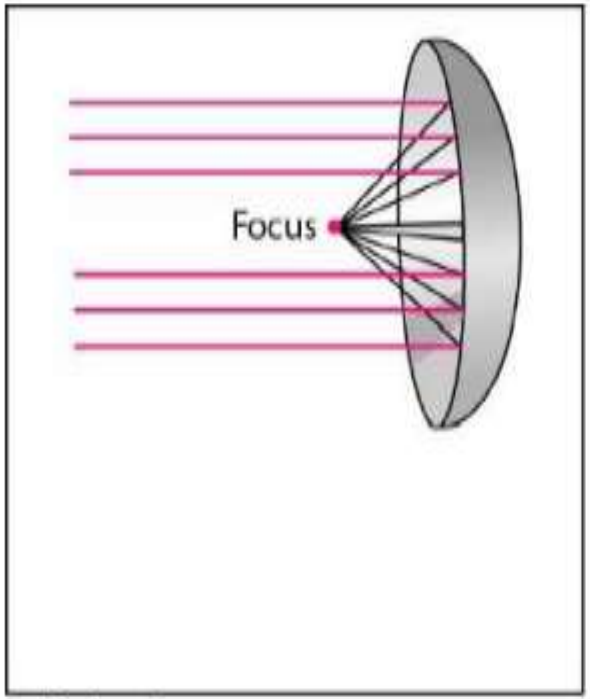
Micro Waves

• Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.

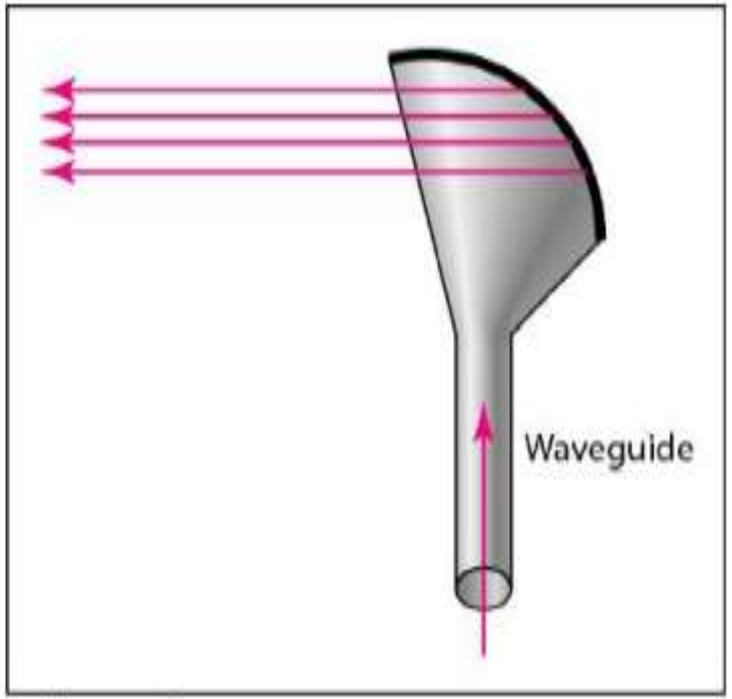
• Microwaves are unidirectional. The sending and receiving antennas need to be aligned.

• The unidirectional property has an obvious advantage.

• A pair of antennas can be aligned without interfering with another pair of aligned antennas



a. Dish antenna



b. Horn antenna

Infrared Waves

• Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication

• Infrared waves, having high frequencies, cannot penetrate walls

• This advantageous characteristic prevents interference between one system and another; a short range communication system in one room cannot be affected by another system in the next room.

Computer Networks

Data Link Layer Design Issues

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Data Link Layer Design Issues

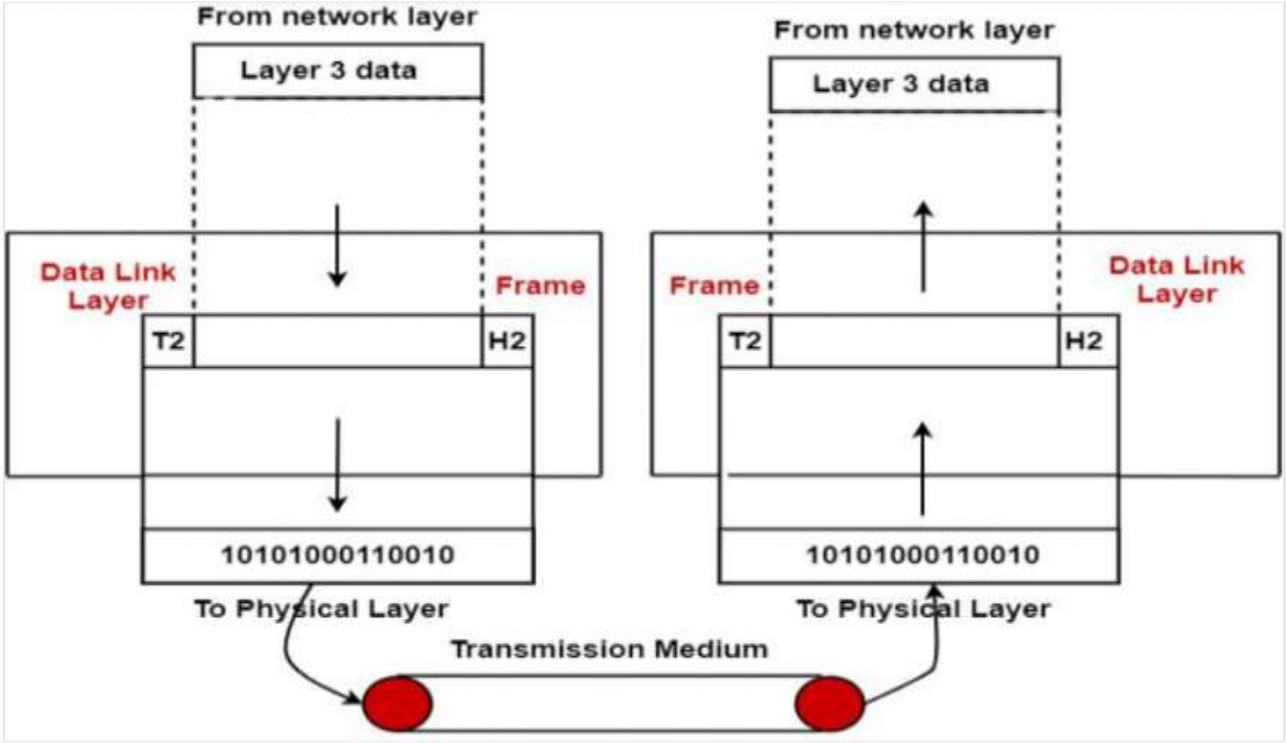
Computer Networks: MCA, I Year/II-Sem.

Outline

- Introduction to Data Link Layer
- Functionalities
- Error Detection Codes
- CRC

Data Link Layer

- The primary service of the data link layer is to support error-free transmission.
- The physical layer sends the information from the sender's hub to the receiver's hub as raw bits.
- The data link layer must identify and correct any bug in the communicated data.
- It takes packets from the network layer and divides the packets into frames which are shared by the sender through the physical layer



Design Issues/Functionalities

- Services providing to Network Layer
- Framings
- Physical Addressing
- Error Control
- Flow Control
- Access Control

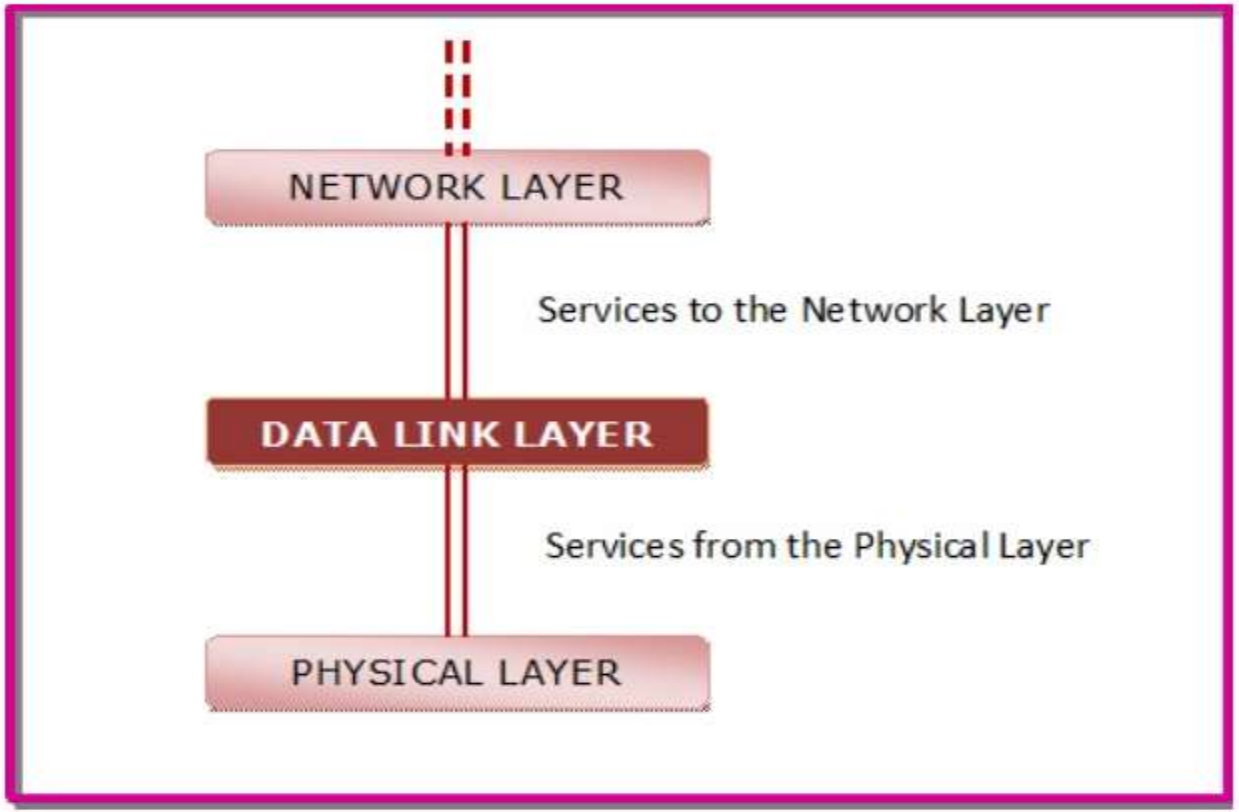
Services providing to Network Layer

In the OSI Model, each layer uses the services of the layer below it and provides services to the layer above it. The data link layer uses the services offered by the physical layer.

The primary function of this layer is to provide a well defined service interface to network layer above it.

The types of services provided can be of three types −

- Unacknowledged connectionless service
- Acknowledged connectionless service
- Acknowledged connection - oriented service

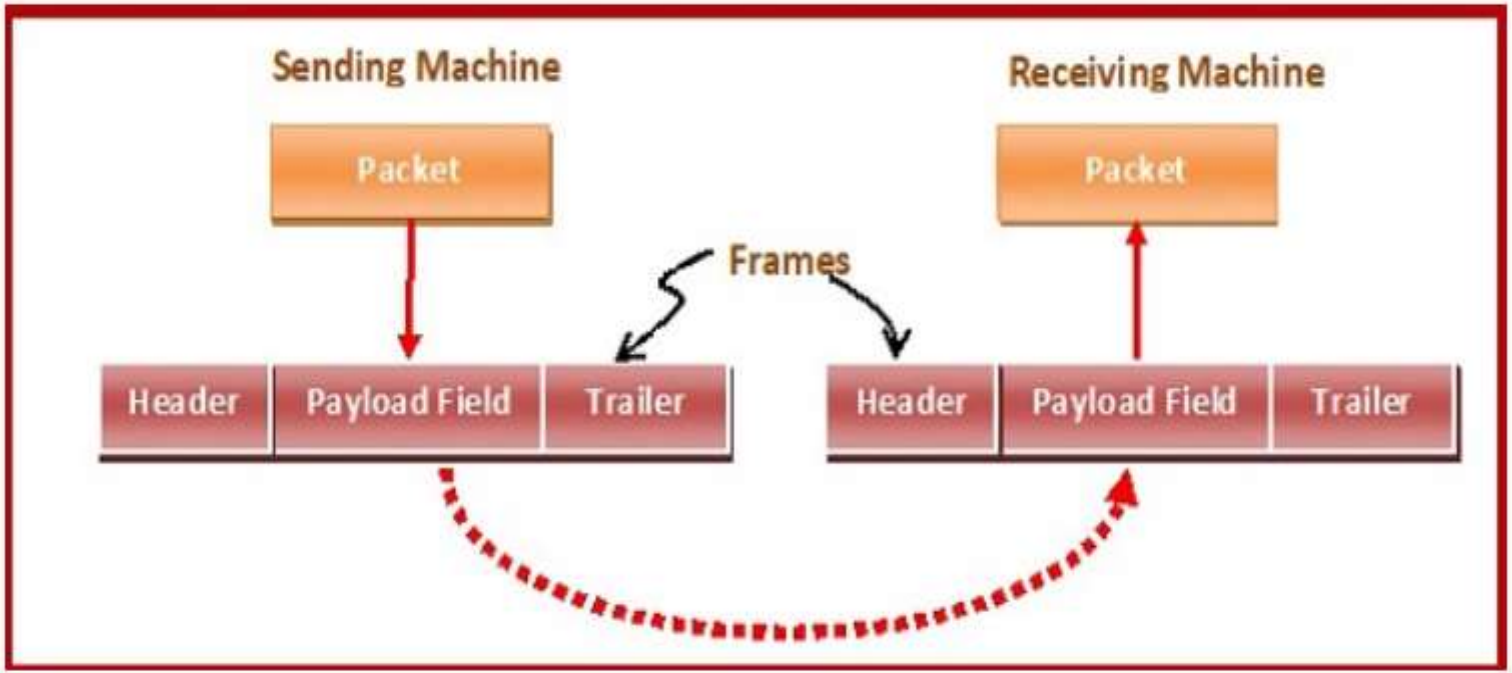

NETWORK LAYER
Services to the Network Layer
DATA LINK LAYER
Services from the Physical Layer
PHYSICAL LAYER

Framing

The data link layer encapsulates each data packet from the network layer into frames that are then transmitted.

A frame has three parts, namely −

- Frame Header
- Payload field that contains the data packet from network layer
- Trailer


Sending Machine
Receiving Machine
Packet
Packet
Frames
Header
Payload Field
Trailer
Header
Payload Field
Trailer

Physical Addressing

The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network

Flow Control

• A receiving node can receive the frames at a faster rate than it can process the frame.

• Without flow control, the receiver's buffer can overflow, and frames can get lost.

• To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link. This prevents traffic jam at the receiver side

Error Control

Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.

Error detection:

Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.

Error correction:

Error correction is similar to the Error detection, except that receiving node not only detects the errors but also determine where the errors have occurred in the frame

Access Control

Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link

What is an Error?

- A condition when the receiver's information does not match with the sender's information
- During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver
- That means a 0 bit may change to 1 or a 1 bit may change to 0

Error Detection

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted

To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message

Error Detection Methods

1. Simple Parity check
2. Two-dimensional Parity check
3. Checksum
4. Cyclic Redundancy check

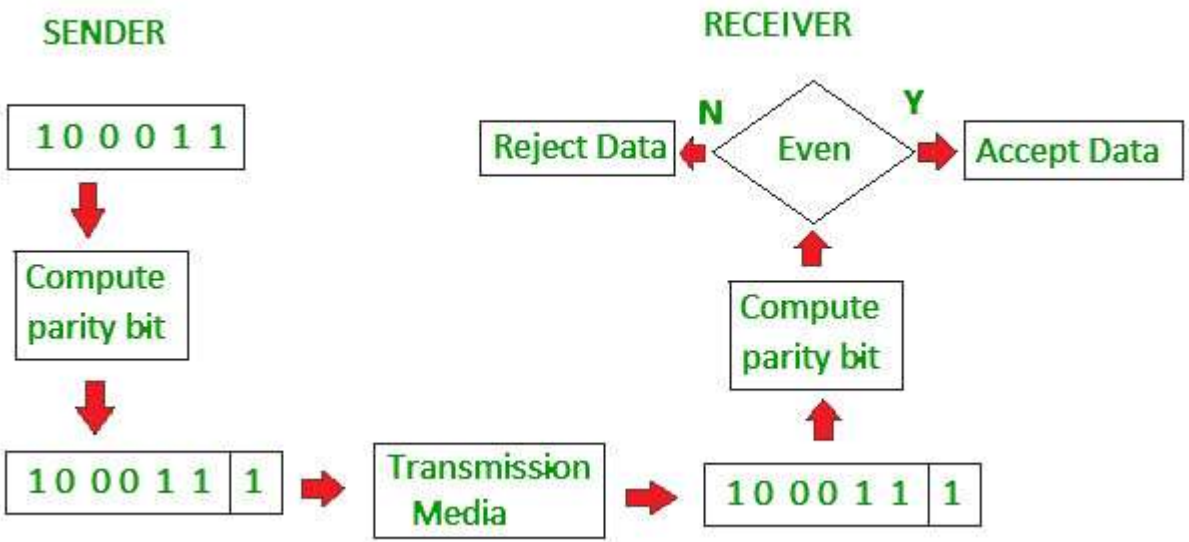
Simple parity Check

Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

1 is added to the block if it contains odd number of 1's, and

0 is added if it contains even number of 1's

This scheme makes the total number of 1's even, that is why it is called even parity checking


SENDER
RECEIVER
1 0 0 0 1 1
Compute parity bit
1 0 0 0 1 1 1
Transmission Media
1 0 0 0 1 1 1
Compute parity bit
Even
N
Y
Reject Data
Accept Data

Two dimensional parity Check

- Parity check bits are calculated for each row, which is equivalent to a simple parity check bit.
- Parity check bits are also calculated for all columns, then both are sent along with the data.
- At the receiving end these are compared with the parity bits calculated on the received data.

Original Data

10011001	11100010	00100100	10000100

Row parities

10011001	0
11100010	0
00100100	0
10000100	0
11011011	0

Column parities

100110010	111000100	001001000	100001000	110110110

Data to be sent

Check Sum

• In checksum error detection scheme, the data is divided into k segments each of m bits

• In the sender’s end the segments are added using 1’s complement arithmetic to get the sum. The sum is complemented to get the checksum

• The checksum segment is sent along with the data segments

• At the receiver’s end, all received segments are added using 1’s complement arithmetic to get the sum. The sum is complemented

• If the result is zero, the received data is accepted; otherwise discarded.

Original Data

10011001	11100010	00100100	10000100
1	2	3	4

k=4, m=8

Sender

```
1        1 0 0 1 1 0 0 1
2        1 1 1 0 0 0 1 0
       ---------------
       (1)0 1 1 1 1 0 1 1
                       1
       ---------------
         0 1 1 1 1 1 0 0
3        0 0 1 0 0 1 0 0
       ---------------
         1 0 1 0 0 0 0 0
4        1 0 0 0 0 1 0 0
       ---------------
       (1)0 0 1 0 0 1 0 0
                       1
       ---------------
Sum:     0 0 1 0 0 1 0 1
       ---------------
CheckSum: 1 1 0 1 1 0 1 0
```

Reciever

```
1        1 0 0 1 1 0 0 1
2        1 1 1 0 0 0 1 0
       ---------------
       (1)0 1 1 1 1 0 1 1
                       1
       ---------------
         0 1 1 1 1 1 0 0
3        0 0 1 0 0 1 0 0
       ---------------
         1 0 1 0 0 0 0 0
4        1 0 0 0 0 1 0 0
       ---------------
       (1)0 0 1 0 0 1 0 0
                       1
       ---------------
         0 0 1 0 0 1 0 1
         1 1 0 1 1 0 1 0
       ---------------
Sum:     1 1 1 1 1 1 1 1
       ---------------
Complement: 0 0 0 0 0 0 0 0
```

Conclusion: Accept Data

CRC

• Unlike checksum scheme, which is based on addition, CRC is based on binary division.

• In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.

• At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.

• A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

original message

1 0 1 0 0 0 0

@ means X-OR

Generator polynomial

x^3+1

$1.x^3+0.x^2+0.x^1+1.x^0$

CRC generator

1 0 0 1 4-bit

If CRC generator is of n bit then append (n-1) zeros in the end of original message

Sender

```
1 0 0 1 | 1 0 1 0 0 0 0 0 0 0
        @ 1 0 0 1
          0 0 1 1 0 0 0 0 0 0
          @ 1 0 0 1
            0 1 0 1 0 0 0 0
            @ 1 0 0 1
              0 0 1 1 0 0 0
              @ 1 0 0 1
                0 1 0 1 0
                @ 1 0 0 1
                  0 0 1 1
```

Message to be transmitted

```
1 0 1 0 0 0 0 0 0 0
        + 0 1 1
-----------------
1 0 1 0 0 0 0 0 1 1
```

```
1 0 0 1 | 1 0 1 0 0 0 0 0 1 1
        @ 1 0 0 1
          0 0 1 1 0 0 0 0 1 1
          @ 1 0 0 1
            0 1 0 1 0 0 1 1
            @ 1 0 0 1
              0 0 1 1 0 1 1
              @ 1 0 0 1
                0 1 0 0 1
                @ 1 0 0 1
                  0 0 0 0
```

Receiver

Zero means data is accepted

Computer Networks

Data Link Layer Protocols

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Data Link Layer Protocols

Computer Networks: MCA, I Year/II-Sem.

Outline

- Introduction to Data Link Layer Protocols
- Types
- For Noiseless Channels
- For Noisy Channels

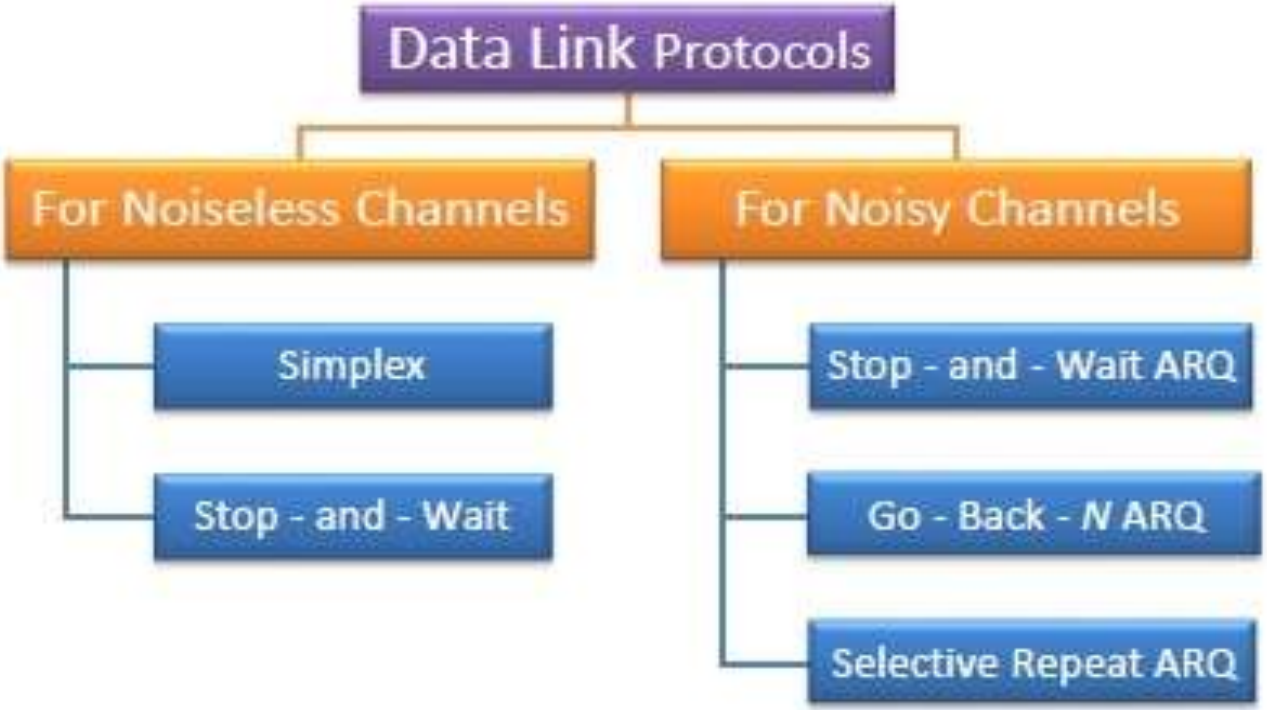
Introduction

•Protocols in the data link layer are designed so that this layer can perform its basic functions: framing, error control and flow control.

• Framing is the process of dividing bit - streams from physical layer into data frames whose size ranges from a few hundred to a few thousand bytes.

• Error control mechanisms deals with transmission errors and retransmission of corrupted and lost frames.

• Flow control regulates speed of delivery and so that a fast sender does not drown a slow receiver


Data Link Protocols
For Noiseless Channels
For Noisy Channels
Simplex
Stop - and - Wait
Stop - and - Wait ARQ
Go - Back - N ARQ
Selective Repeat ARQ

Simplex Protocol

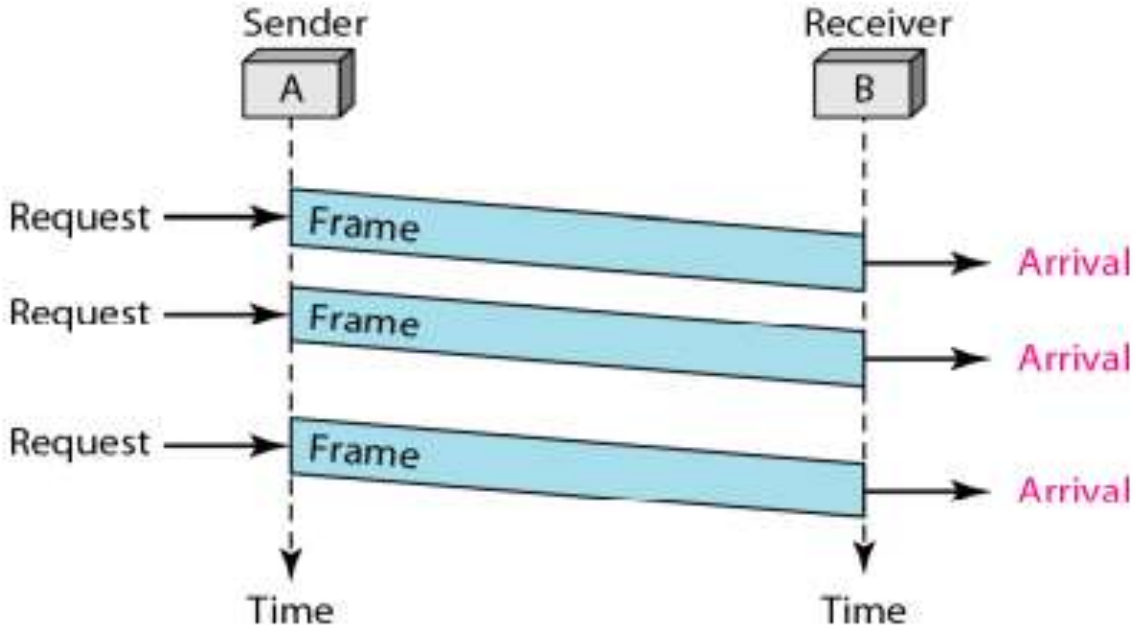
• The sender sends a sequence of frames without even thinking about the receiver. Data are transmitted in one direction only.

• Both sender & receiver always ready.

• Processing time can be ignored.

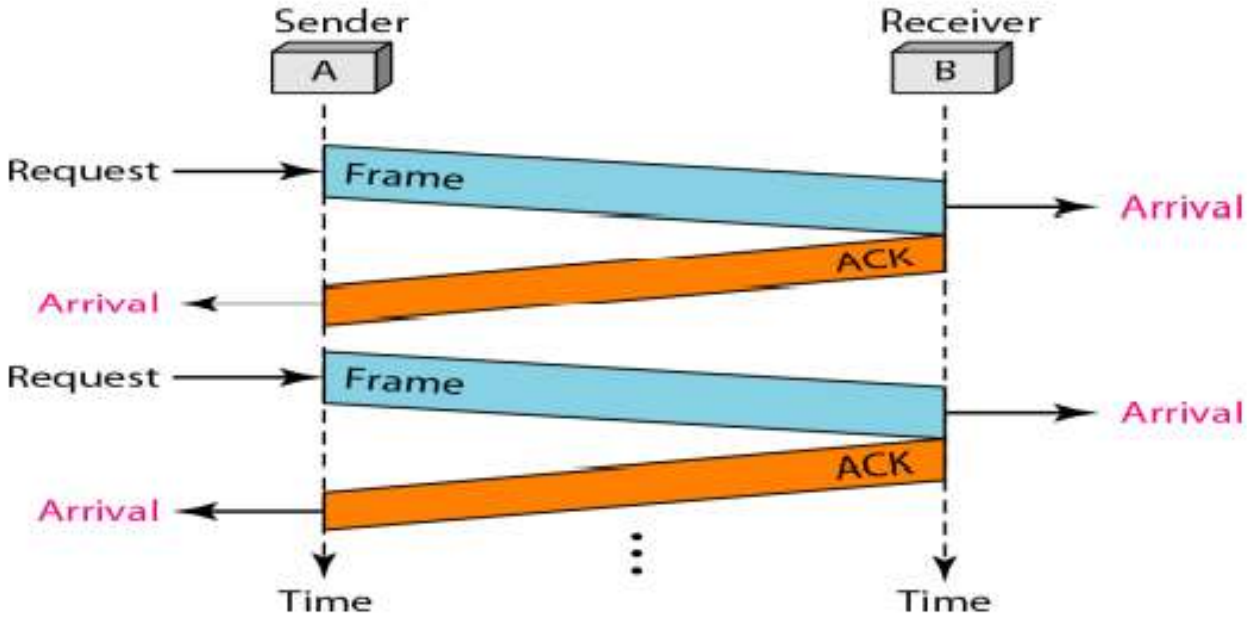
• Infinite buffer space is available. And best of all, the communication channel between the data link layers never damages or loses frames.

• This thoroughly unrealistic protocol, which we will nickname “Utopia,” .The utopia protocol is unrealistic because it does not handle either flow control or error correction


Sender
Receiver
A
B
Request
Frame
Arrival
Request
Frame
Arrival
Request
Frame
Arrival
Time
Time

Stop and Wait Protocol

- The sender sends one frame and waits for feedback from the receiver.
- When the ACK arrives, the sender sends the next frame It is Stop-and-Wait Protocol because the sender sends one frame, stops until it receives confirmation from the receiver (okay to go ahead), and then sends the next frame.
- Still have unidirectional communication for data frames, but auxiliary ACK frames (simple tokens of acknowledgment) travel from the other direction. adding flow control to our previous protocol.


Sender
A
Receiver
B
Request
Frame
Arrival
ACK
Arrival
Request
Frame
Arrival
ACK
Arrival
Time
Time

Stop and Wait ARQ

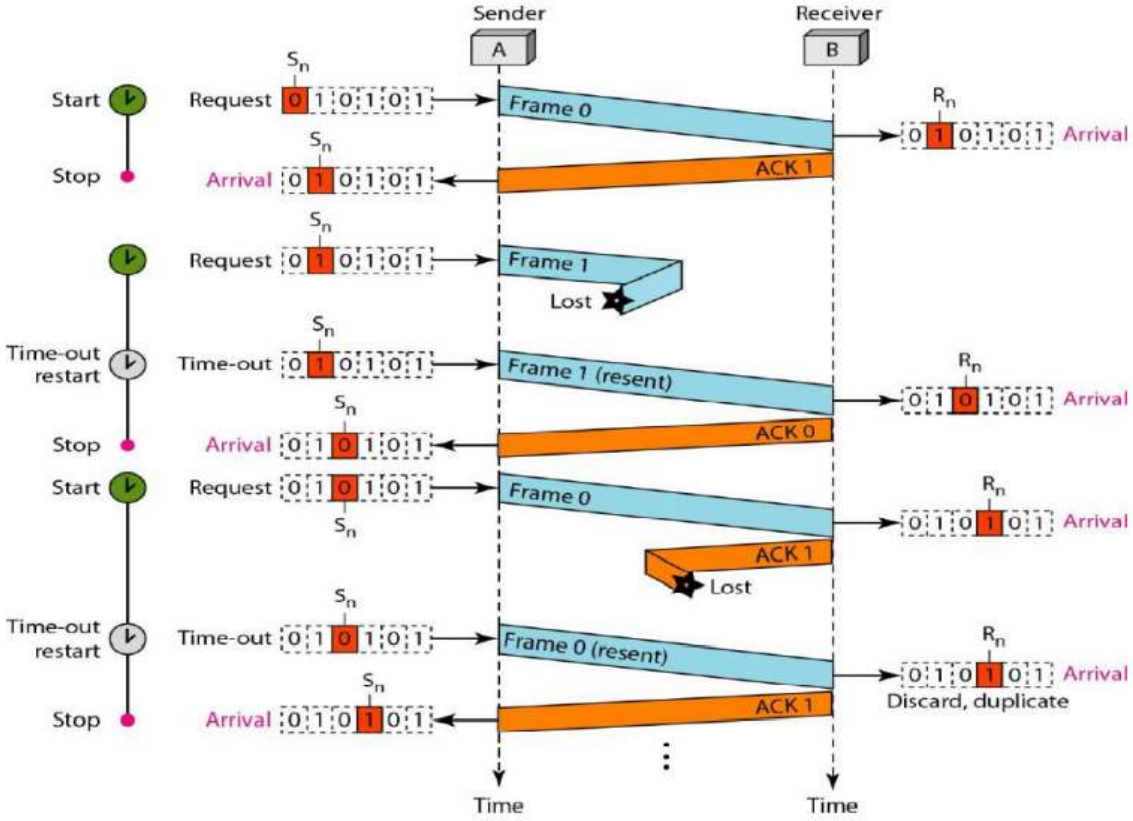
• The lost frames need to be resent in this protocol.

• If the receiver does not respond when there is an error, how can the sender know which frame to resend? To remedy this problem, the sender keeps a copy of the sent frame.

• At the same time, it starts a timer. If the timer expires and there is no ACK for the sent frame, the frame is resent, the copy is held, and the timer is restarted.

• Since the protocol uses the stop-and-wait mechanism, there is only one specific frame that needs an ACK Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame

• The sequence numbers are based on modulo-2 arithmetic



Go-Back-N ARQ

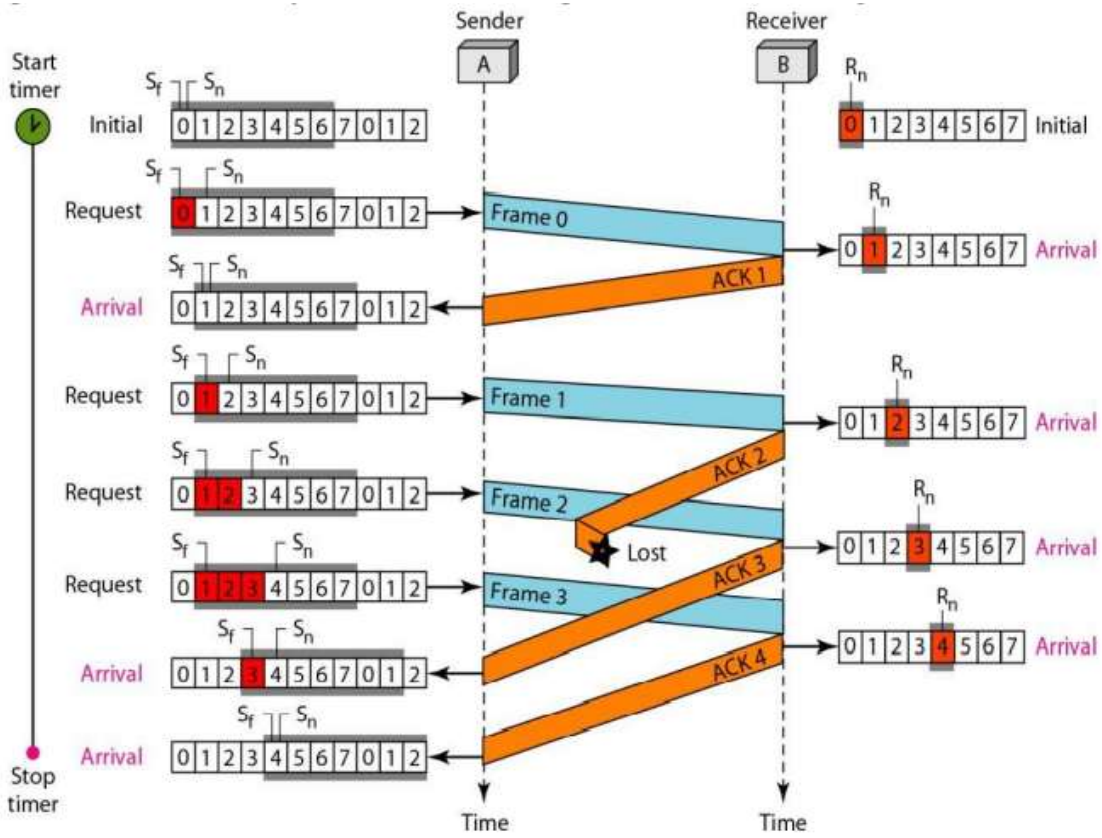
• To improve the efficiency of transmission (filling the pipe), multiple frames must be in transition while waiting for acknowledgment.

• In other words, we need to let more than one frame be outstanding to keep the channel busy while the sender is waiting for acknowledgment.

• The first is called Go-Back-N Automatic Repeat.

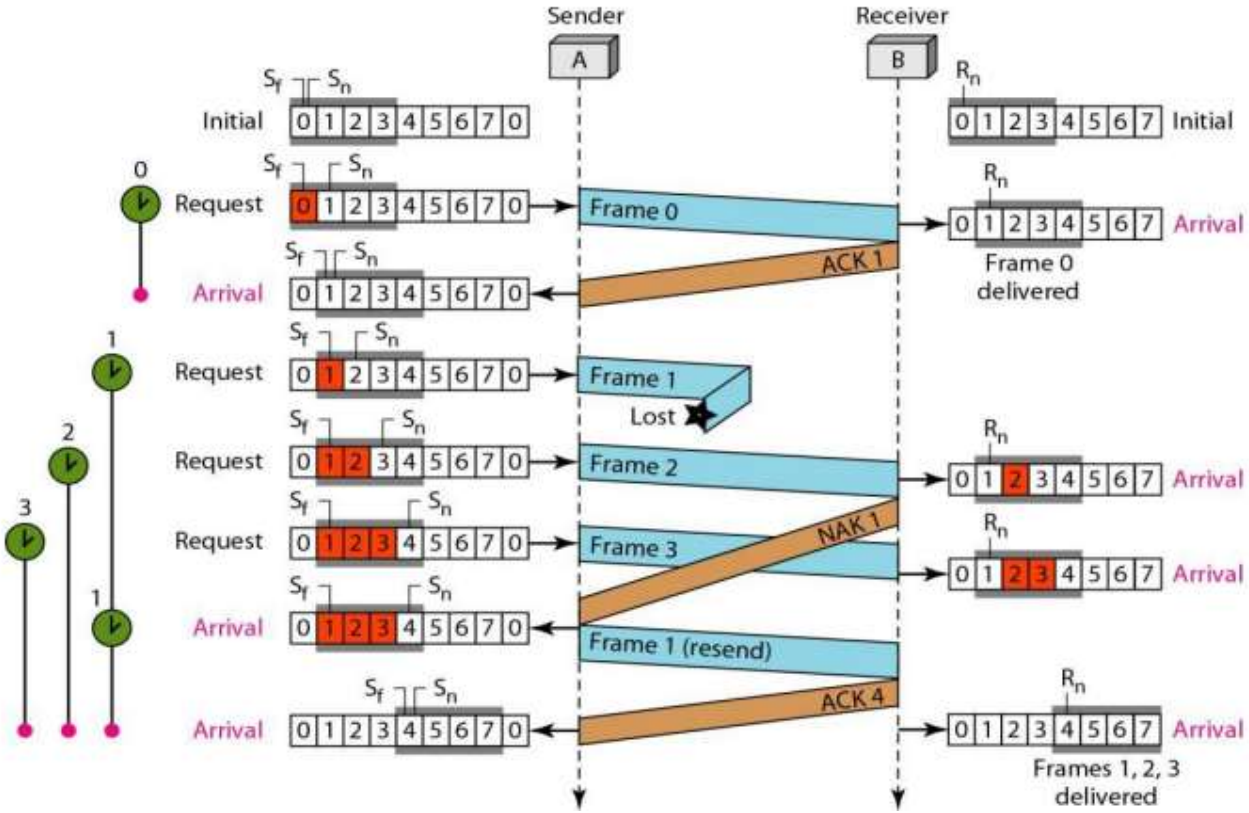
• In this protocol we can send several frames before receiving acknowledgments; we keep a copy of these frames until the acknowledgments arrive

• In the Go-Back-N Protocol, the sequence numbers are modulo 2m, where m is the size of the sequence number field in bits



Selective Repeat ARQ

- One main difference is the number of timers.
- Here, each frame sent or resent needs a timer, which means that the timers need to be numbered (0, 1,2, and 3).
- The timer for frame 0 starts at the first request, but stops when the ACK for this frame arrives.
- There are two conditions for the delivery of frames to the network layer: First, a set of consecutive frames must have arrived.
- Second, the set starts from the beginning of the window. After the first arrival, there was only one frame and it started from the beginning of the window. After the last arrival, there are three frames and the first one starts from the beginning of the window.



Computer Networks

Channel Allocation Methods

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Channel Allocation Methods

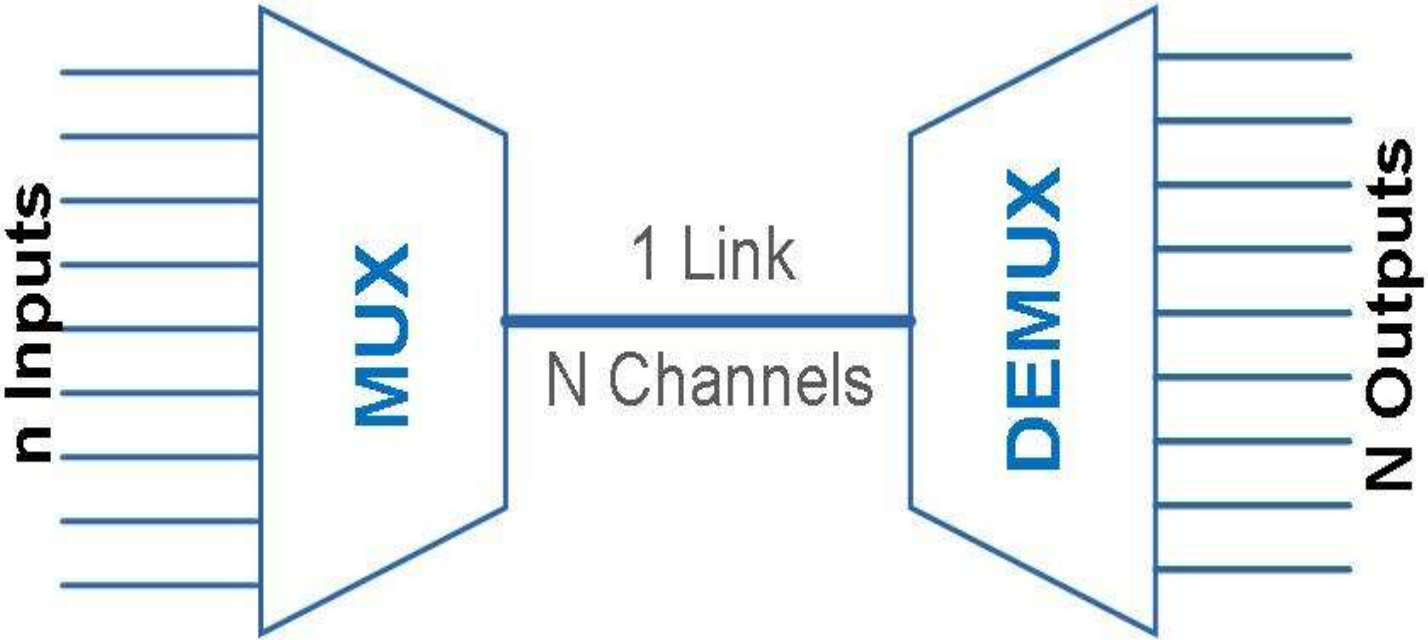
Computer Networks: MCA, I Year/II-Sem.

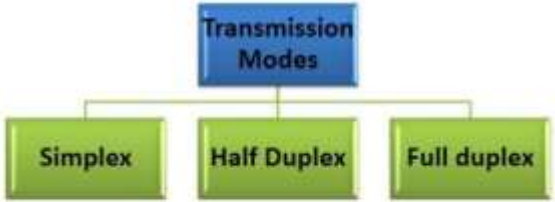
Outline

- MULTIPLEXING
- TDM
- FDM

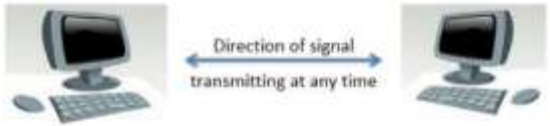
Multiplexing

- Multiple Access is the use of multiplexing techniques to provide communication service to multiple users over a single channel
- It allows for many users at one time by sharing a finite amount of spectrum

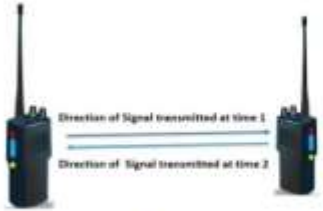

n Inputs
MUX
1 Link
N Channels
DEMUX
N Outputs



Simplex
(one direction only)



Full Duplex
(both directions anytime)



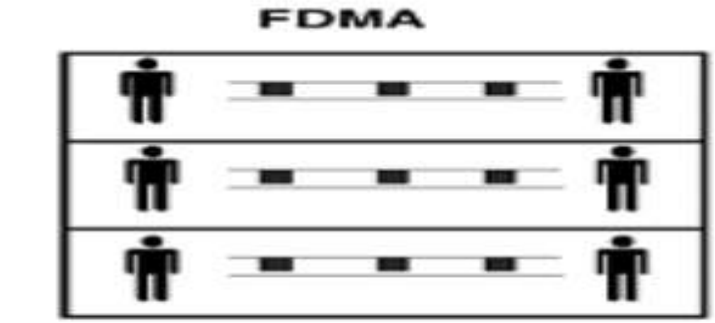
Half Duplex
(one direction at a time)

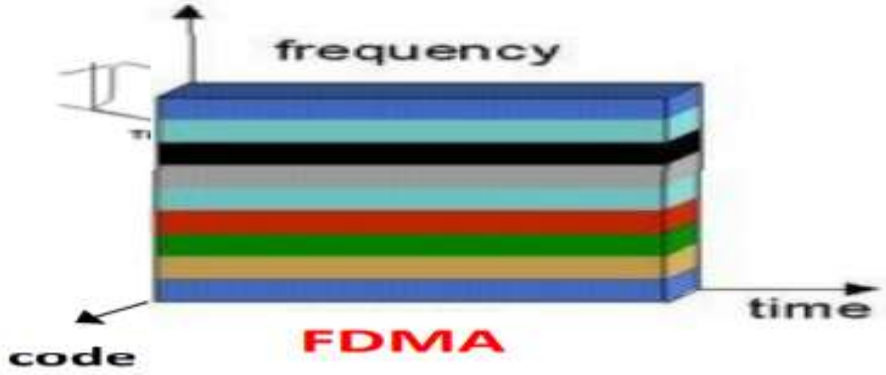
FDM

• Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted

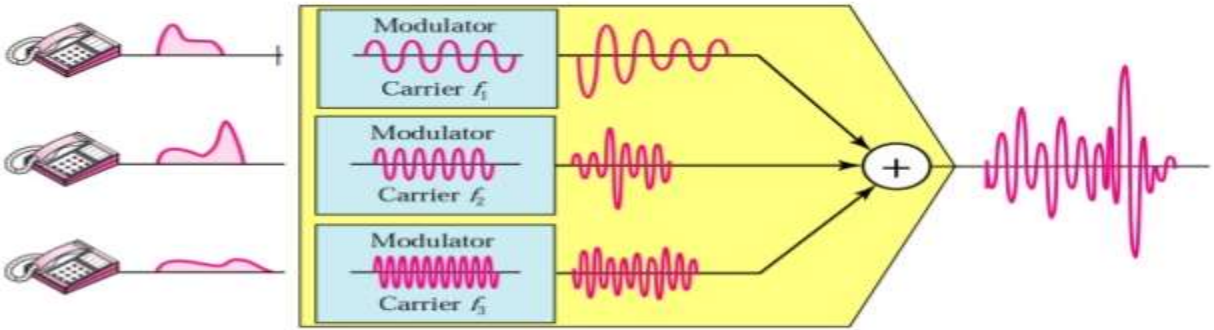
• The available bandwidth is subdivided into a number of narrower band channels.

• Each user is allocated a unique frequency band in which to transmit and receive on

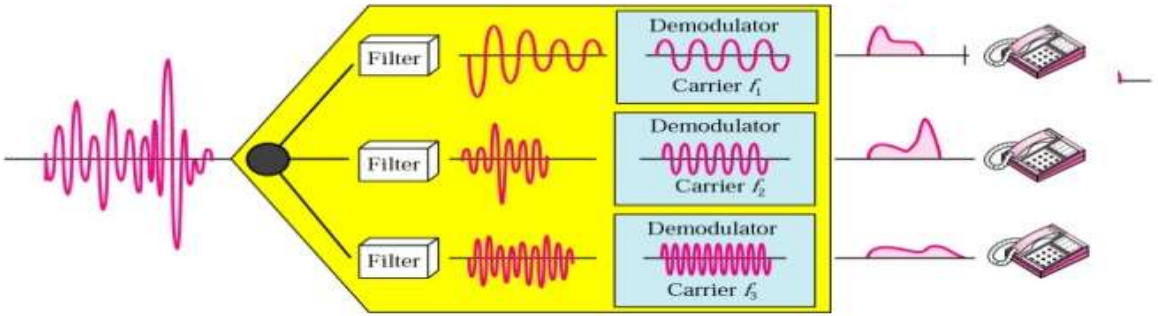

FDMA


frequency
time
code
FDMA

Multiplexing Process in FDM



De-multiplexing Process in FDM



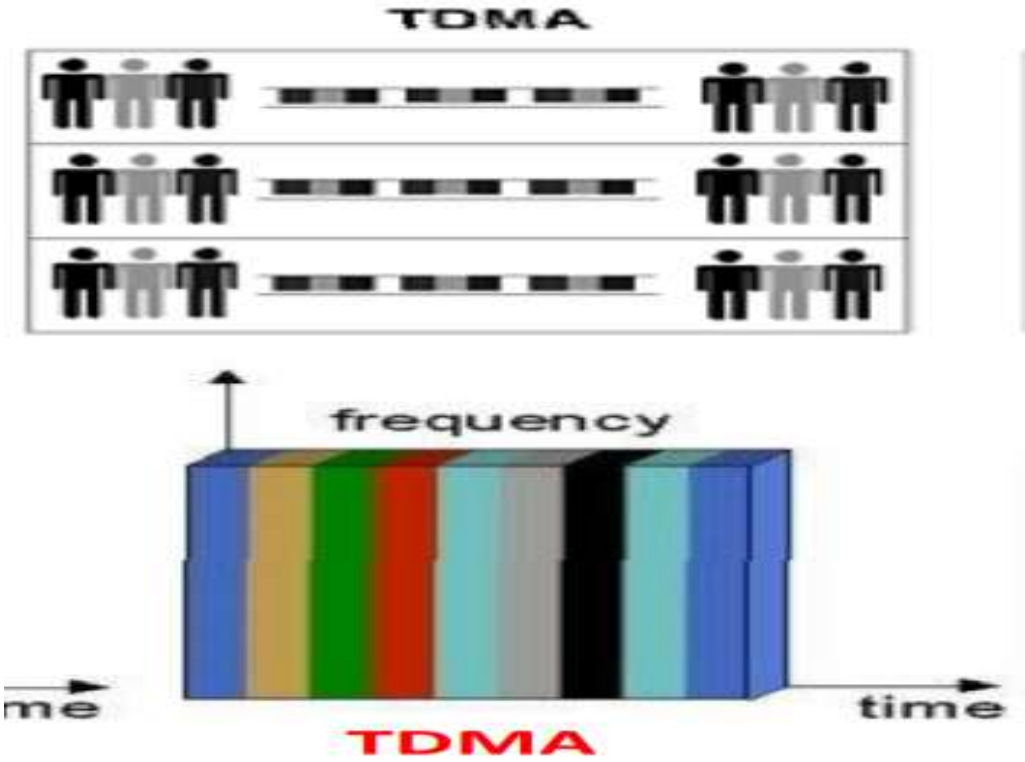
TDM

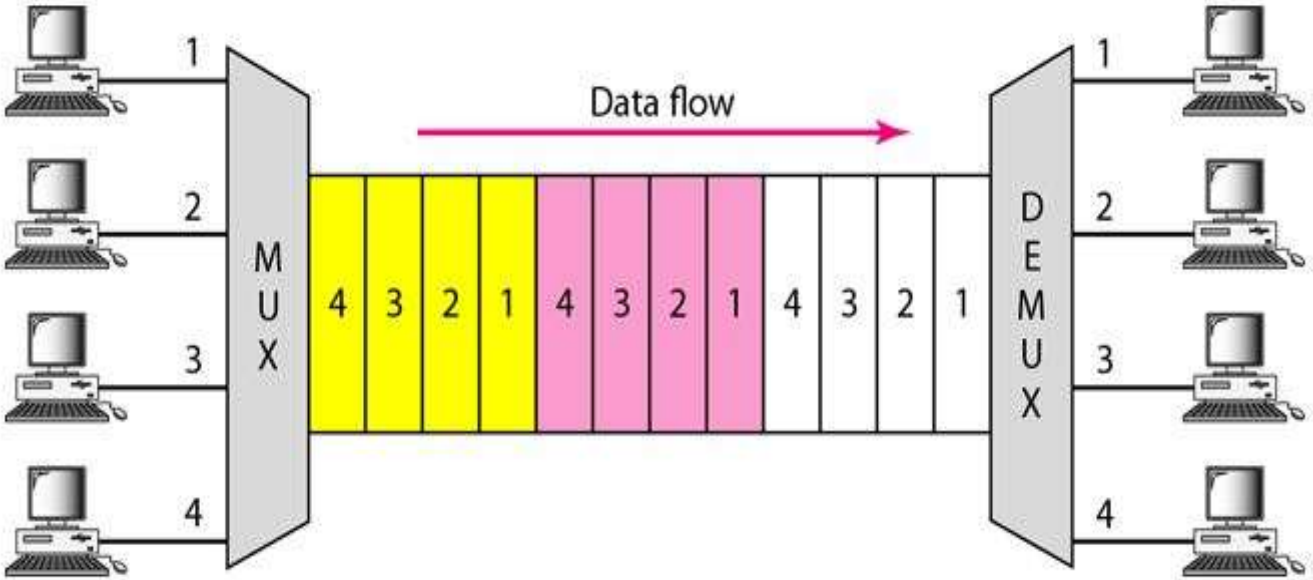
•Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a line Instead of sharing a portion of the bandwidth as in FDM, time is shared

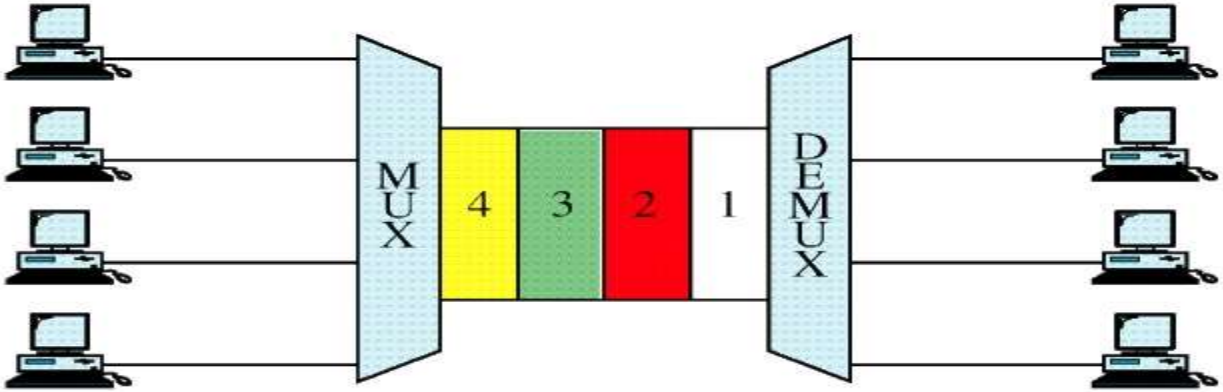
• Each connection occupies a portion of time in the link

• Digital data from different sources are combined into one timeshared link

• However, this does not mean that the sources cannot produce analog data; analog data can be sampled, changed to digital data, and then multiplexed by using TDM


TDMA
frequency
me
time
TDMA




MUX
4
3
2
1
DEMUX

Computer Networks

ALOHA

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : ALOHA

Computer Networks: MCA, I Year/II-Sem.

Outline

- Introduction to ALOHA
- Pure ALOHA
- Slotted ALOHA

ALOHA

• In the 1970s, Norman Abramson and his colleagues at the University of Hawaii devised a new and elegant method to solve the channel allocation problem

• Although Abramson's work, called the ALOHA system, used ground-based radio broadcasting, the basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared channel

• There are two versions of ALOHA: pure and slotted.

• They differ with respect to whether time is divided into discrete slots into which all frames must fit.

• Pure ALOHA does not require global time synchronization; slotted ALOHA does

Pure ALOHA

• The basic idea of an ALOHA system is simple: let users transmit whenever they have data to be sent.

• There will be collisions, of course, and the colliding frames will be damaged

• However, due to the feedback property of broadcasting, a sender can always find out whether its frame was destroyed by listening to the channel, the same way other users do.

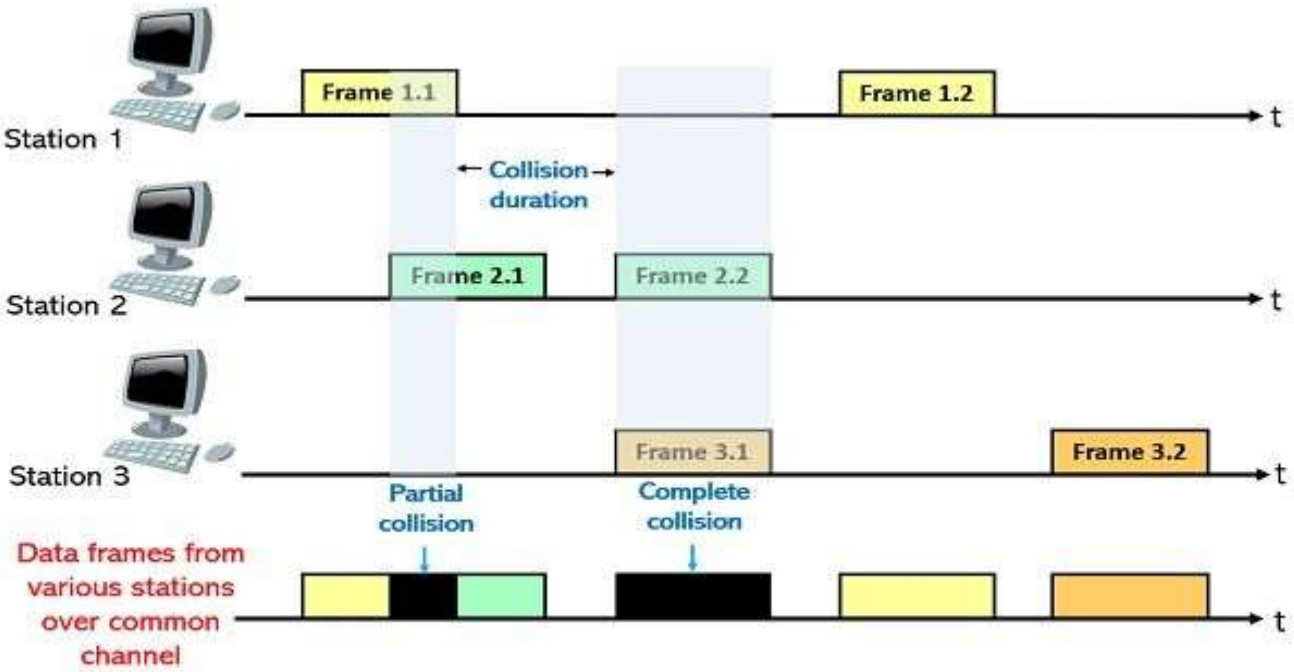
• With a LAN, the feedback is immediate; with a satellite, there is a delay of 270 msec before the sender knows if the transmission was successful.

• If listening while transmitting is not possible for some reason, acknowledgements are needed

• If the frame was destroyed, the sender just waits a random amount of time and sends it again.

• The waiting time must be random or the same frames will collide over and over, in lockstep.

• Systems in which multiple users share a common channel in a way that can lead to conflicts are widely known as contention systems


Station 1
Frame 1.1
Frame 1.2
t
Collision duration
Station 2
Frame 2.1
Frame 2.2
t
Station 3
Frame 3.1
Frame 3.2
t
Partial collision
Complete collision
Data frames from various stations over common channel
t

Pure ALOHA

Slotted ALOHA

• In 1972, Roberts published a method for doubling the capacity of an ALOHA system (Robert, 1972).

• His proposal was to divide time into discrete intervals, each interval corresponding to one frame.

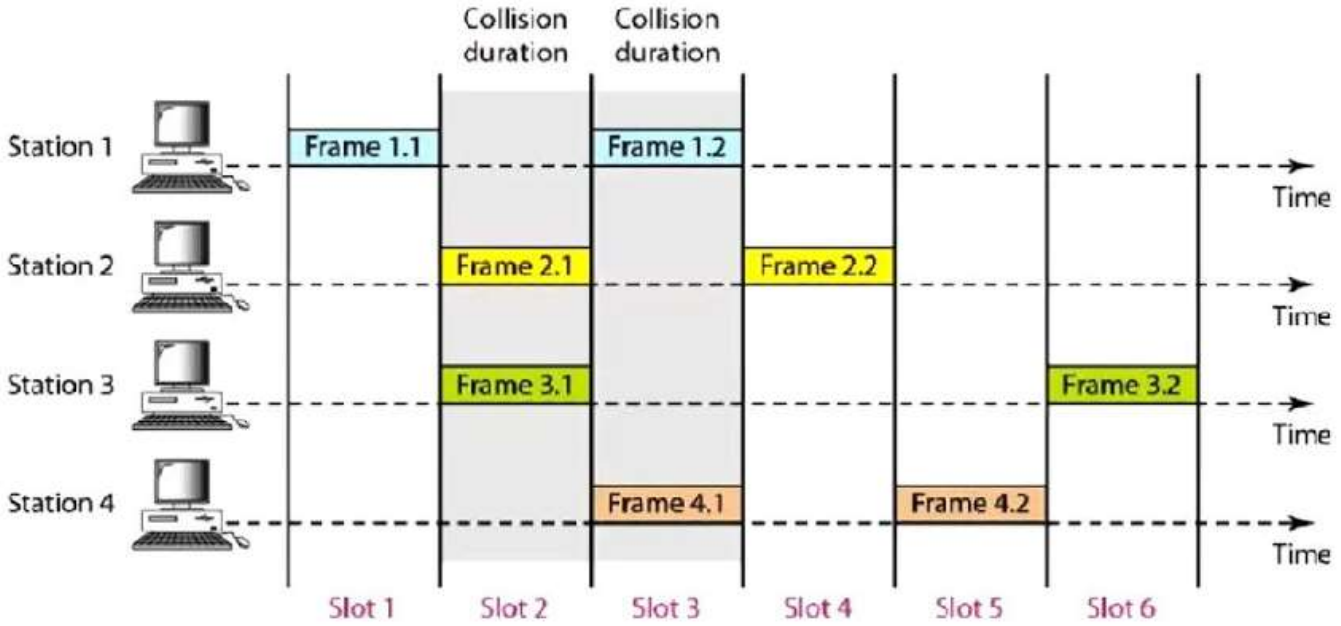
• This approach requires the users to agree on slot boundaries.

• One way to achieve synchronization would be to have one special station emit a pip at the start of each interval, like a clock.

• In Roberts' method, which has come to be known as slotted ALOHA, in contrast to Abramson's pure ALOHA

• A computer is not permitted to send whenever a carriage return is typed.

• Instead, it is required to wait for the beginning of the next slot. Thus, the continuous pure ALOHA is turned 77 into a discrete one


Collision duration
Collision duration
Station 1
Station 2
Station 3
Station 4
Frame 1.1
Frame 1.2
Frame 2.1
Frame 2.2
Frame 3.1
Frame 3.2
Frame 4.1
Frame 4.2
Time
Time
Time
Time
Slot 1
Slot 2
Slot 3
Slot 4
Slot 5
Slot 6

CSMA

- In this section we will discuss some protocols for improving performance
- Protocols in which stations listen for a carrier (i.e., a transmission) and act accordingly are called carrier sense protocols
- A number of them have been proposed
- Kleinrock and Tobagi (1975) have analysed several such protocols in detail
- Below we will mention several versions of the carrier sense protocols

- 1- Persistent CSMA
- Non – Persistent CSMA
- P – Persistent CSMA

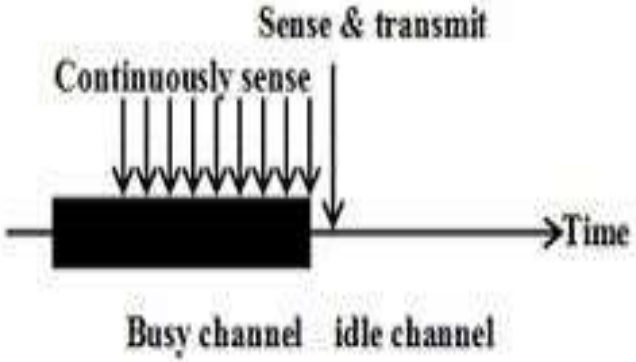
1-persistent CSMA

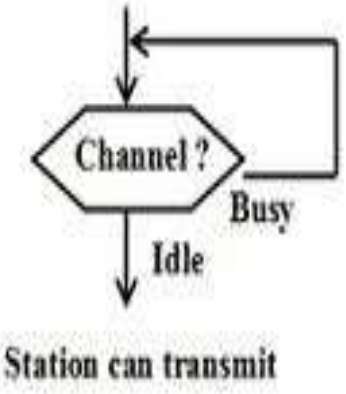
• When a station has data to send, it first listens to the channel to see if anyone else is transmitting at that moment.

• If the channel is busy, the station waits until it becomes idle. When the station detects an idle channel, it transmits a frame.

• If a collision occurs, the station waits a random amount of time and starts all over again.

• The protocol is called 1- persistent because the station transmits with a probability of 1 when it finds the channel idle





1-persistent CSMA

Non-persistent CSMA

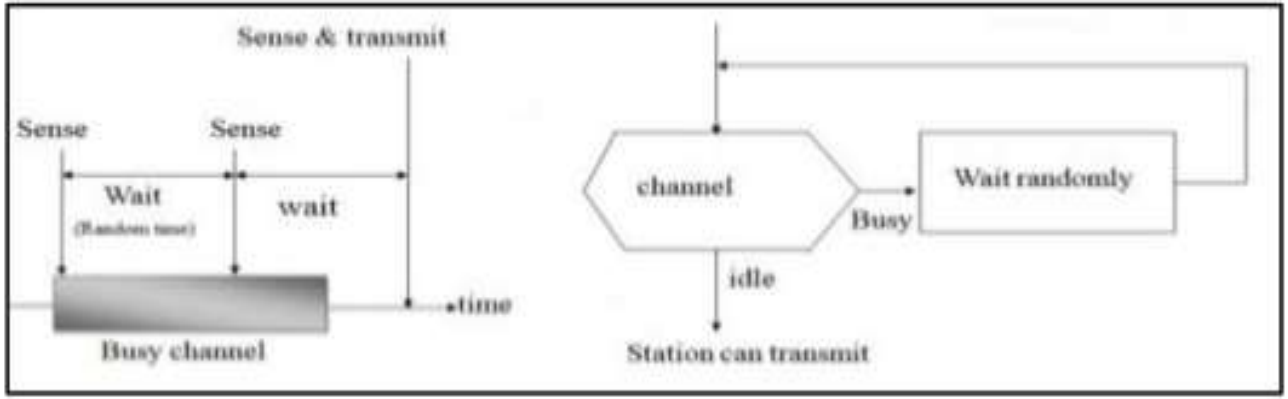
• A second carrier sense protocol is non-persistent CSMA.

• In this protocol, a conscious attempt is made to be less greedy than in the previous one. Before sending, a station senses the channel.

• If no one else is sending, the station begins doing so itself.

• However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission.

• Instead, it waits a random period of time and then repeats the algorithm. Consequently, this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA



- This approach **reduces collision**, results in overall **higher medium throughput** but with a **penalty of longer initial delay** compared to 1–persistent.

P-persistent CSMA

• The last protocol is p-persistent CSMA. It applies to slotted channels and works as follows.

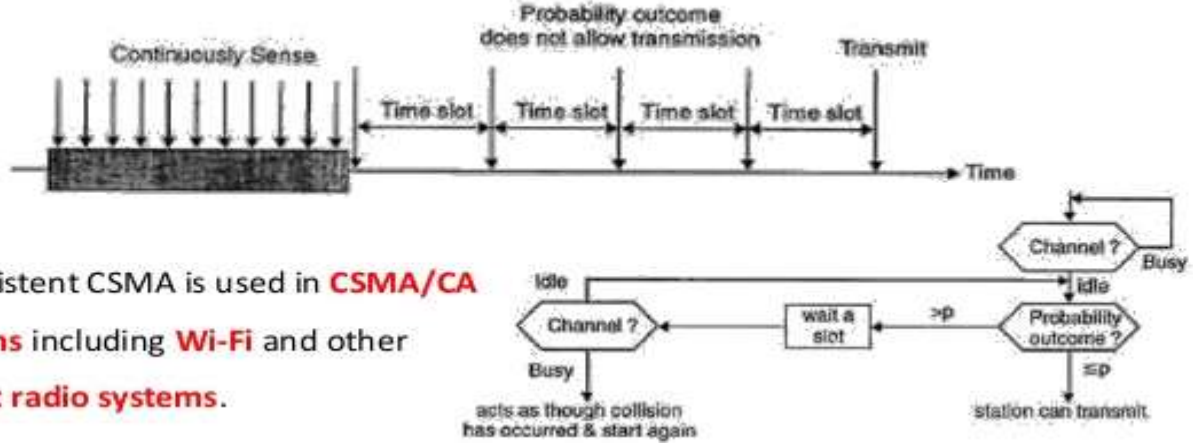
• When a station becomes ready to send, it senses the channel. If it is idle, it transmits with a probability p.

• With a probability q = 1 - p, it defers until the next slot. If that slot is also idle, It either transmits or defers again, with probabilities p and q.

• This process is repeated until either the frame has been transmitted or another station has begun transmitting.

• In the latter case, the unlucky station acts as if there had been a collision (i.e., it waits a random time and starts again).

• If the station initially senses the channel busy, it waits until the next slot and applies the above algorithm



- P-Persistent CSMA is used in **CSMA/CA systems** including **Wi-Fi** and other **packet radio systems**.

Computer Networks

CSMA

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : CSMA

Computer Networks: MCA, I Year/II-Sem.

Outline

- Introduction to CSMA
- 1-Persistent CSMA
- Non-Persistent CSMA
- P-Persistent CSMA
- CSMA/CD
- CSMA/CA

CSMA

- In this section we will discuss some protocols for improving performance
- Protocols in which stations listen for a carrier (i.e., a transmission) and act accordingly are called carrier sense protocols
- A number of them have been proposed
- Kleinrock and Tobagi (1975) have analysed several such protocols in detail
- Below we will mention several versions of the carrier sense protocols

- 1- Persistent CSMA
- Non – Persistent CSMA
- P – Persistent CSMA

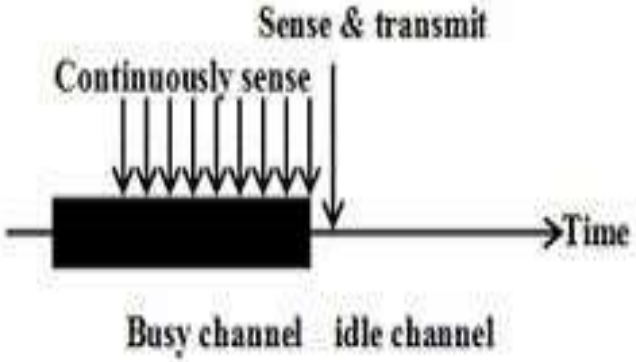
1-persistent CSMA

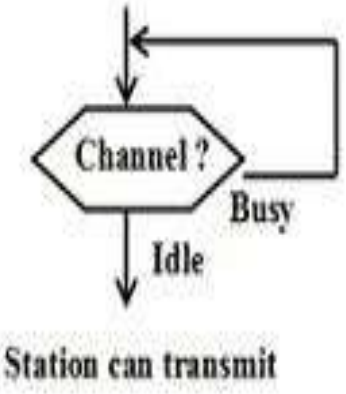
• When a station has data to send, it first listens to the channel to see if anyone else is transmitting at that moment.

• If the channel is busy, the station waits until it becomes idle. When the station detects an idle channel, it transmits a frame.

• If a collision occurs, the station waits a random amount of time and starts all over again.

• The protocol is called 1- persistent because the station transmits with a probability of 1 when it finds the channel idle





1-persistent CSMA

Non-persistent CSMA

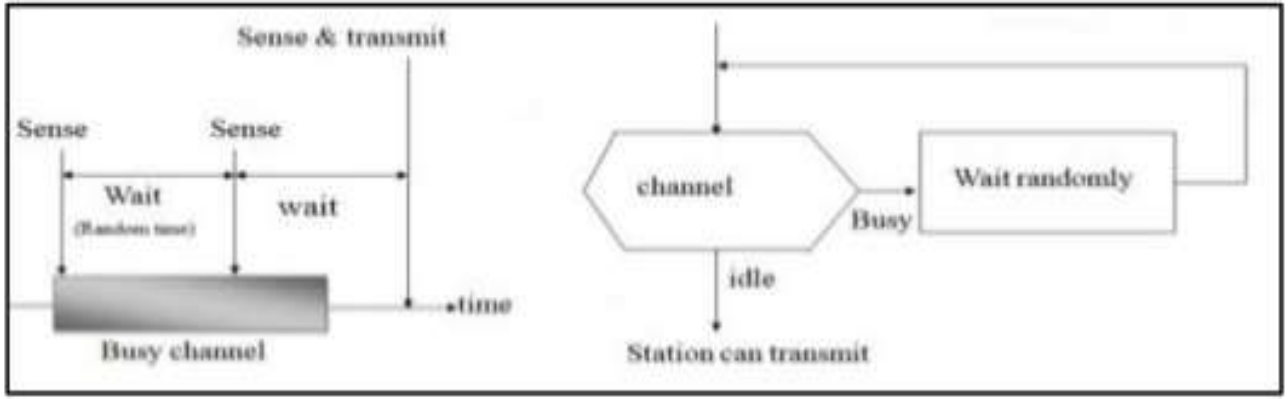
• A second carrier sense protocol is non-persistent CSMA.

• In this protocol, a conscious attempt is made to be less greedy than in the previous one. Before sending, a station senses the channel.

• If no one else is sending, the station begins doing so itself.

• However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission.

• Instead, it waits a random period of time and then repeats the algorithm. Consequently, this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA



- This approach **reduces collision**, results in overall **higher medium throughput** but with a **penalty of longer initial delay** compared to 1–persistent.

P-persistent CSMA

• The last protocol is p-persistent CSMA. It applies to slotted channels and works as follows.

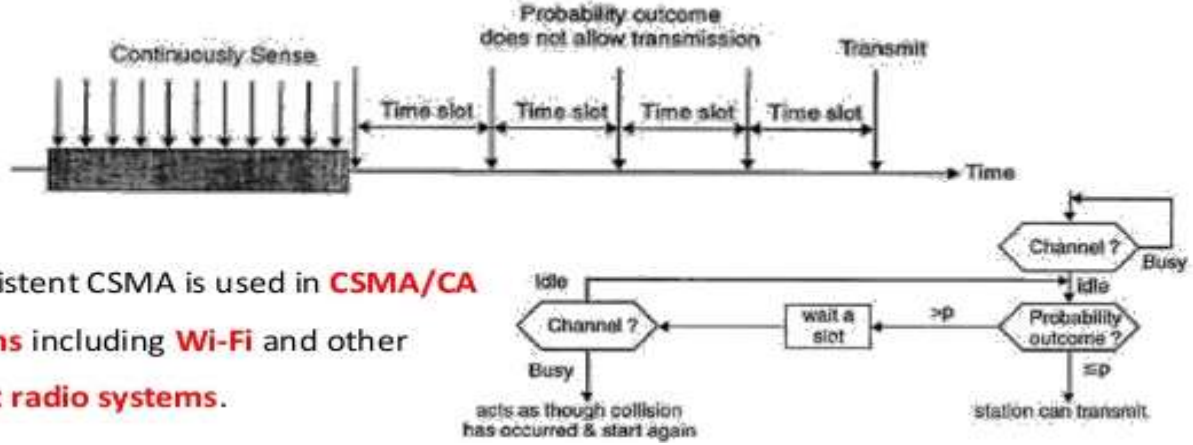
• When a station becomes ready to send, it senses the channel. If it is idle, it transmits with a probability p.

• With a probability q = 1 - p, it defers until the next slot. If that slot is also idle, It either transmits or defers again, with probabilities p and q.

• This process is repeated until either the frame has been transmitted or another station has begun transmitting.

• In the latter case, the unlucky station acts as if there had been a collision (i.e., it waits a random time and starts again).

• If the station initially senses the channel busy, it waits until the next slot and applies the above algorithm



- P-Persistent CSMA is used in **CSMA/CA systems** including **Wi-Fi** and other **packet radio systems**.

CSMA/CD

• This protocol, known as CSMA/CD (CSMA with Collision Detection) is widely used on LANs in the MAC sub layer.

• In particular, it is the basis of the popular Ethernet LAN, so it is worth devoting some time to looking at it in detail.

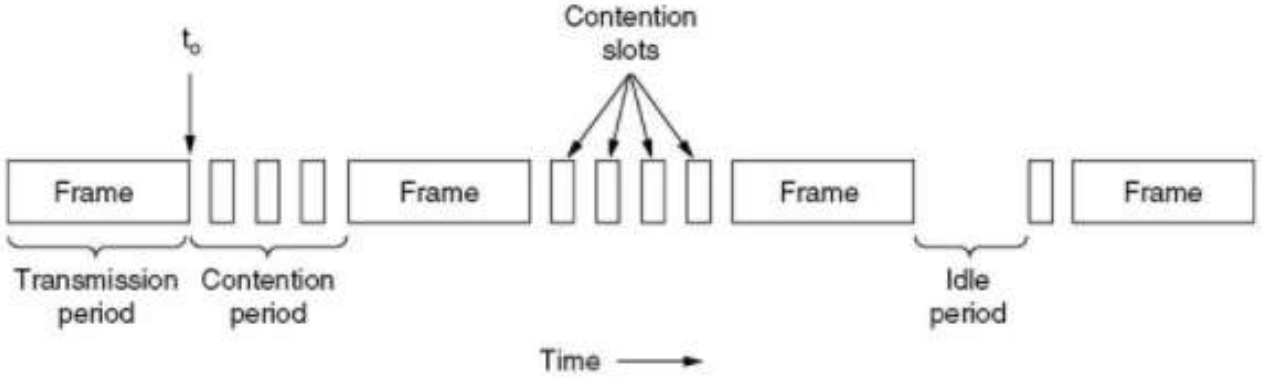
• CSMA/CD, as well as many other LAN protocols, uses the conceptual model

• At the point marked t0, a station has finished transmitting its frame.

• Any other station having a frame to send may now attempt to do so.

• If two or more stations decide to transmit simultaneously, there will be a collision.

• Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal


Contention slots
t_o
Frame
Frame
Frame
Frame
Transmission period
Contention period
Idle period
Time

• After a station detects a collision, it aborts its transmission, waits a random period of time, and then tries again, assuming that no other station has started transmitting in the meantime.

• Therefore, our model for CSMA/CD will consist of alternating contention and transmission periods, with idle periods occurring when all stations are quiet

• Now let us look closely at the details of the contention algorithm

• Suppose that two stations both begin transmitting at exactly time t0

• How long will it take them to realize that there has been a collision

• The answer to this question is vital to determining the length of the contention period and hence what the delay and throughput will be

• The minimum time to detect the collision is then just the time it takes the signal to propagate from one station to the other

CSMA/CA

- CSMA/CA stands for **Carrier Sense Multiple Access** with **Collision Avoidance**
- It means that it is a network protocol that uses to avoid a collision rather than allowing it to occur, and it does not deal with the recovery of packets after a collision
- It is similar to the CSMA CD protocol that operates in the media access control layer
- In CSMA CA, whenever a station sends a data frame to a channel, it checks whether it is in use
- If the shared channel is busy, the station waits until the channel enters idle mode

S. No	CSMA CD	CSMA CA
1.	It is the type of CSMA to detect the collision on a shared channel.	It is the type of CSMA to avoid collision on a shared channel.
2.	It is the collision detection protocol.	It is the collision avoidance protocol.
3.	It is used in 802.3 Ethernet network cable.	It is used in the 802.11 Ethernet network.
4.	It works in wired networks.	It works in wireless networks.
5.	It is effective after collision detection on a network.	It is effective before collision detection on a network.
6.	Whenever a data packet conflicts in a shared channel, it resends the data frame.	Whereas the CSMA CA waits until the channel is busy and does not recover after a collision.
7.	It minimizes the recovery time.	It minimizes the risk of collision.
8.	The efficiency of CSMA CD is high as compared to CSMA.	The efficiency of CSMA CA is similar to CSMA.
9.	It is more popular than the CSMA CA protocol.	It is less popular than CSMA CD.

Computer Networks

Collision free Protocols

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Collision free Protocols

Computer Networks: MCA, I Year/II-Sem.

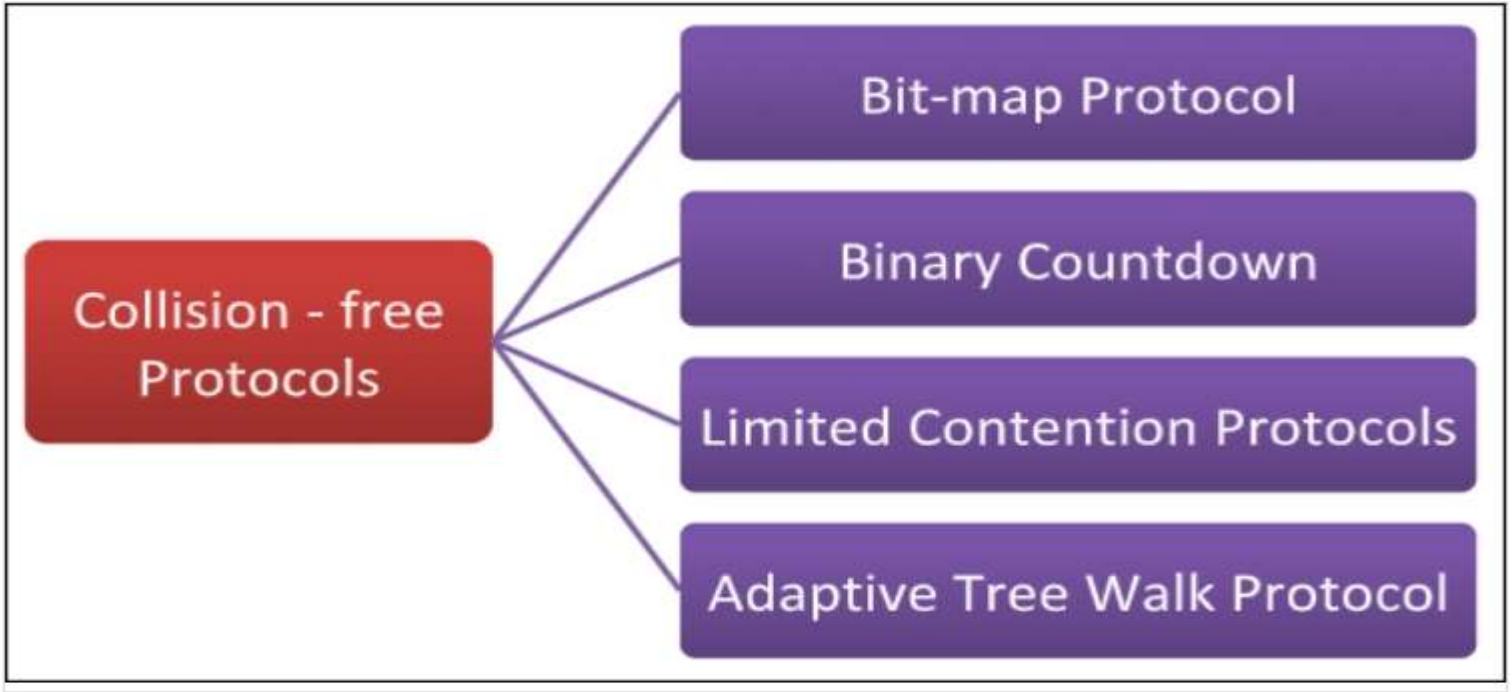
Outline

- Introduction to Collision Free Protocols
- Bit-map Protocol
- Binary-Countdown
- CSMA/CD
- CSMA/CA

Collision free Protocols

- Collisions adversely affect the system performance, especially when the cable is long and the frames are short
- And CSMA/CD is not universally applicable
- In this section, we will examine some protocols that resolve the contention for the channel without any collisions at all, not even during the contention period.
- Most of these are not currently used in major systems, but in a rapidly changing field, having some protocols with excellent properties available for future systems is often a good thing

Types of Collision free Protocols



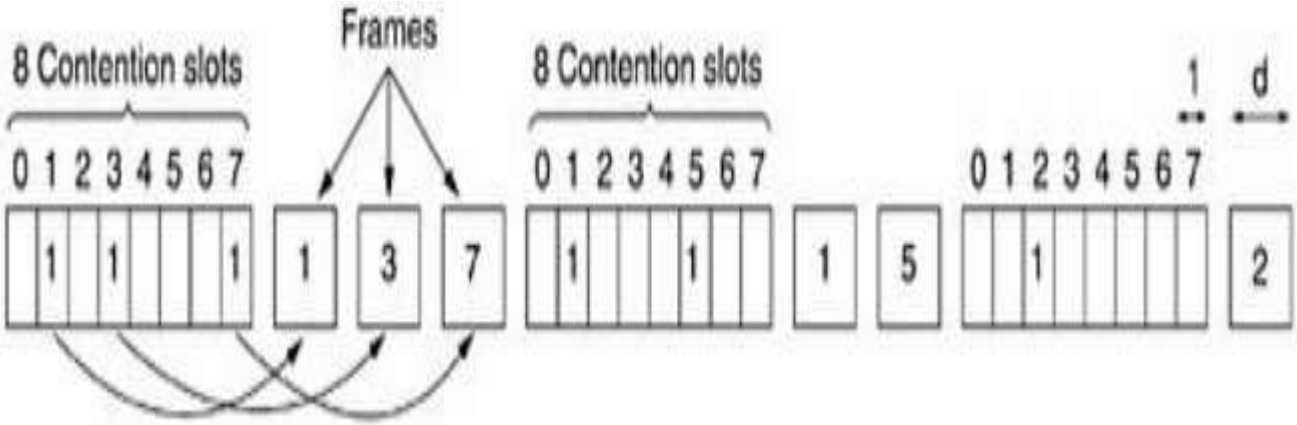
Bit-Map Protocol

• In this collision-free protocol, the basic bit-map method, each contention period consists of exactly N slots.

• If station 0 has a frame to send, it transmits a 1 bit during the zeroth slot.

• No other station is allowed to transmit during this slot.

• Regardless of what station 0 does, station 1 gets the opportunity to transmit a 1 during slot 1, but only if it has a frame queued



Transmission of frames in Bit-Map Protocol

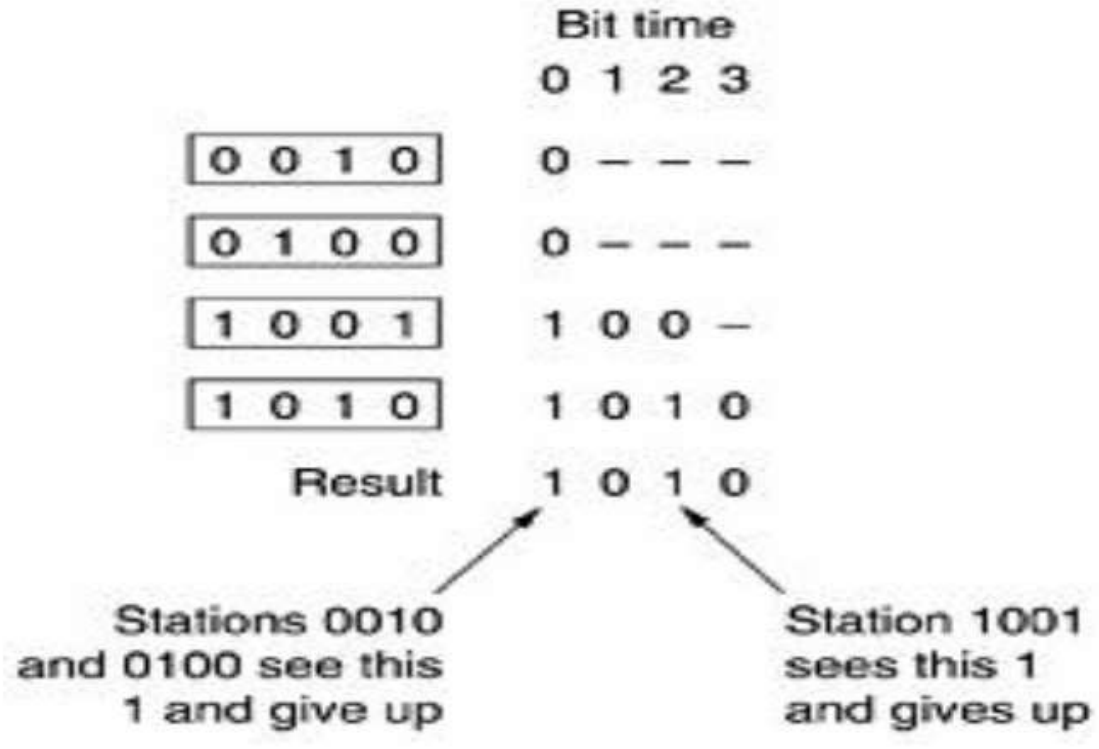
Binary-Countdown

•A problem with the basic bit-map protocol is that the overhead is 1 bit per station, so it does not scale well to networks with thousands of stations

• We can do better than that by using binary station addresses.

• A station wanting to use the channel now broadcasts its address as a binary bit string, starting with the high-order bit

• All addresses are assumed to be the same length

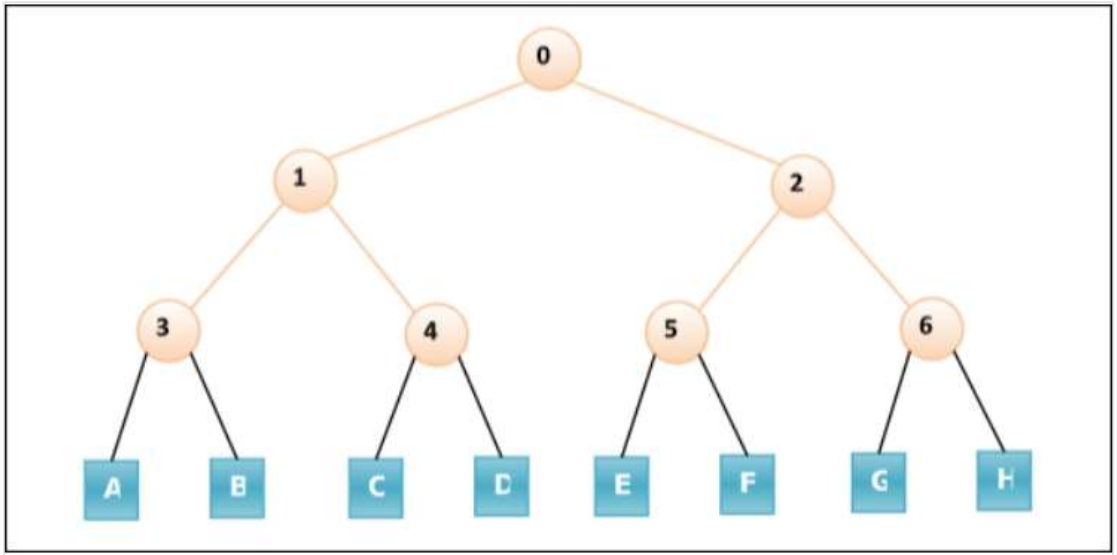

Bit time
0 1 2 3
0 0 1 0
0 – – –
0 1 0 0
0 – – –
1 0 0 1
1 0 0 –
1 0 1 0
1 0 1 0
Result
1 0 1 0
Stations 0010 and 0100 see this 1 and give up
Station 1001 sees this 1 and gives up

Limited Contention Protocols

- These protocols combines the advantages of collision based protocols and collision free protocols
- Under light load, they behave like ALOHA scheme.
- Under heavy load, they behave like bitmap protocols

Adaptive Tree Walk Protocol

In adaptive tree walk protocol, the stations or nodes are arranged in the form of a binary tree as follows -



•Initially all nodes (A, B ……. G, H) are permitted to compete for the channel

• If a node is successful in acquiring the channel, it transmits its frame

•In case of collision, the nodes are divided into two groups (A, B, C, D in one group and E, F, G, H in another group). Nodes belonging to only one of them is permitted for competing

•This process continues until successful transmission occurs.

Computer Networks

IEEE Standards

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : IEEE Standards

Computer Networks: MCA, I Year/II-Sem.

Outline

- Introduction
- Ethernet Evolution
- 802.11
- Bluetooth

IEEE Standards

• In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers.

• Project 802 does not seek to replace any part of the OSI or the Internet model. Instead, it is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

• The standard was adopted by the American National Standards Institute (ANSI). In 1987, the International Organization for Standardization (ISO) also approved it as an international standard under the designation ISO 8802. The relationship of the 802 Standard to the traditional OSI model

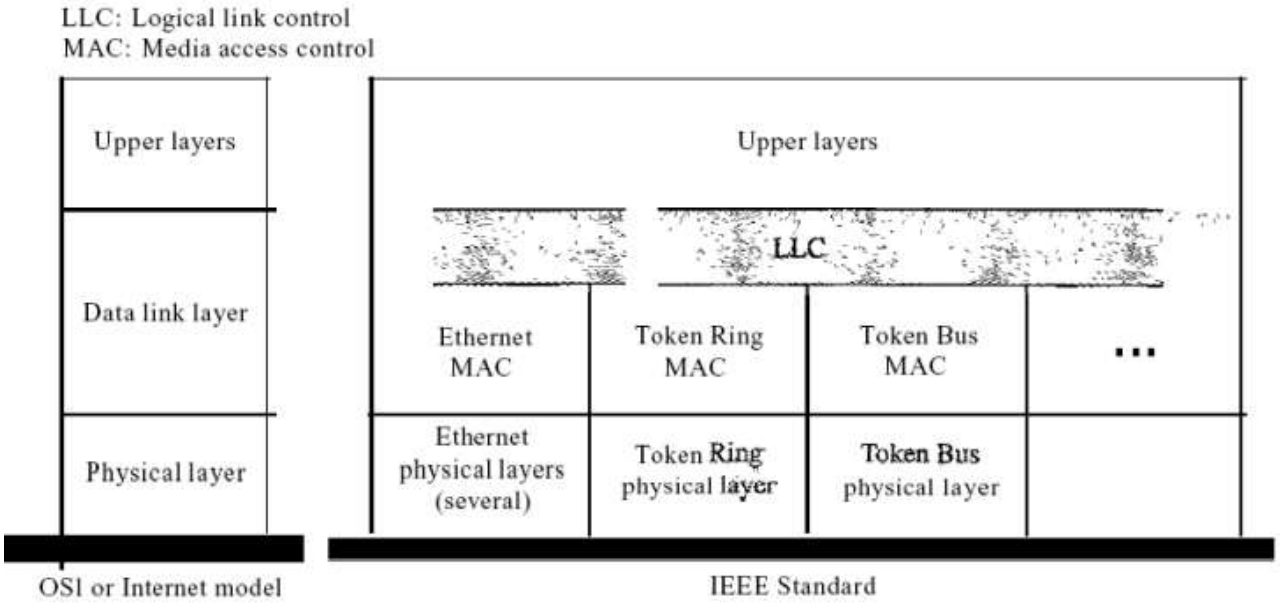


Figure 1 *IEEE standardfor LANs*

Logical Link Control

• Data Link Layer As we mentioned before, the data link layer in the IEEE standard is divided into two sub-layers:

• LLC and MAC.

Logical Link Control (LLC) We said that data link control handles framing, flow control, and error control.

In IEEE Project 802, flow control, error control,and part of the framing duties are collected into one sublayer called the logical link control. Framing is handled in both the LLC sublayer and the MAC sublayer.

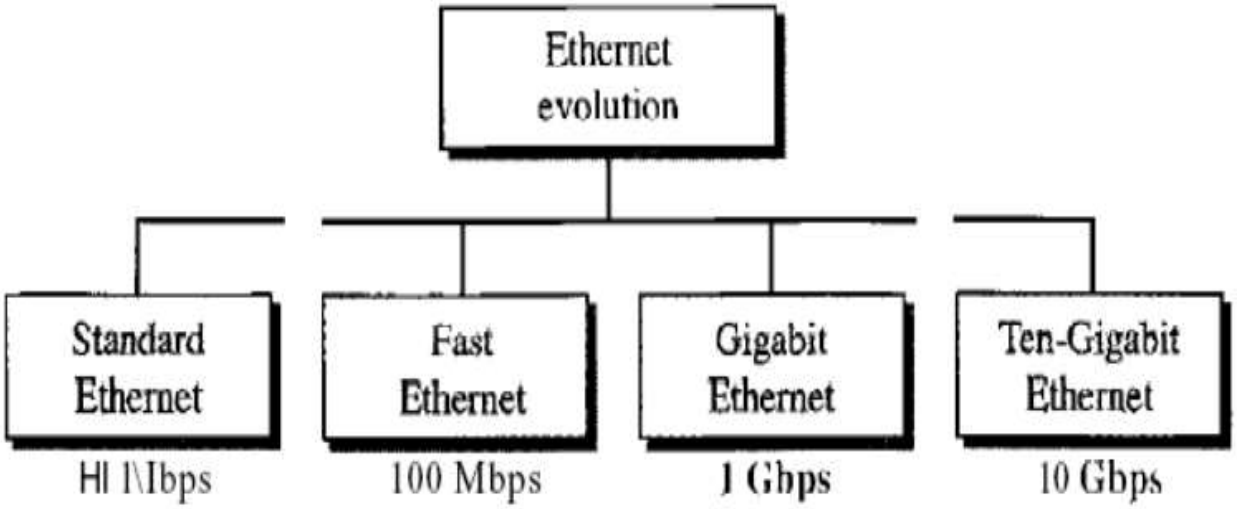
Media Access Control

- Media Access Control (MAC) IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN.
- For example, it defines CSMA/CD as the media access method for Ethernet LANs and the token passing method for Token Ring and Token Bus LANs.
- As we discussed in the previous section, part of the framing function is also handled by the MAC layer. In contrast to the LLC sublayer, the MAC sublayer contains a number of distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol

Physical Layer

- Physical Layer The physical layer is dependent on the implementation and type of physical media used.
- IEEE defines detailed specifications for each LAN implementation.
- For example, although there is only one MAC sublayer for Standard Ethernet, there is a different physical layer specifications for each Ethernet implementation

Ethernet Evolution



IEEE 802.11

The standard defines two kinds of services:

1. Basic service set (BSS) and the
2. Extended service set (ESS).

Basic Service Set IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN.

A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).

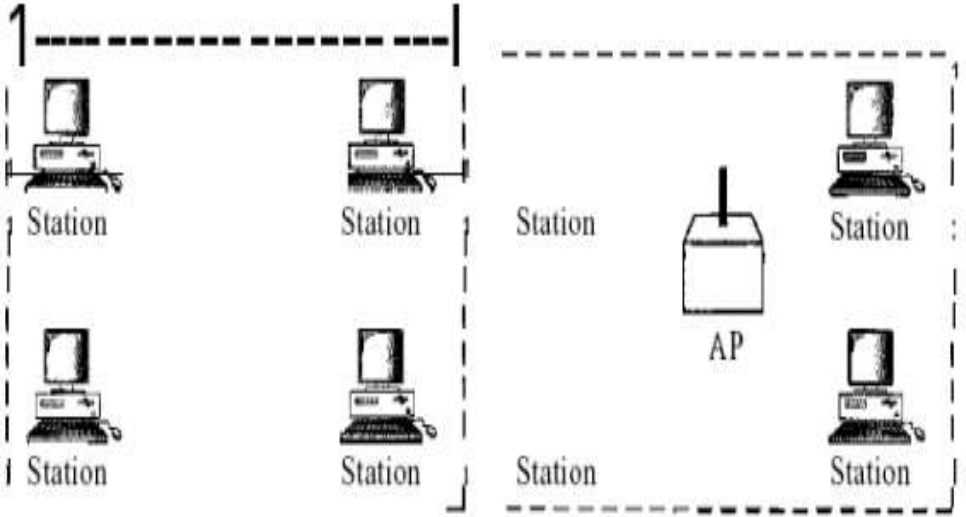
Figure 9 shows two sets in this standard.

The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture.

In this architecture, stations can form a network without the need of an 89 AP; they can locate one another and agree to be part of a BSS.

A BSS with an AP is sometimes referred to as an infrastructure network

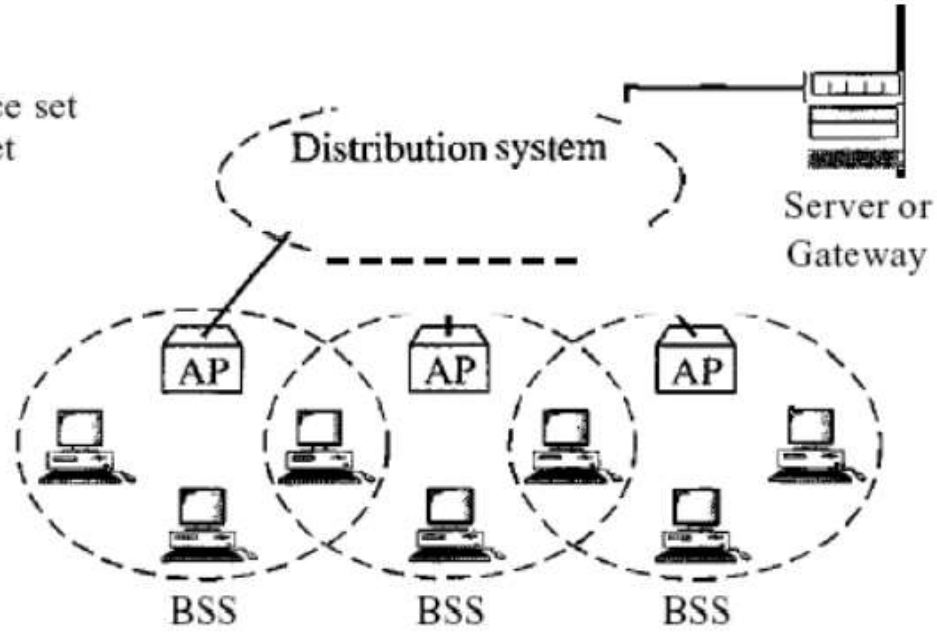
BSS: Basic service set
AP: Access point



Extended Service Set

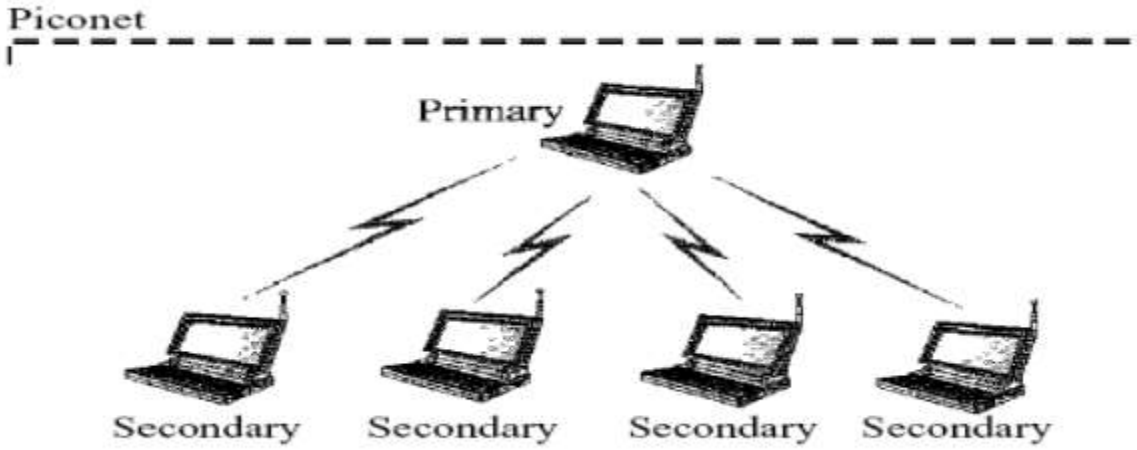
- An extended service set (ESS) is made up of two or more BSSs with APs.
- In this case, the BSSs are connected through a distribution system, which is usually a wired LAN. The distribution system connects the APs in the BSSs.
- IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet.
- Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS.
- The stationary stations are AP stations that are part of a wired LAN. Figure 10 shows an ESS

ESS: Extended service set
BSS: Basic service set
AP: Access point



Bluetooth

- Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on.
- A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet.
- A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability. A Bluetooth LAN, by nature, cannot be large. If there are many gadgets that try to connect, there is chaos.


Piconet
Primary
Secondary
Secondary
Secondary
Secondary

- A Bluetooth device has a built-in short-range radio transmitter.
- The current data rate is 1 Mbps with a 2.4-GHz bandwidth.
- This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth LAN

Computer Networks

Routing Algorithms

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Routing Algorithms

Computer Networks: MCA, I Year/II-Sem.

Outline

- What is Routing
- Routing Example
- Classification of Routing Algorithms
- Shortest Path
- Flooding

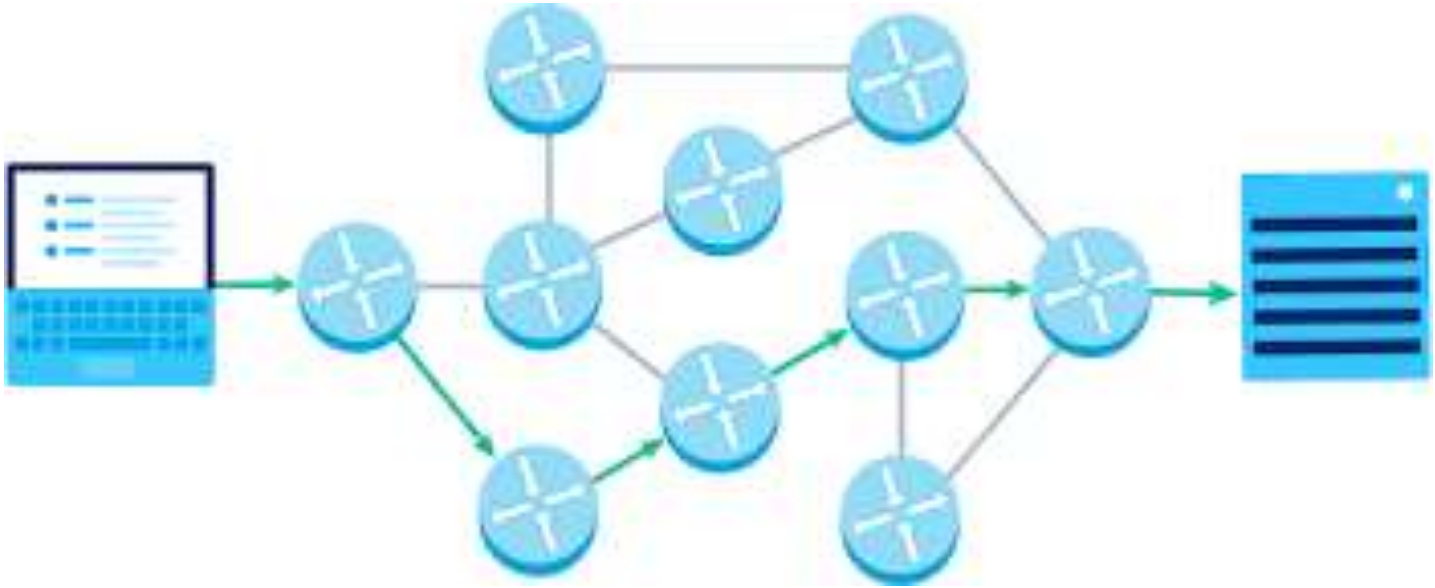
Routing

• **Routing** is the process of selecting best paths in a network

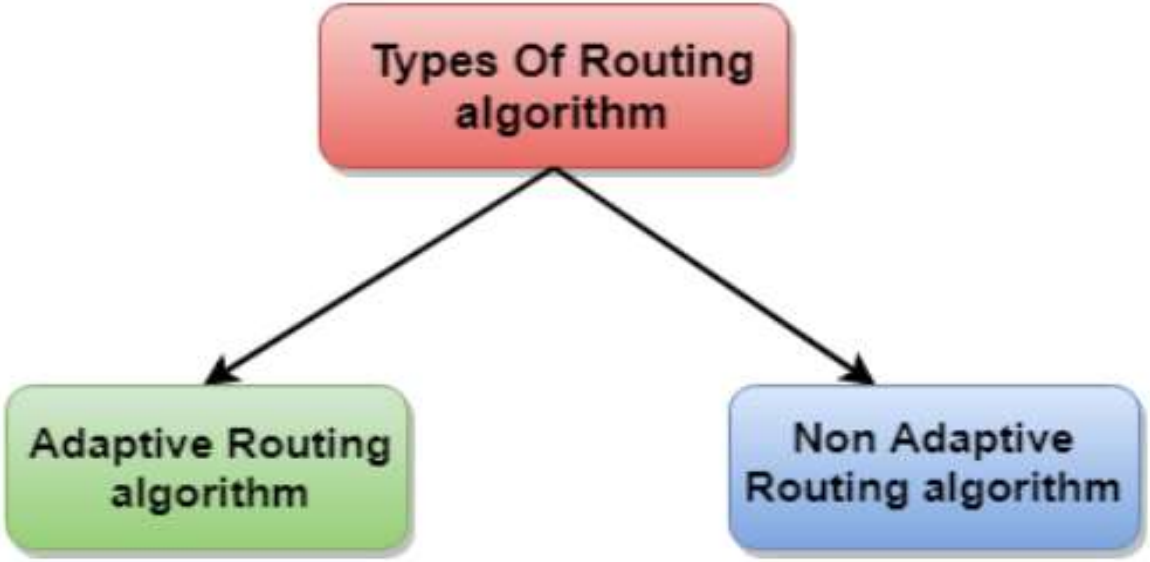
•In the past, the term routing also meant forwarding network traffic among networks

• However, that latter function is better described as forwarding

• Routing is performed for many kinds of networks, including the telephone network (circuit switching), electronic data networks (such as the Internet),and transportation networks



Classification of Routing Algorithms



Adaptive Routing Algorithm

Adaptive algorithm, in contrast, change their routing decisions to reflect changes in the *t*opology, and usually the traffic as well.

Adaptive algorithms differ in

1) Where they get their information (e.g., locally, from adjacent routers, or from all routers)

2) When they change the routes (e.g., every ΔT sec, when the load changes or when the topology changes)

3) What metric is used for optimization (e.g., distance, number of hops, or estimated transit time). This procedure is called dynamic routing

Non-Adaptive Algorithms

- Non-adaptive algorithm do not base their routing decisions on measurements or estimates of the current traffic and topology.
- Instead, the choice of the route to use to get from I to J is computed in advance, off line, and downloaded to the routers when the network is booted.
- This procedure is sometimes called static routing

Different Routing Algorithms

- Shortest path algorithm
- Flooding
- Distance vector routing
- Link state routing
- Hierarchical Routing

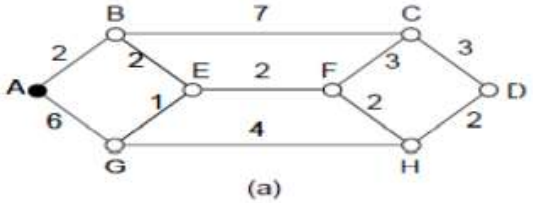
Shortest path algorithm

• The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph representing a communication line or link.

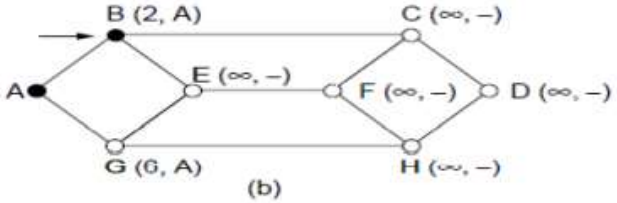
• To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph

1. Start with the local node (router) as the root of the tree. Assign a cost of 0 to this node and make it the first permanent node.
2. Examine each neighbor of the node that was the last permanent node
3. Assign a cumulative cost to each node and make it tentative
4. Among the list of tentative nodes
    a. Find the node with the smallest cost and make it Permanent
    b. If a node can be reached from more than one route then select the route with the shortest cumulative cost.
5. Repeat steps 2 to 4 until every node becomes permanent

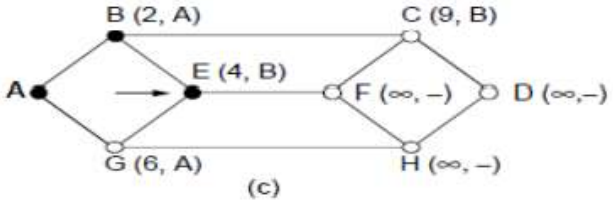
Example



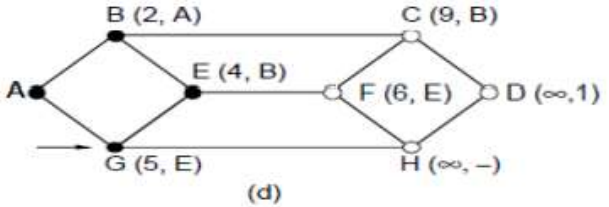
(a)



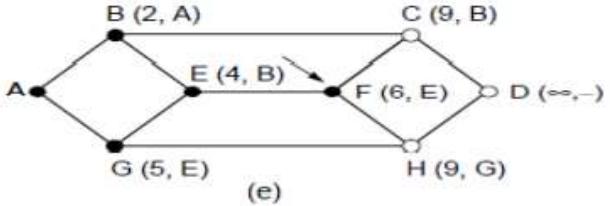
(b)



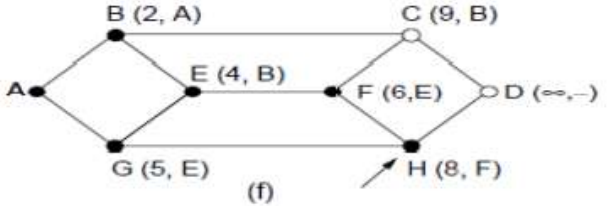
(c)



(d)



(e)



(f)

Flooding

Another static algorithm is flooding, in which every incoming packet is sent out on every outgoing line except the one it arrived on.

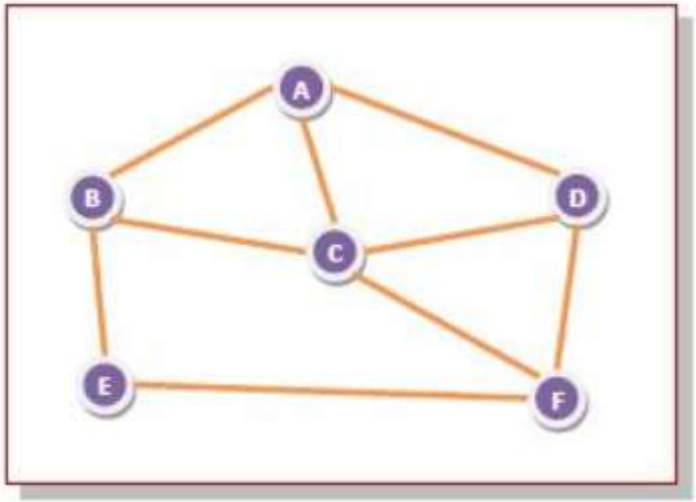
• Flooding obviously generates vast numbers of duplicate packets, in fact, an infinite number unless some measures are taken to damp the process.

• One such measure is to have a hop counter contained in the header of each packet, which is decremented at each hop, with the packet being discarded when the counter reaches zero. Ideally, the hop counter should be initialized to the length of the path from source to destination

• A variation of flooding that is slightly more practical is selective flooding. In this algorithm the routers do not send every incoming packet out on every line, only on those lines that are going approximately in the right direction.

• Flooding is not practical in most applications

Example



Using flooding technique −

An incoming packet to A, will be sent to B, C and D.

B will send the packet to C and E.

C will send the packet to B, D and F.

D will send the packet to C and F.

E will send the packet to F.

F will send the packet to C and E.

Distance Vector Routing Algorithm

• In distance vector routing, the least-cost route between any two nodes is the route with minimum distance.

• In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node.

Mainly 3 things in this

• Initialization

• Sharing

• Updating

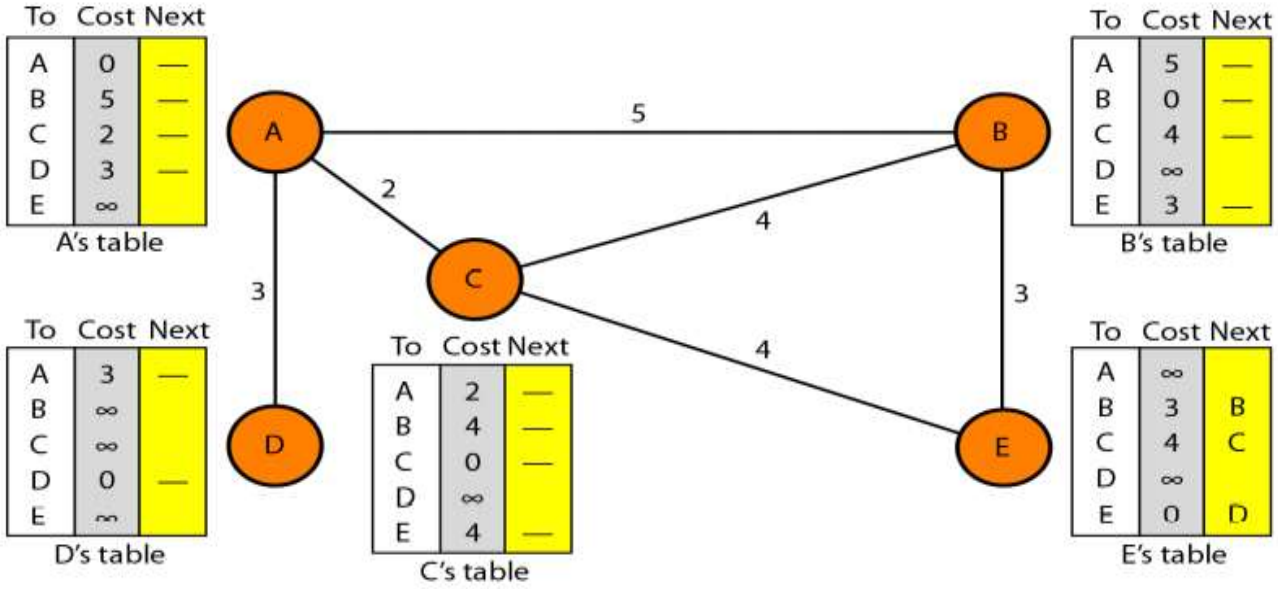
Initialization

• Initialization Each node can know only the distance between itself and its immediate neighbors, those directly connected to it.

• So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors.

• Below fig shows the initial tables for each node.

• The distance for any entry that is not a neighbor is marked as infinite (unreachable)


To Cost Next
A 0 —
B 5 —
C 2 —
D 3 —
E ∞ —
A's table
To Cost Next
A 5 —
B 0 —
C 4 —
D ∞
E 3 —
B's table
To Cost Next
A 3 —
B ∞
C ∞
D 0 —
E ∞
D's table
To Cost Next
A 2 —
B 4 —
C 0 —
D ∞
E 4 —
C's table
To Cost Next
A ∞
B 3 B
C 4 C
D ∞
E 0 D
E's table
A
B
C
D
E
5
2
4
3
3
4

Sharing

• The whole idea of distance vector routing is the sharing of information between neighbors.

• Although node A does not know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E.

• On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C, node C also knows how to reach node D.

• In other words, nodes A and C, as immediate neighbors, can improve their routing tables if they help each other

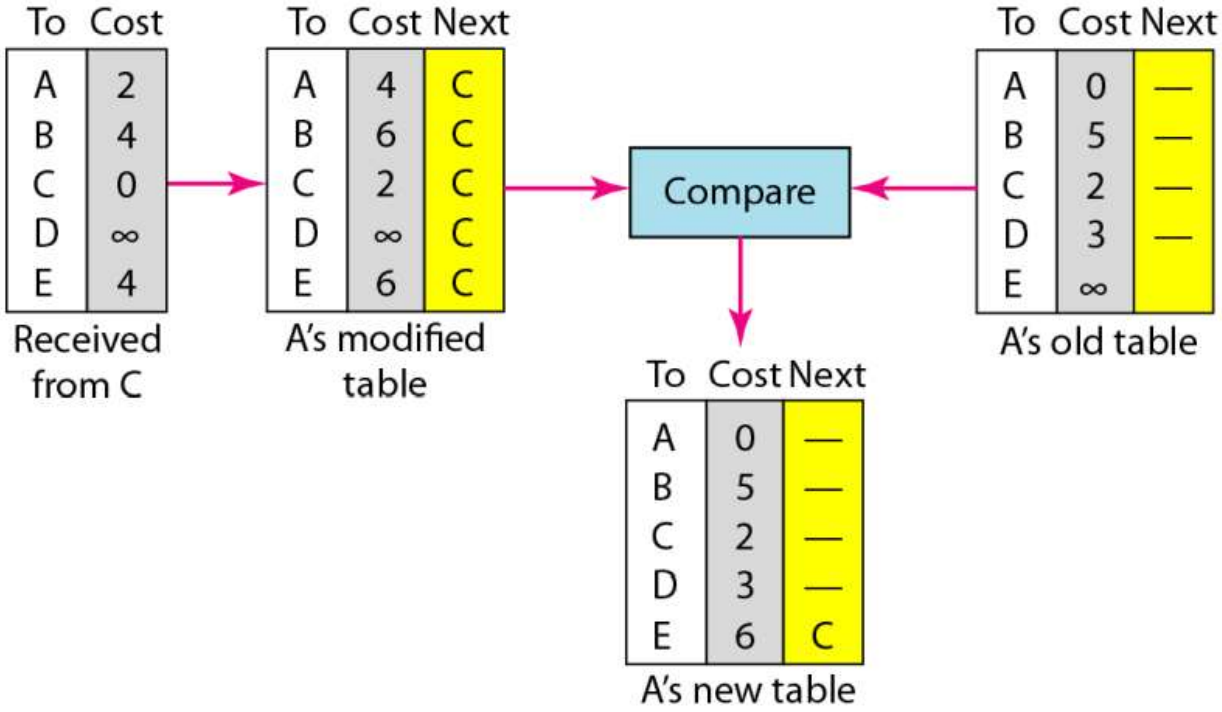
Updating

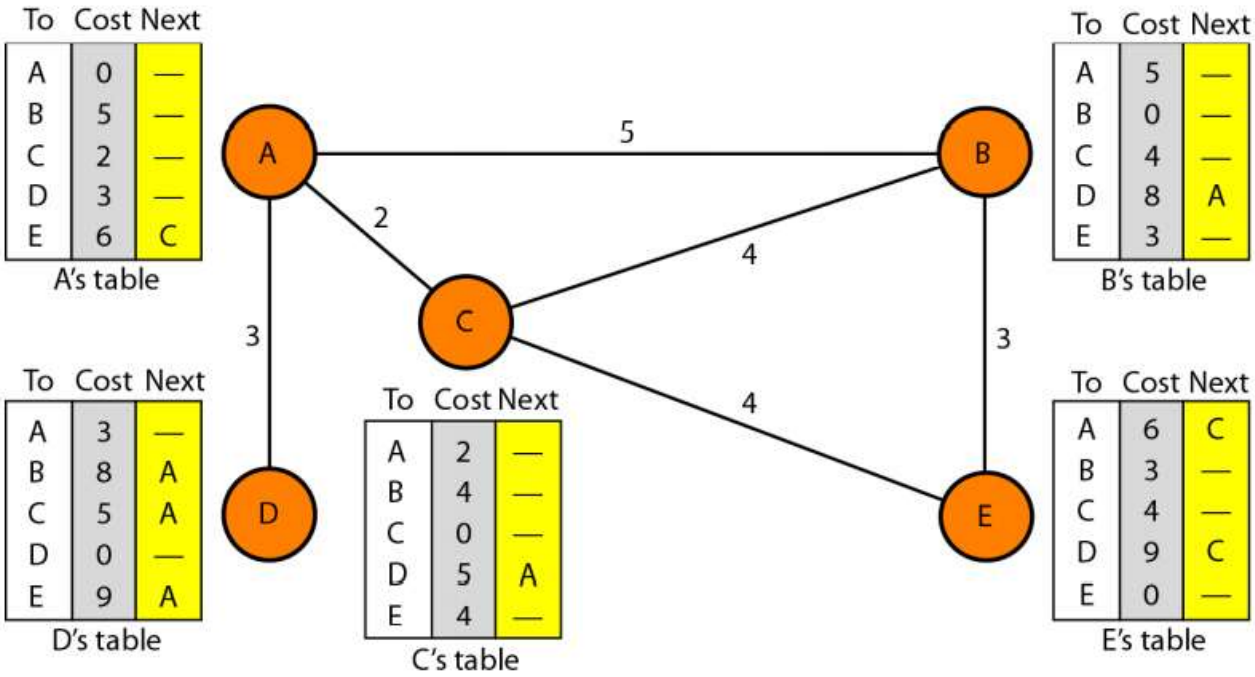
When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps:

1. The receiving node needs to add the cost between itself and the sending node to each value in the second column. (x+y)

2. If the receiving node uses information from any row. The sending node is the next node in the route.

3. The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table. a. If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept. b. If the next-node entry is the same, the receiving node chooses the new row.


To Cost
A 2
B 4
C 0
D ∞
E 4
Received from C
To Cost Next
A 4 C
B 6 C
C 2 C
D ∞ C
E 6 C
A's modified table
Compare
To Cost Next
A 0 —
B 5 —
C 2 —
D 3 —
E ∞
A's old table
To Cost Next
A 0 —
B 5 —
C 2 —
D 3 —
E 6 C
A's new table


To Cost Next
A 0 —
B 5 —
C 2 —
D 3 —
E 6 C
A's table
To Cost Next
A 5 —
B 0 —
C 4 —
D 8 A
E 3 —
B's table
To Cost Next
A 3 —
B 8 A
C 5 A
D 0 —
E 9 A
D's table
To Cost Next
A 2 —
B 4 —
C 0 —
D 5 A
E 4 —
C's table
To Cost Next
A 6 C
B 3 —
C 4 —
D 9 C
E 0 —
E's table
A
B
C
D
E
5
2
4
3
3
4

Computer Networks

ATM LANS

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : ATM LANS

Computer Networks: MCA, I Year/II-Sem.

Outline

- Introduction to ATM
- ATM Cell Format
- ATM Layers

Introduction to ATM

• ATM is a technology that has some event in the development of broadband ISDN in the 1970s and 1980s, which can be considered an evolution of packet switching.

•*Each cell is 53 bytes long* – 5 bytes header and 48 bytes payload. Making an ATM call requires first sending a message to set up a connection.

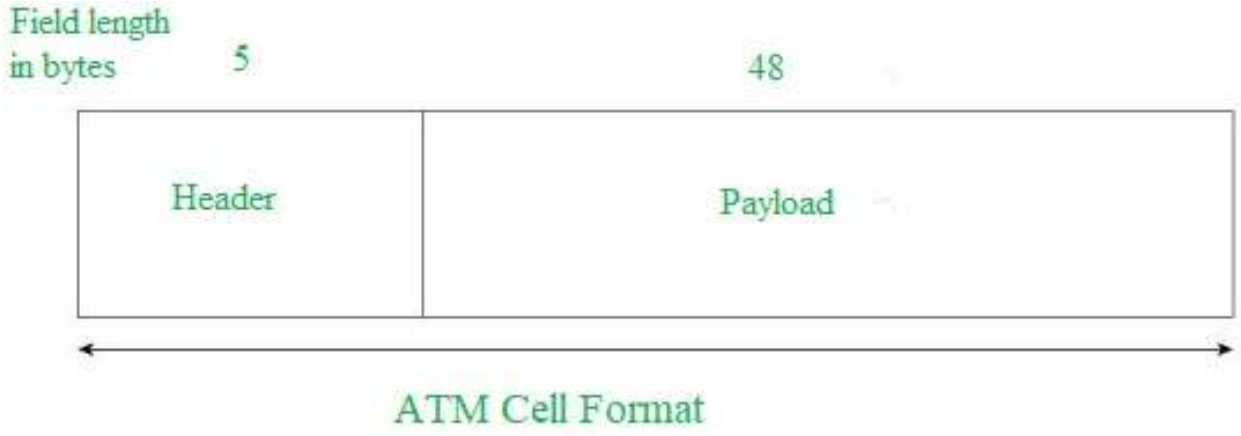
•Thus it can carry multiple types of traffic with **end-to-end** quality of service.

•ATM is independent of a transmission medium, they may be sent on a wire or fiber by themselves or they may also be packaged inside the payload of other carrier systems.

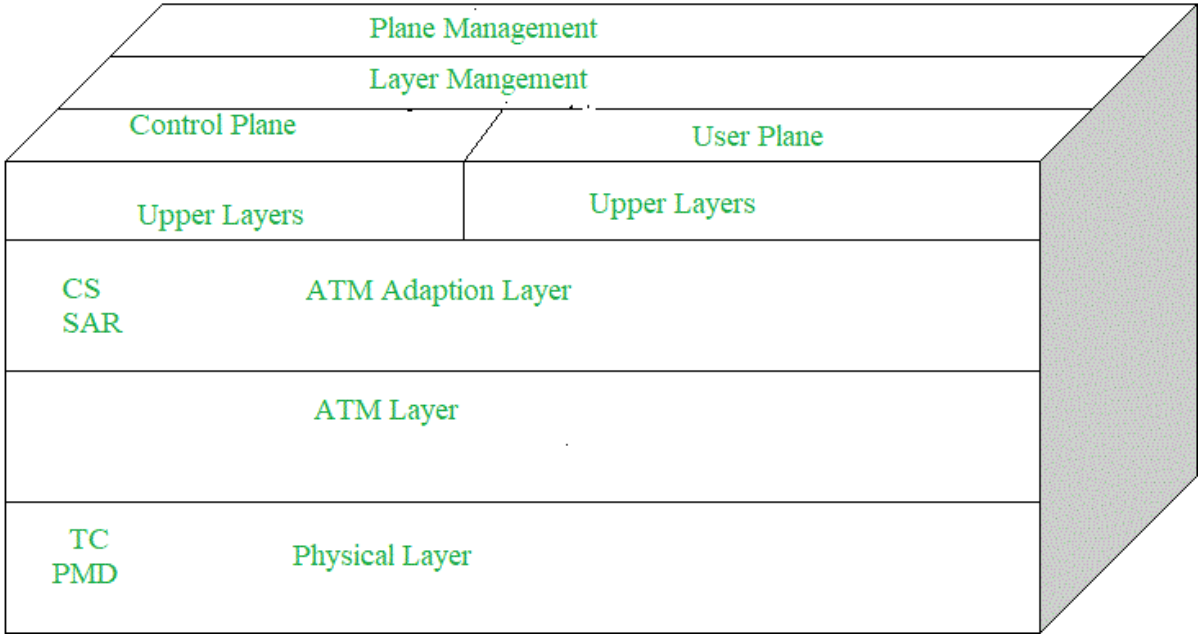
ATM Cell Format

As information is transmitted in ATM in the form of fixed-size units called **cells**.

As known already each cell is 53 bytes long which consists of a 5 bytes header and 48 bytes payload.



ATM Layers


Plane Management
Layer Mangement
Control Plane
User Plane
Upper Layers
Upper Layers
CS
SAR
ATM Adaption Layer
ATM Layer
TC
PMD
Physical Layer

ATM Adaption Layer (AAL) –

It is meant for isolating higher-layer protocols from details of ATM processes and prepares for conversion of user data into cells and segments it into 48-byte cell payloads. AAL protocol excepts transmission from upper-layer services and helps them in mapping applications, e.g., voice, data to ATM cells.

Physical Layer –

It manages the medium-dependent transmission and is divided into two parts physical medium-dependent sublayer and transmission convergence sublayer.

The main functions are as follows:

It converts cells into a bitstream.

It controls the transmission and receipt of bits in the physical medium.

It can track the ATM cell boundaries.

Look for the packaging of cells into the appropriate type of frames.

• **ATM Layer –**

It handles transmission, switching, congestion control, cell header processing, sequential delivery, etc., and is responsible for simultaneously sharing the virtual circuits over the physical link known as cell multiplexing and passing cells through an ATM network known as cell relay making use of the VPI and VCI information in the cell header.

Computer Networks

Internetworking

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Internetworking

Computer Networks: MCA, I Year/II-Sem.

Outline

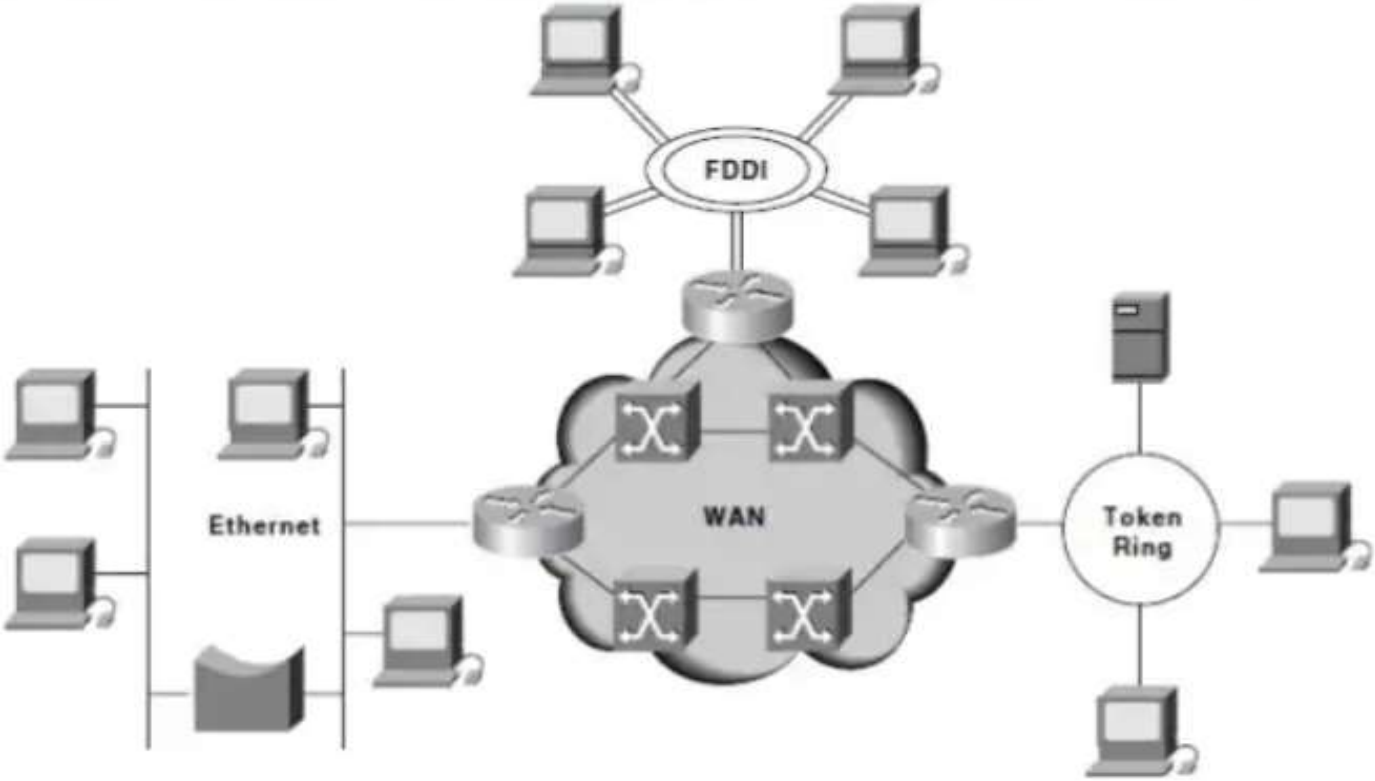
- Internetworking
- Tunneling
- Fragmentation

Internetworking

• **Internetworking** started as a way to connect disparate types of computer networking technology.

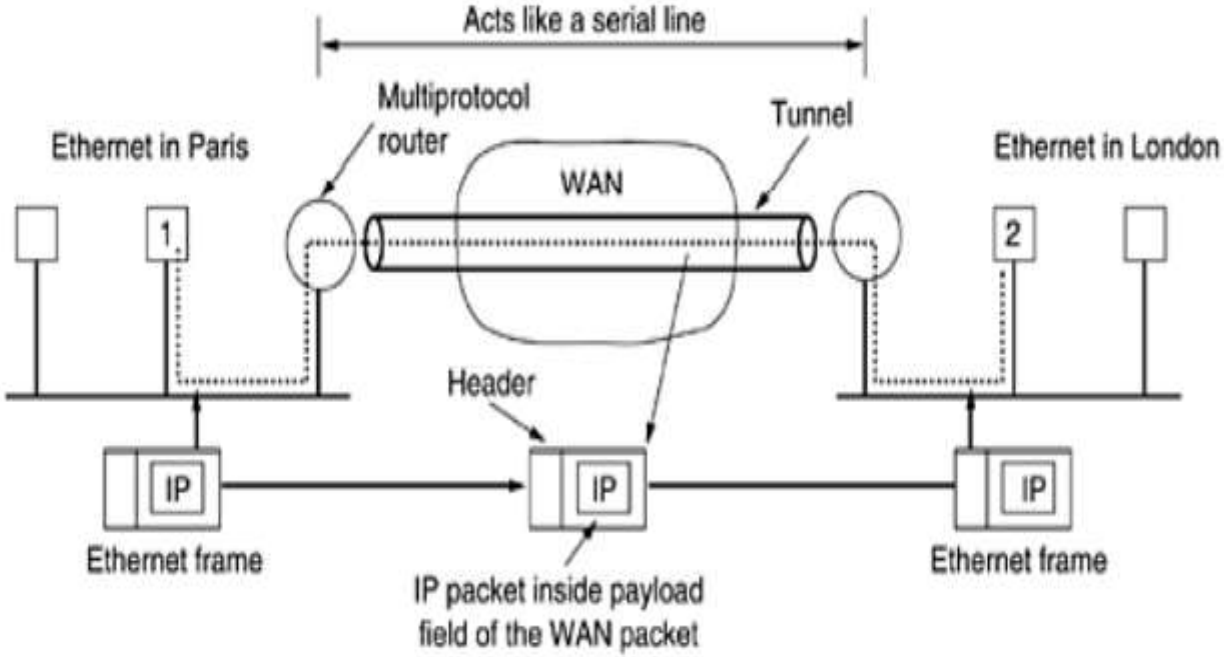
• Computer network term is used to describe two or more computers that are linked to each other.

• When two or more computer LANs or WANs or computer network segments are connected using devices such as a *router* and configure by logical addressing scheme with a protocol such as IP, then it is called as **computer internetworking**.


FDDI
Ethernet
WAN
Token
Ring

Tunneling

- Handling the general case of making two different networks interwork is exceedingly difficult.
- However, there is a common special case that is manageable.
- This case is where the source and destination hosts are on the same type of network, but there is a different network in between.
- As an example, think of an international bank with a TCP/IP-based Ethernet in Paris, a TCP/IP-based Ethernet in London, and a non-IP wide area network (e.g., ATM) in between,


Acts like a serial line
Multiprotocol router
Tunnel
Ethernet in Paris
WAN
Ethernet in London
1
2
Header
IP
IP
IP
Ethernet frame
IP packet inside payload field of the WAN packet
Ethernet frame

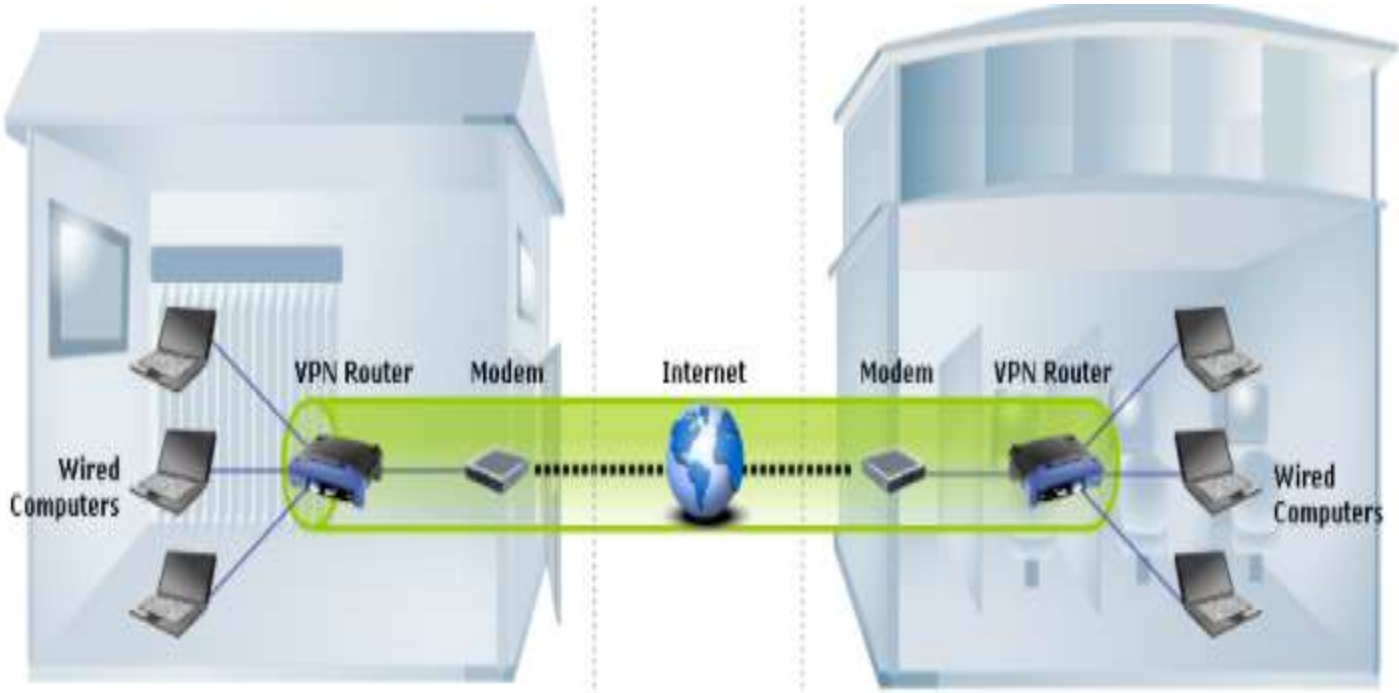
- The solution to this problem is a technique called tunneling.
- To send an IP packet to host 2, host 1 constructs the packet containing the IP address of host 2, inserts it into an Ethernet frame addressed to the Paris multiprotocol router, and puts it on the Ethernet.
- When the multiprotocol router gets the frame, it removes the IP packet, inserts it in the payload field of the WAN network layer packet, and addresses the latter to the WAN address of the London multiprotocol router.
- When it gets there, the London router removes the IP packet and sends it to host 2 inside an Ethernet frame.

• The WAN can be seen as a big tunnel extending from one multiprotocol router to the other.

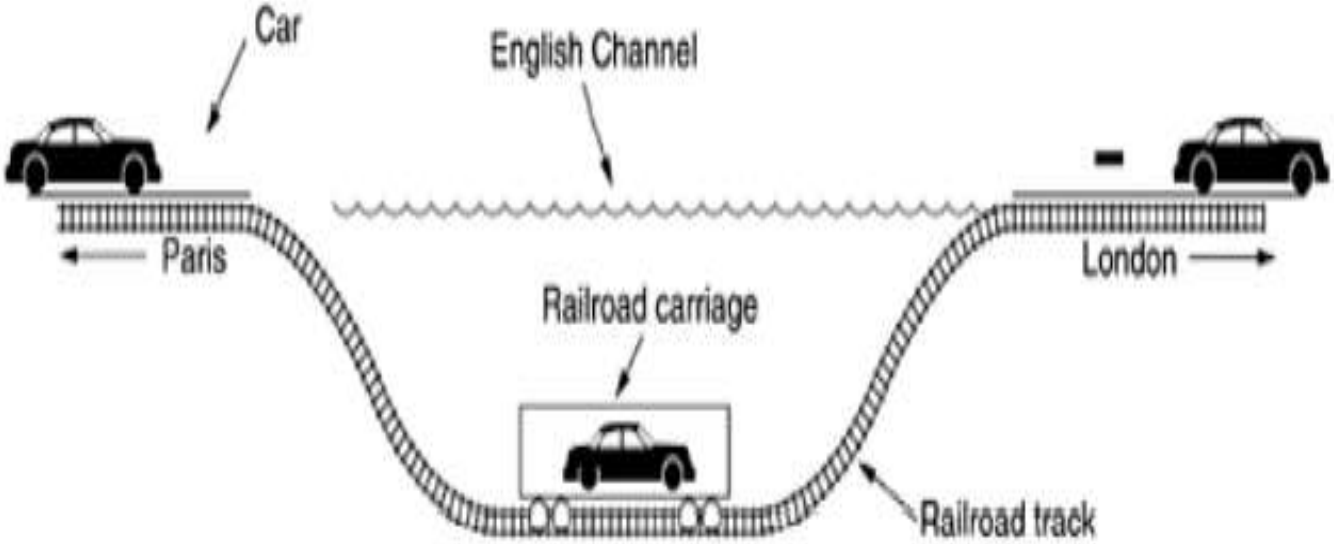
• The IP packet just travels from one end of the tunnel to the other, snug in its nice box. Neither do the hosts on either Ethernet.

• Only the multiprotocol router has to understand IP and WAN packets.

• In effect, the entire distance from the middle of one multiprotocol router to the middle of the other acts like a serial line.


VPN Router
Modem
Internet
Modem
VPN Router
Wired
Computers
Wired
Computers

Example for Tunneling



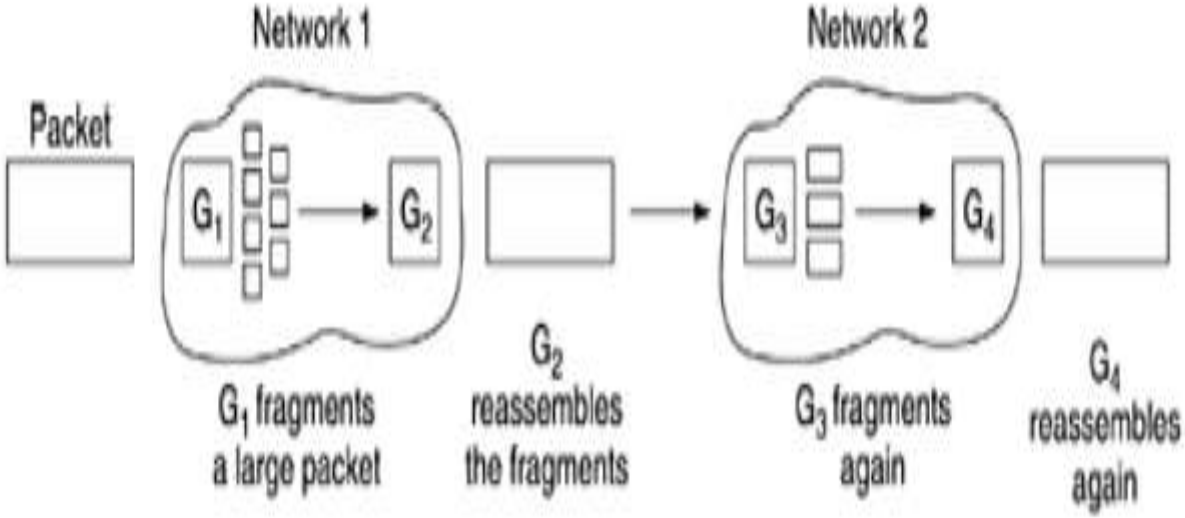
Fragmentation

Each network imposes some maximum size on its packets. These limits have various causes, among them:

1. Hardware (e.g., the size of an Ethernet frame).
2. Operating system (e.g., all buffers are 512 bytes).
3. Protocols (e.g., the number of bits in the packet length field).
4. Compliance with some (inter)national standard.
5. Desire to reduce error-induced retransmissions to some level.
6. Desire to prevent one packet from occupying the channel too long

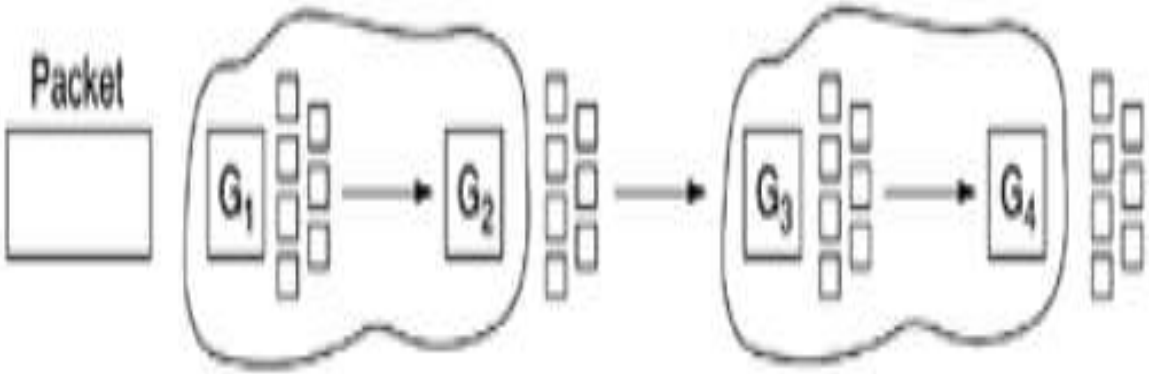
Transparent Fragmentation

- The first strategy is to make fragmentation caused by a "small-packet" network transparent to any subsequent networks through which the packet must pass on its way to the ultimate destination.
- In this approach, the small-packet network has gateways (most likely, specialized routers) that interface to other networks.
- When an oversized packet arrives at a gateway, the gateway breaks it up into fragments. Each fragment is addressed to the same exit gateway, where the pieces are recombined.
- In this way passage through the small-packet network has been made transparent. Subsequent networks are not even aware that fragmentation has occurred


Network 1
Network 2
Packet
G1
G2
G3
G4
G1 fragments a large packet
G2 reassembles the fragments
G3 fragments again
G4 reassembles again

Non-transparent Fragmentation

- The other fragmentation strategy is to refrain from recombining fragments at any intermediate gateways.
- Once a packet has been fragmented, each fragment is treated as though it were an original packet.
- All fragments are passed through the exit gateway.
- Recombination occurs only at the destination host. IP works this way.



G_1 fragments a large packet

The fragments are not reassembled until the final destination (a host) is reached

Computer Networks

Routing Algorithms

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Routing Algorithms

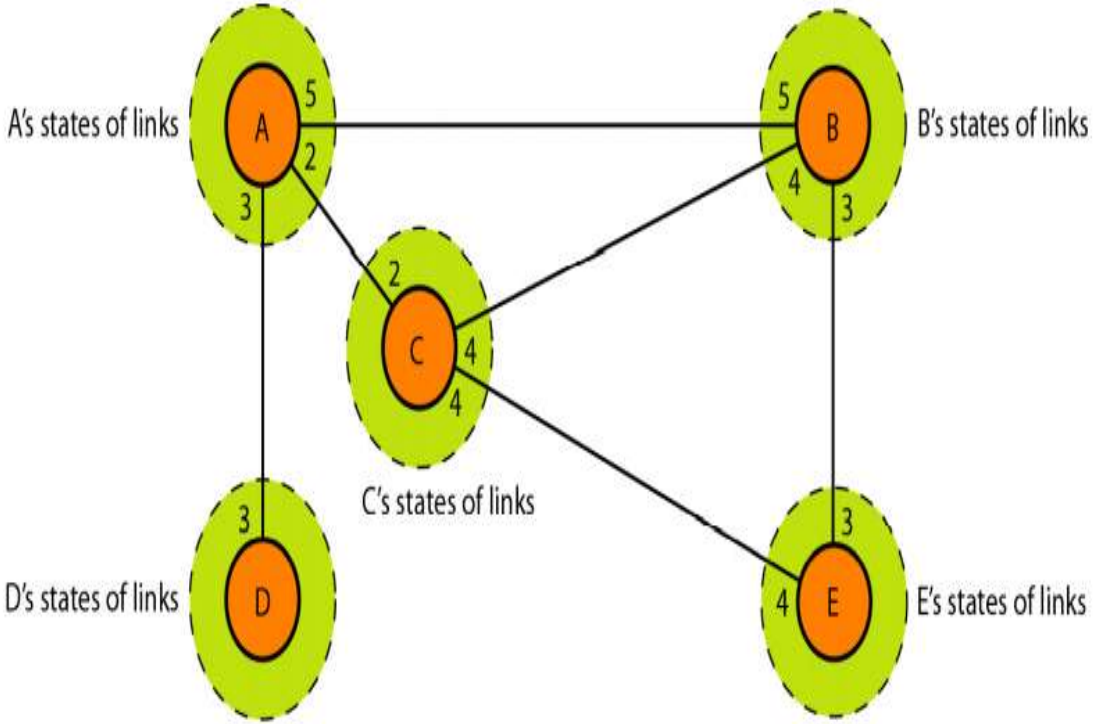
Computer Networks: MCA, I Year/II-Sem.

Outline

- Link State Routing Algorithm
- Creation of LSP
- Flooding of LSP
- Formation of Shortest path Tree

Link State Routing

- Link state routing is based on the assumption that, although the global knowledge about the topology is not clear.
- Each node has partial knowledge: it knows the state (type, condition, and cost) of its links.
- In other words, the whole topology can be compiled from the partial knowledge of each node


A's states of links
A
5
2
3
B
5
4
3
B's states of links
C
2
4
4
C's states of links
D
3
D's states of links
E
3
4
E's states of links

Building Routing Table

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

Creation of Link State Packet (LSP)

- A link state packet can carry a large amount of information.
- For the moment, we assume that it carries a minimum amount of data: the node identity, the list of links, a sequence number, and age.
- The first two, node identity and the list of links, are needed to make the topology.
- The third, sequence number, facilitates flooding and distinguishes new LSPs from old ones.
- The fourth, age, prevents old LSPs from remaining in the domain for a long time.

LSPs are generated on two occasions:

1. When there is a change in the topology of the domain
2. On a periodic basis: The period in this case is much longer compared to distance vector. The timer set for periodic dissemination is normally in the range of 60 min or 2 h based on the implementation. A longer period ensures that flooding does not create too much traffic on the network.

Flooding of LSPs

After a node has prepared an LSP, it must be disseminated to all other nodes, not only to its neighbors.

The process is called flooding and based on the following

1. The creating node sends a copy of the LSP out of each interface
2. A node that receives an LSP compares it with the copy it may already have. If the newly arrived LSP is older than the one it has (found by checking the sequence number), it discards the LSP.

If it is newer, the node does the following:

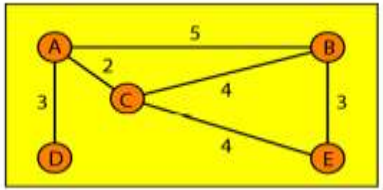
a. It discards the old LSP and keeps the new one.

b. It sends a copy of it out of each interface except the one from which the packet arrived.

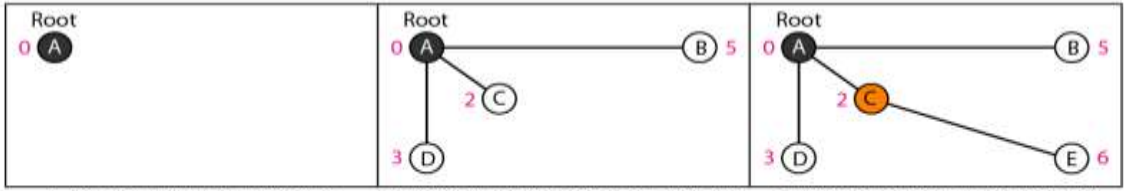
This guarantees that flooding stops somewhere in the domain (where a node has only one interface)

Formation of Shortest Path Tree

- Dijkstra Algorithm A shortest path tree is a tree in which the path between the root and every other node is the shortest
- The Dijkstra algorithm creates a shortest path tree from a graph
- The algorithm divides the nodes into two sets: tentative and permanent
- It finds the neighbors of a current node, makes them tentative, examines them, and if they pass the criteria, makes them permanent



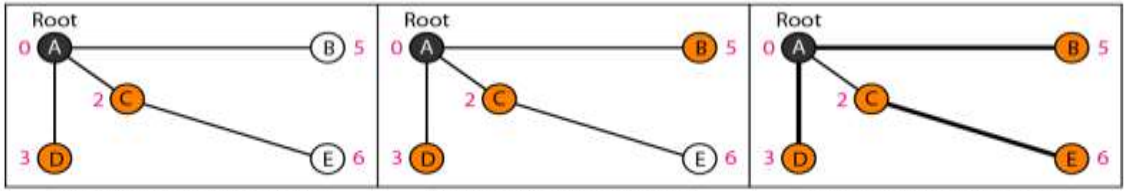
Topology



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.

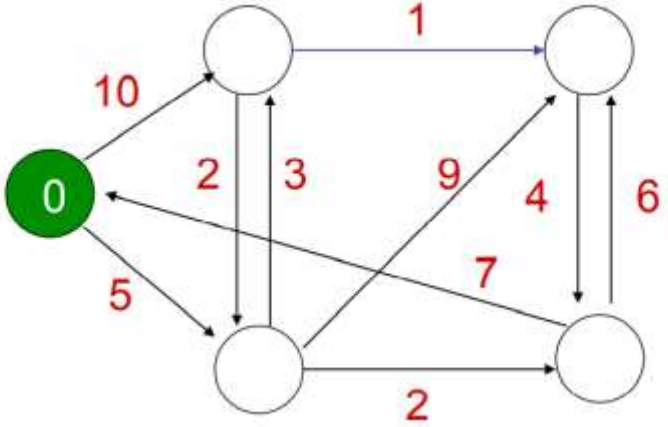
6. Move E to permanent list (tentative list is empty).

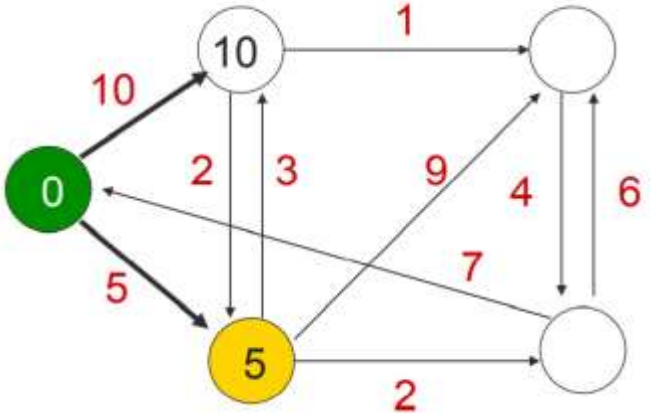
Calculation of Routing Table

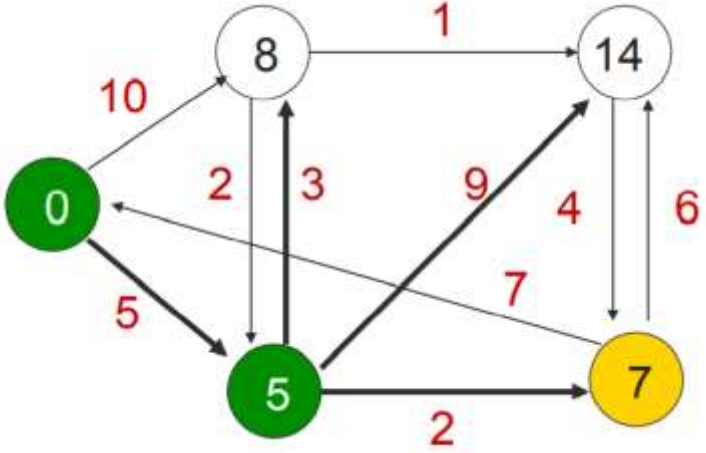
routing table for node A

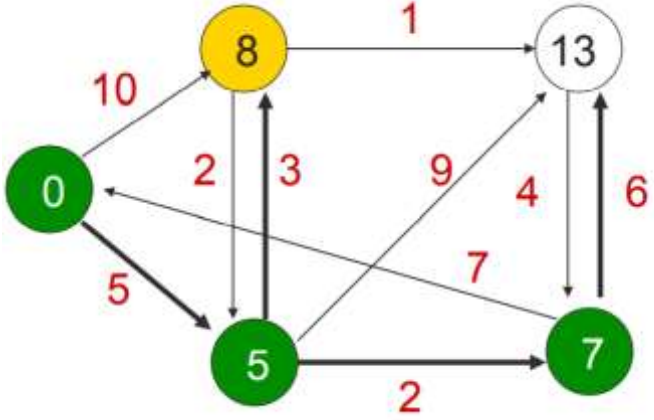
Node	*Cost*	*Next Router*
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

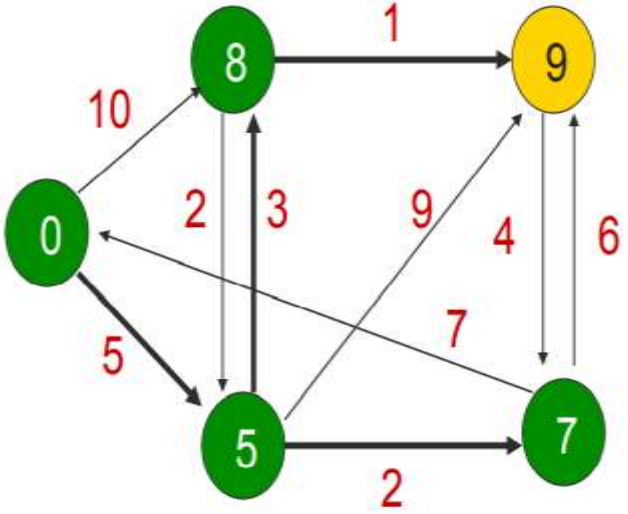
Example

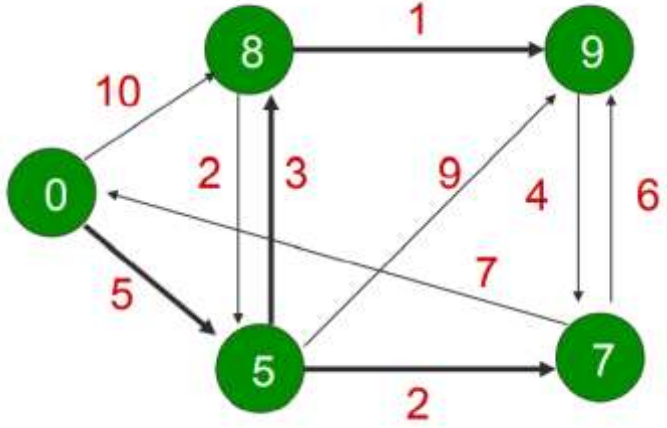





8
1
14
10
0
2
3
9
4
6
7
5
7
2


8
1
13
10
0
2
3
9
4
6
7
5
7
2


8
1
9
10
0
2
3
9
4
6
7
5
5
7
2


8
1
9
10
0
2
3
9
4
6
7
5
5
7
2

Computer Networks

Hierarchical Routing

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Hierarchical Routing

Computer Networks: MCA, I Year/II-Sem.

Outline

- Hierarchical Routing
- Broadcast Routing
- Congestion Control & Congestion prevention polices
- Choke Packet
- Load Shedding

Hierarchical Routing

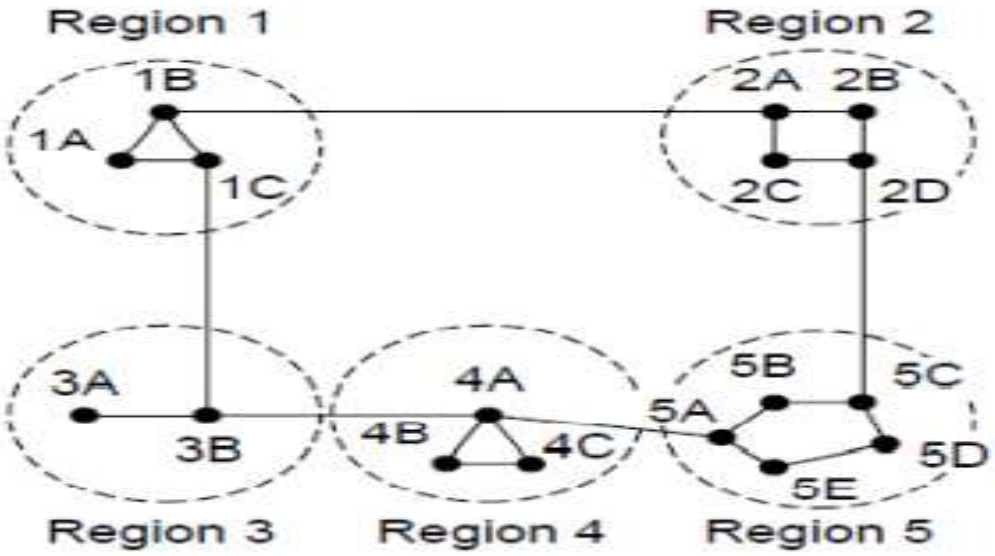
- As networks grow in size, the router routing tables grow proportionally.
- Not only is router memory consumed by ever-increasing tables
- But more CPU time is needed to scan them and more bandwidth is needed to send status reports about them.
- At a certain point, the network may grow to the point where it is no longer feasible for every router to have an entry for every other router, so the routing will have to be done hierarchically, as it is in the telephone network

• When hierarchical routing is used, the routers are divided into what we will call regions.

• Each router knows all the details about how to route packets to destinations within its own region but knows nothing about the internal structure of other regions.

• For huge networks, a two-level hierarchy may be insufficient; it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups, and so on, until we run out of names for aggregations

Example


Region 1
1B
1A
1C
Region 2
2A
2B
2C
2D
3A
3B
4A
4B
4C
5A
5B
5C
5D
5E
Region 3
Region 4
Region 5

Full table for 1A

Dest.	Line	Hops
1A	—	—
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

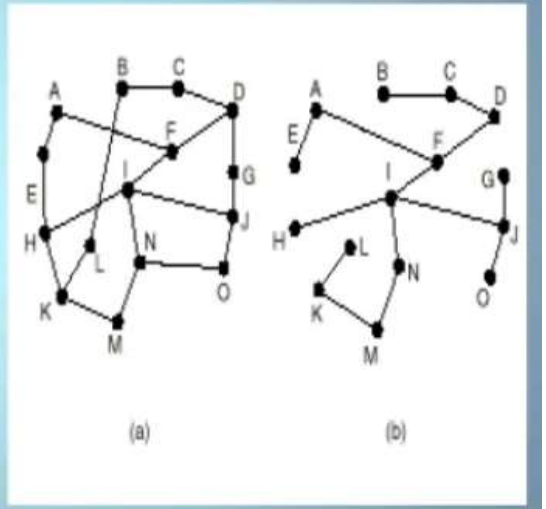
Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

Broadcast Routing

- Send a separate packet to each destination
- Use flooding
- Use multidestination routing
  - Each packet contains a list of destinations
  - Routers duplicate packet for all matching outgoing lines
- Use spanning tree routing
  - a subset of the subnet that includes all routers but contains no loops.

Spanning Tree Broadcasting

- Uses the minimum number of packets necessary
- Routers must be able to compute spanning tree
  - Available with link state routing
  - Not available with distance vector routing



- Reverse Path Forwarding
  - Use When knowledge of a spanning tree is not available
  - Provides an approximation of spanning tree routing
  - Routers check to see if incoming packet arrives from the same line that the router uses to route outgoing packets to the broadcast source
    - If so, the router duplicates the packet on all other outgoing lines
    - Otherwise, the router discards the packet

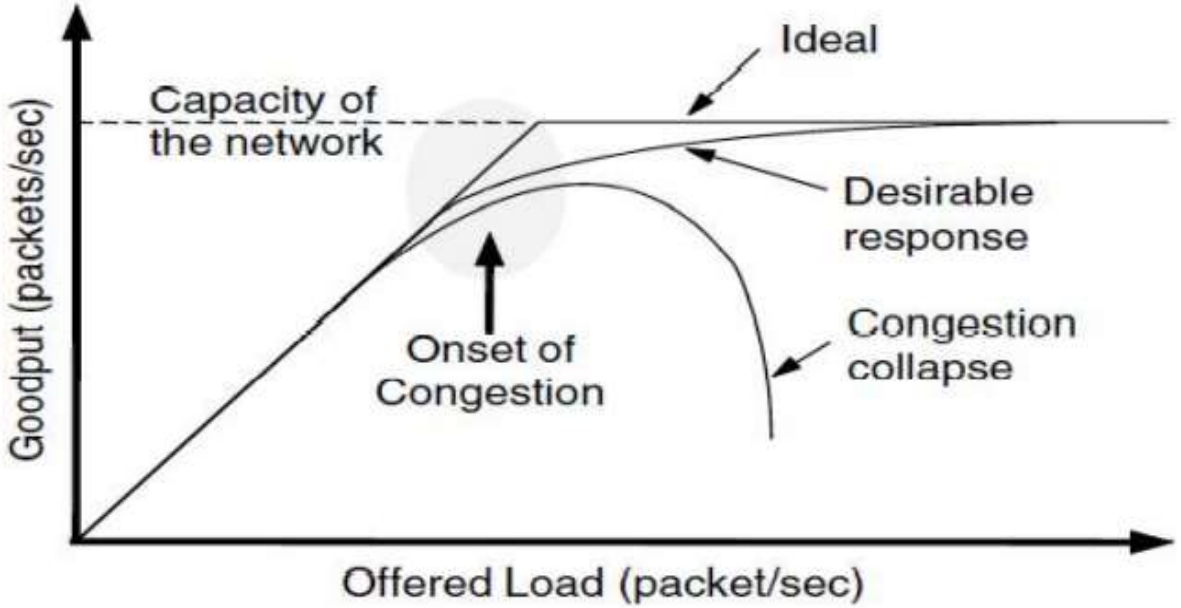
Congestion Control

• Too many packets present in (a part of) the network causes packet delay and loss that degrades performance. **This situation is called congestion**

• The network and transport layers share the responsibility for handling congestion. Since congestion occurs within the network, it is the network layer that directly experiences it and must ultimately determine what to do with the excess packets

• However, the most effective way to control congestion is to reduce the load that the transport layer is placing on the network

• This requires the network and transport layers to work together


Ideal
Capacity of
the network
Desirable
response
Congestion
collapse
Onset of
Congestion
Goodput (packets/sec)
Offered Load (packet/sec)

• Above Figure depicts the onset of congestion.

• When the number of packets hosts send into the network is well within its carrying capacity, the number delivered is proportional to the number sent.

• If twice as many are sent, twice as many are delivered.

• However, as the offered load approaches the carrying capacity, bursts of traffic occasionally fill up the buffers inside routers and some packets are lost.

• These lost packets consume some of the capacity, so the number of delivered packets falls below the ideal curve. The network is now congested

Congestion Prevention polices

1. Warning bit
2. Choke packets
3. Load shedding
4. Random early discard
5. Traffic shaping

Warning bit

1. A special bit in the packet header is set by the router to warn the source when congestion is detected.
2. The bit is copied and piggy-backed on the ACK and sent to the sender.
3. The sender monitors the number of ACK packets it receives with the warning bit set and adjusts its transmission rate accordingly

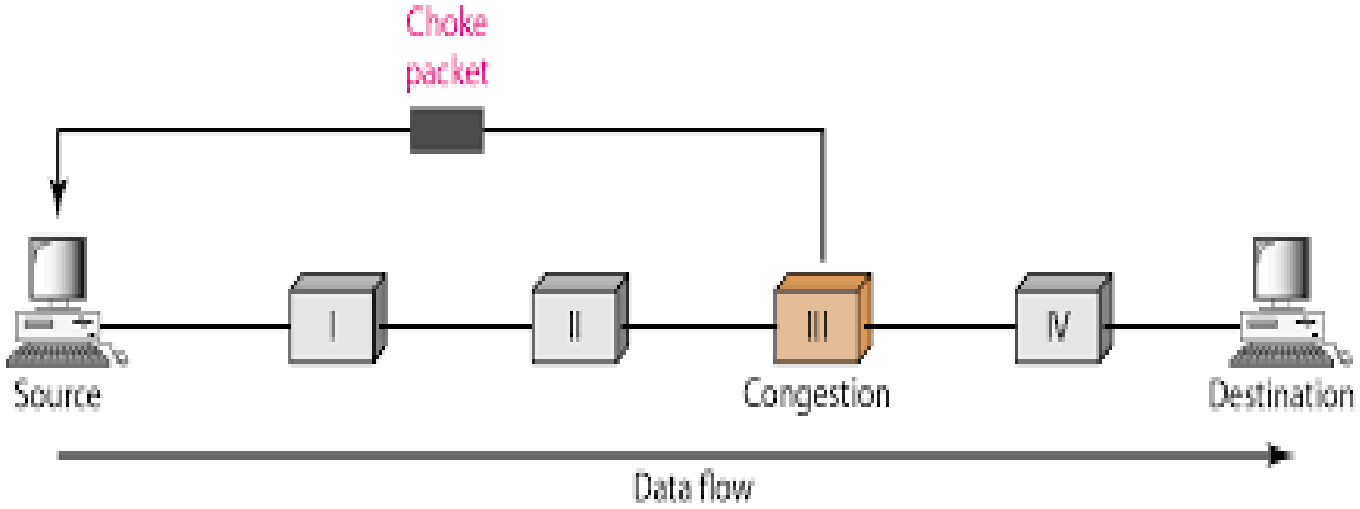
Choke Packets

A choke packet is a control packet generated at a congested node and transmitted to restrict traffic flow.

The source, on receiving the choke packet must reduce its transmission rate by a certain percentage.

An example of a choke packet is the ICMP Source Quench Packet.

Hop-by-Hop Choke Packets 1. Over long distances or at high speeds choke packets are not very effective. 2. A more efficient method is to send to choke packets hop-by-hop. 3. This requires each hop to reduce its transmission even before the choke packet arrive at the source


Choke
packet
I
II
III
IV
Source
Congestion
Destination
Data flow

Load Shedding

1. When buffers become full, routers simply discard packets
2. Which packet is chosen to be the victim depends on the application and on the error strategy used in the data link layer
3. For a file transfer, for, e.g. cannot discard older packets since this will cause a gap in the received data
4. For real-time voice or video it is probably better to throw away old data and keep new packets
5. Get the application to mark packets with discard priority

Random Early Discard (RED)

1. This is a proactive approach in which the router discards one or more packets before the buffer becomes completely full.
2. Each time a packet arrives, the RED algorithm computes the average queue length, avg.
3. If avg is lower than some lower threshold, congestion is assumed to be minimal or non-existent and the packet is queued.
4. If avg is greater than some upper threshold, congestion is assumed to be serious and the packet is discarded.
5. If avg is between the two thresholds, this might indicate the onset of congestion. The probability of congestion is then calculated

Traffic Shaping

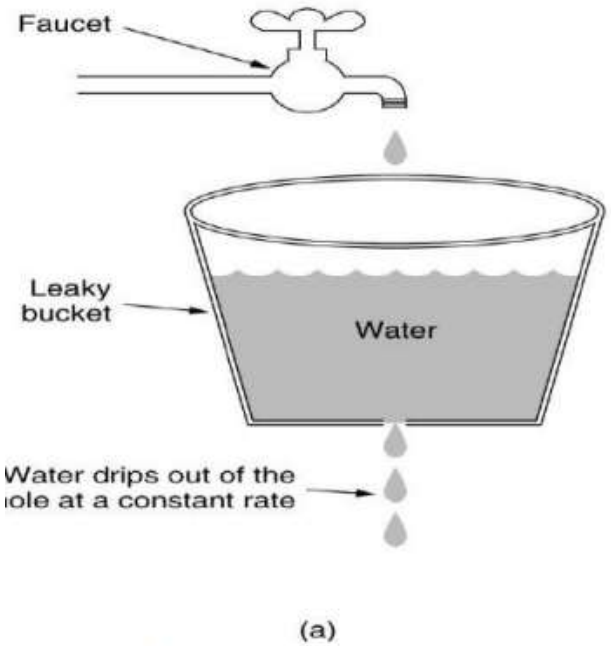
1. Another method of congestion control is to “shape” the traffic before it enters the network.
2. Traffic shaping controls the rate at which packets are sent (not just how many). Used in ATM and Integrated Services networks.
3. At connection set-up time, the sender and carrier negotiate a traffic pattern (shape). Two traffic shaping algorithms are: Leaky Bucket Token Bucket

The Leaky Bucket Algorithm

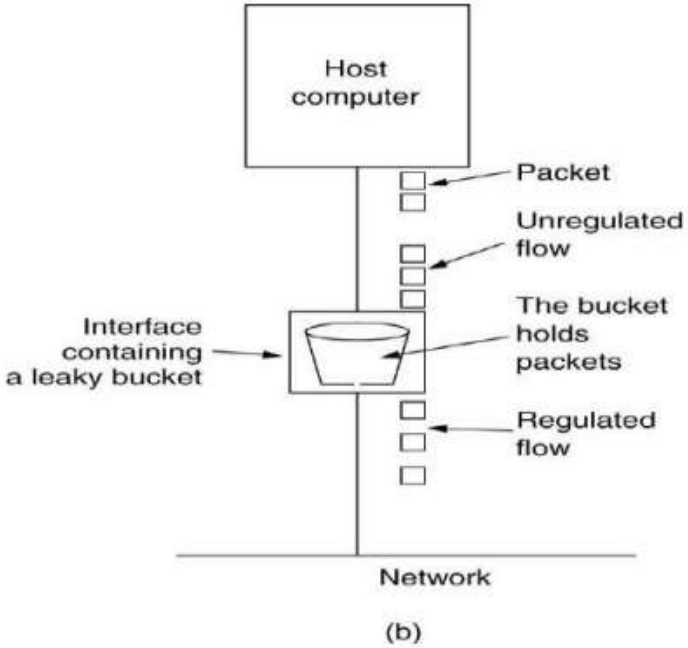
- The Leaky Bucket Algorithm used to control rate in a network.
- It is implemented as a single server queue with constant service time.
- If the bucket (buffer) overflows then packets are discarded
- The leaky bucket enforces a constant output rate (average rate) regardless of the burstiness of the input. Does nothing when input is idle.

•. The host injects one packet per clock tick onto the network. This results in a uniform flow of packets, smoothing out bursts and reducing congestion.

• When packets are the same size (as in ATM cells), the one packet per tick is okay. For variable length packets though, it is better to allow a fixed number of bytes per tick. E.g. 1024 bytes per tick will allow one 1024-byte packet or two 512-byte packets or four 256- byte packets on 1 tick



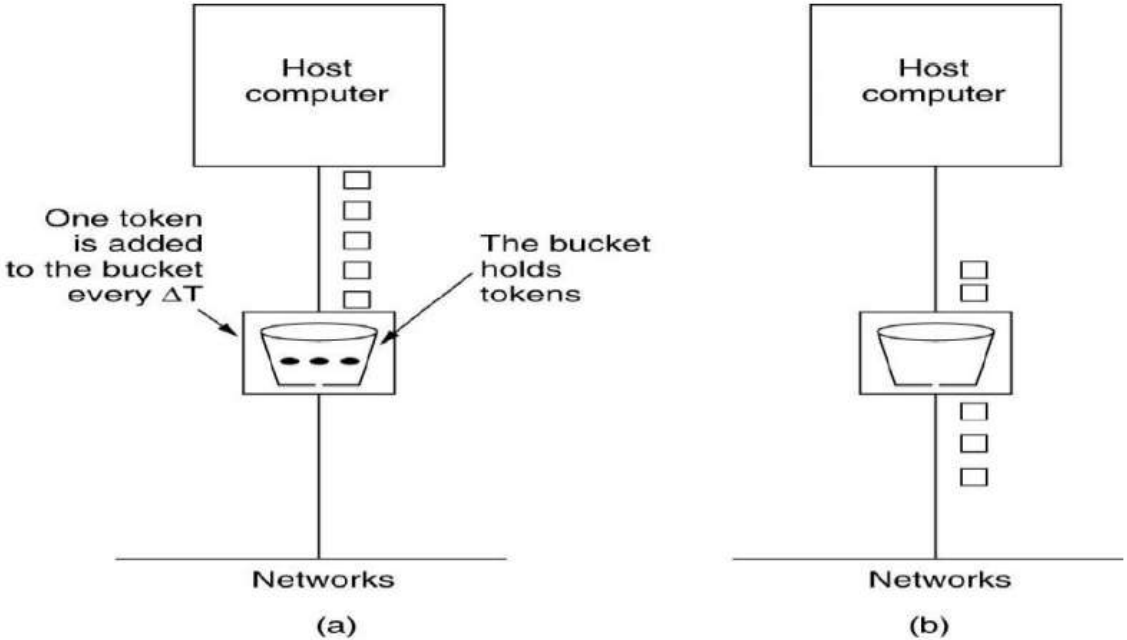
(a) A leaky bucket with water.



(b) a leaky bucket with packets.

Token Bucket Algorithm

1. In contrast to the LB, the Token Bucket Algorithm, allows the output rate to vary, depending on the size of the burst.
2. In the TB algorithm, the bucket holds tokens. To transmit a packet, the host must capture and destroy one token.
3. Tokens are generated by a clock at the rate of one token every □t sec.
4. Idle hosts can capture and save up tokens (up to the max. size of the bucket) in order to send larger bursts later.



(a) Before. (b) After.

Leaky Bucket vs. Token Bucket

1. LB discards packets; TB does not. TB discards tokens.
2. With TB, a packet can only be transmitted if there are enough tokens to cover its length in bytes.
3. LB sends packets at an average rate. TB allows for large bursts to be sent faster by speeding up the output.
4. TB allows saving up tokens (permissions) to send large bursts. LB does not allow saving

Computer Networks

Congestion Control

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Congestion Control

Computer Networks: MCA, I Year/II-Sem.

Outline

- Congestion Control & Congestion prevention polices
- Choke Packet
- Load Shedding

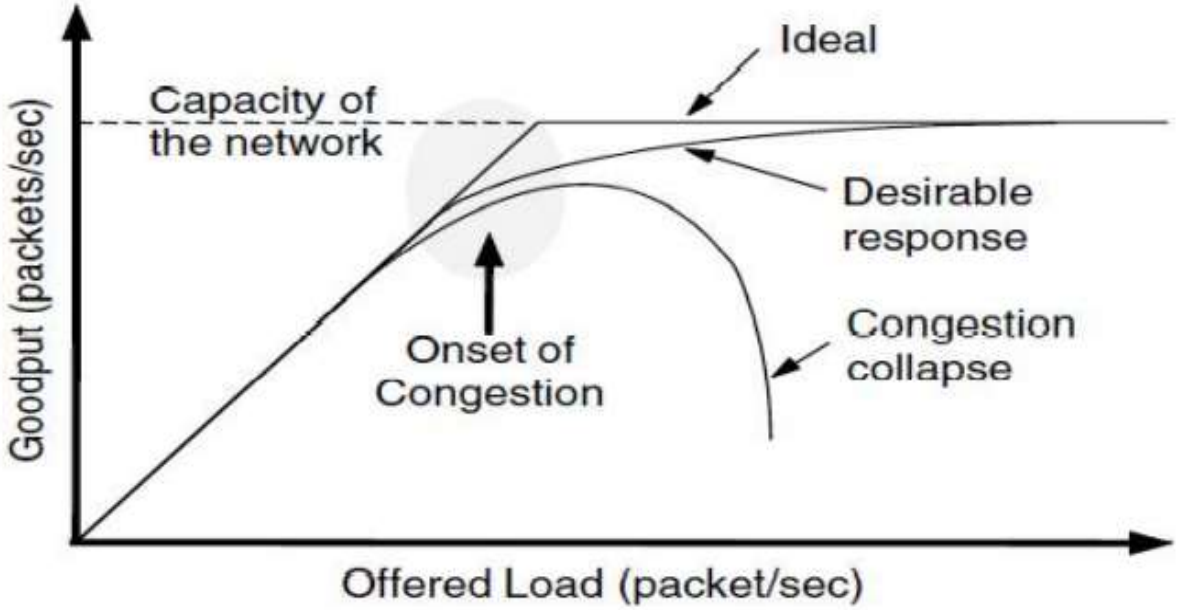
Congestion Control

• Too many packets present in (a part of) the network causes packet delay and loss that degrades performance. **This situation is called congestion**

• The network and transport layers share the responsibility for handling congestion. Since congestion occurs within the network, it is the network layer that directly experiences it and must ultimately determine what to do with the excess packets

• However, the most effective way to control congestion is to reduce the load that the transport layer is placing on the network

• This requires the network and transport layers to work together


Ideal
Capacity of
the network
Desirable
response
Congestion
collapse
Onset of
Congestion
Goodput (packets/sec)
Offered Load (packet/sec)

• Above Figure depicts the onset of congestion.

• When the number of packets hosts send into the network is well within its carrying capacity, the number delivered is proportional to the number sent.

• If twice as many are sent, twice as many are delivered.

• However, as the offered load approaches the carrying capacity, bursts of traffic occasionally fill up the buffers inside routers and some packets are lost.

• These lost packets consume some of the capacity, so the number of delivered packets falls below the ideal curve. The network is now congested

Congestion Prevention polices

1. Warning bit
2. Choke packets
3. Load shedding
4. Random early discard
5. Traffic shaping

Warning bit

1. A special bit in the packet header is set by the router to warn the source when congestion is detected.
2. The bit is copied and piggy-backed on the ACK and sent to the sender.
3. The sender monitors the number of ACK packets it receives with the warning bit set and adjusts its transmission rate accordingly

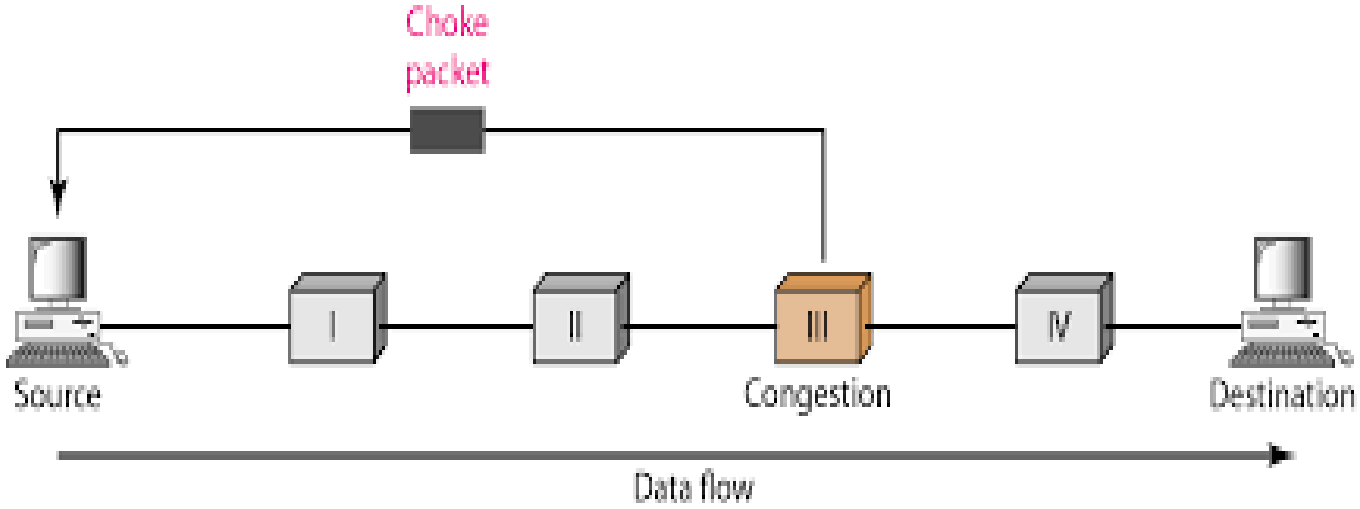
Choke Packets

A choke packet is a control packet generated at a congested node and transmitted to restrict traffic flow.

The source, on receiving the choke packet must reduce its transmission rate by a certain percentage.

An example of a choke packet is the ICMP Source Quench Packet.

Hop-by-Hop Choke Packets 1. Over long distances or at high speeds choke packets are not very effective. 2. A more efficient method is to send to choke packets hop-by-hop. 3. This requires each hop to reduce its transmission even before the choke packet arrive at the source


Choke
packet
I
II
III
IV
Source
Congestion
Destination
Data flow

Load Shedding

1. When buffers become full, routers simply discard packets
2. Which packet is chosen to be the victim depends on the application and on the error strategy used in the data link layer
3. For a file transfer, for, e.g. cannot discard older packets since this will cause a gap in the received data
4. For real-time voice or video it is probably better to throw away old data and keep new packets
5. Get the application to mark packets with discard priority

Random Early Discard (RED)

1. This is a proactive approach in which the router discards one or more packets before the buffer becomes completely full.
2. Each time a packet arrives, the RED algorithm computes the average queue length, avg.
3. If avg is lower than some lower threshold, congestion is assumed to be minimal or non-existent and the packet is queued.
4. If avg is greater than some upper threshold, congestion is assumed to be serious and the packet is discarded.
5. If avg is between the two thresholds, this might indicate the onset of congestion. The probability of congestion is then calculated

Traffic Shaping

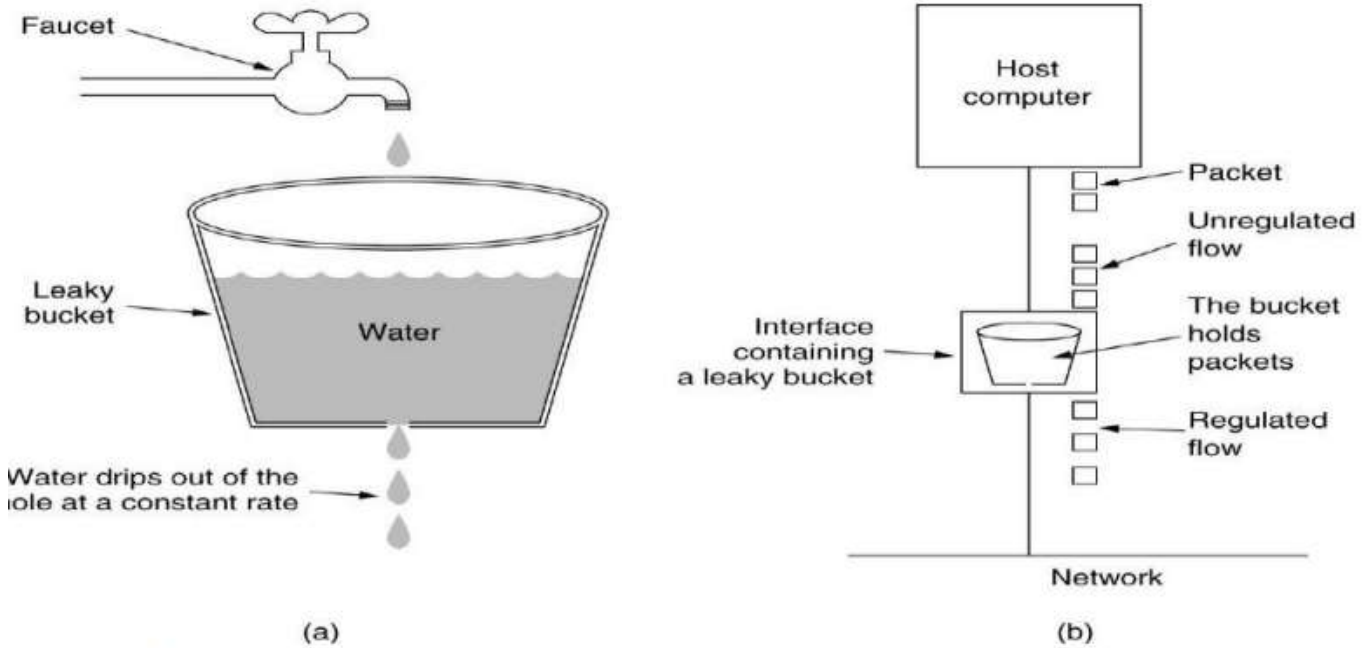
1. Another method of congestion control is to “shape” the traffic before it enters the network.
2. Traffic shaping controls the rate at which packets are sent (not just how many). Used in ATM and Integrated Services networks.
3. At connection set-up time, the sender and carrier negotiate a traffic pattern (shape). Two traffic shaping algorithms are: Leaky Bucket Token Bucket

The Leaky Bucket Algorithm

- The Leaky Bucket Algorithm used to control rate in a network
- It is implemented as a single server queue with constant service time.
- If the bucket (buffer) overflows then packets are discarded
- The leaky bucket enforces a constant output rate (average rate) regardless of the burstiness of the input. Does nothing when input is idle.

• The host injects one packet per clock tick onto the network. This results in a uniform flow of packets, smoothing out bursts and reducing congestion

• When packets are the same size (as in ATM cells), the one packet per tick is okay. For variable length packets though, it is better to allow a fixed number of bytes per tick. E.g. 1024 bytes per tick will allow one 1024-byte packet or two 512-byte packets or four 256- byte packets on 1 tick

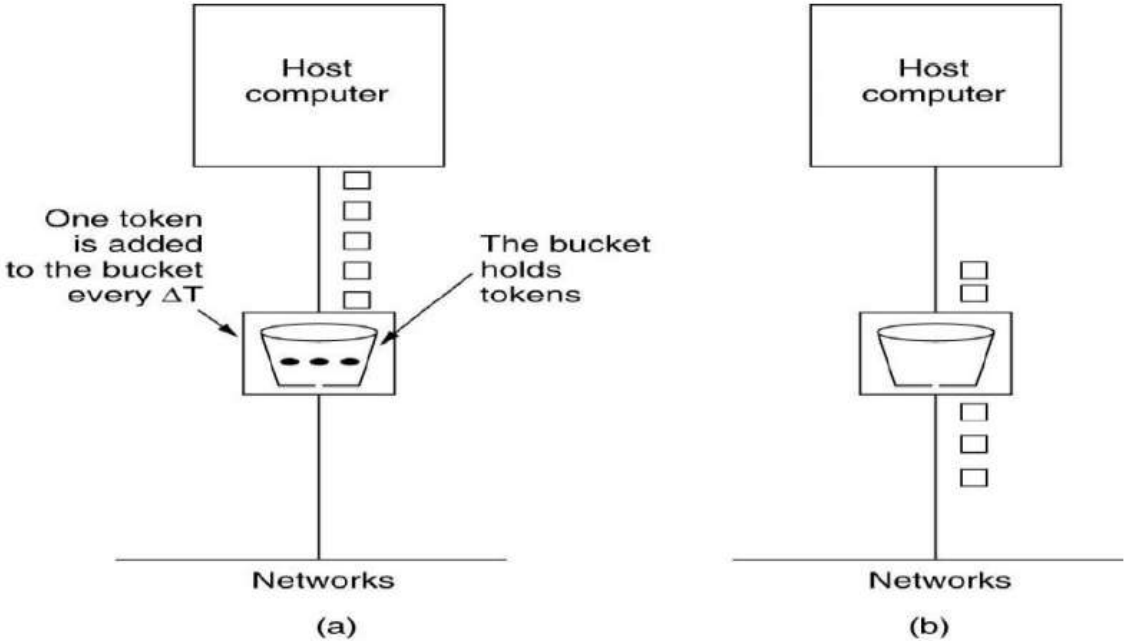


(a) A leaky bucket with water.

(b) a leaky bucket with packets.

Token Bucket Algorithm

1. In contrast to the LB, the Token Bucket Algorithm, allows the output rate to vary, depending on the size of the burst.
2. In the TB algorithm, the bucket holds tokens. To transmit a packet, the host must capture and destroy one token.
3. Tokens are generated by a clock at the rate of one token every □t sec.
4. Idle hosts can capture and save up tokens (up to the max. size of the bucket) in order to send larger bursts later.



(a) Before. (b) After.

Leaky Bucket vs. Token Bucket

1. LB discards packets; TB does not. TB discards tokens.
2. With TB, a packet can only be transmitted if there are enough tokens to cover its length in bytes.
3. LB sends packets at an average rate. TB allows for large bursts to be sent faster by speeding up the output.
4. TB allows saving up tokens (permissions) to send large bursts. LB does not allow saving

Computer Networks

Connection Establishment

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Connection Establishment

Computer Networks: MCA, I Year/II-Sem.

Outline

- Introduction to Transport Layer
- TPDU
- Elements in Transport Layer
- Addressing
- Connection Establishment
- Connection Release

Transport Layer

The network layer provides end-to-end packet delivery using data-grams or virtual circuits. The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine with a desired level of reliability that is independent of the physical networks currently in use.

•Transport Entity: The hardware and/or software which make use of services provided by the network layer, (within the transport layer) is called transport entity.

•Transport Service Provider: Layers 1 to 4 are called Transport Service Provider.

•Transport Service User: The upper layers i.e., layers 5 to 7 are called Transport Service User.

•Transport Service Primitives: Which allow transport users (application programs) to access the transport service.

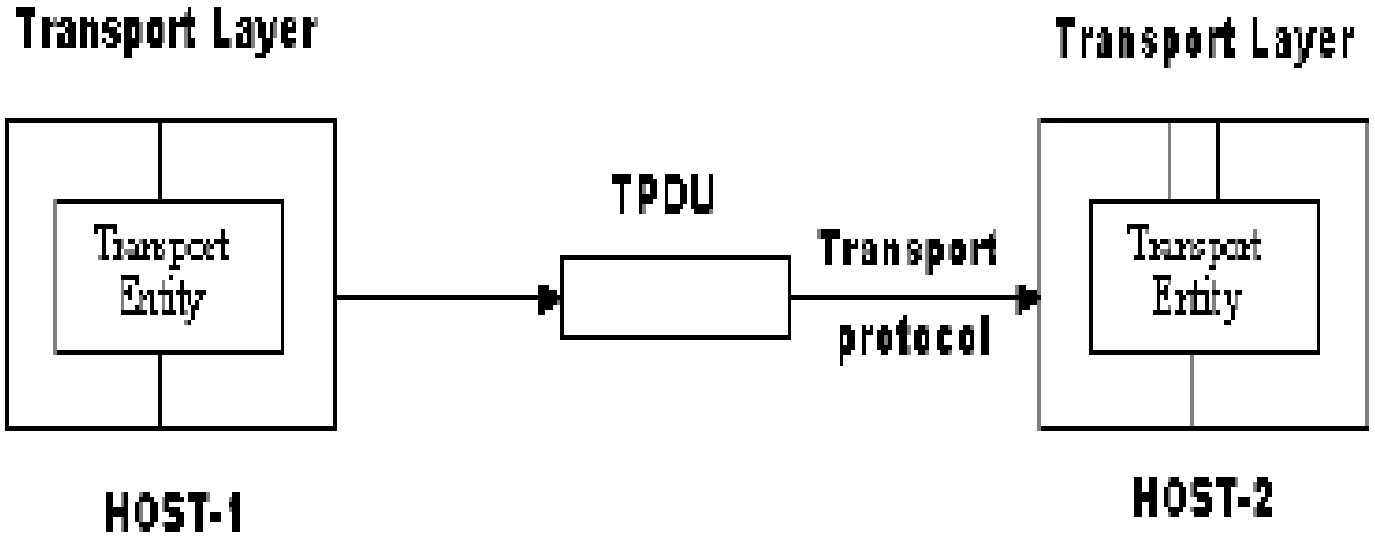
TPDU (Transport Protocol Data Unit)

Transmissions of message between 2 transport entities are carried out by TPDU.

•The transport entity carries out the transport service primitives by blocking the caller and sending a packet the service.

•Encapsulated in the payload of this packet is a transport layer message for the server's transport entity.

•The task of the transport layer is to provide reliable, cost-effective data transport from the source machine to the destination machine, independent of physical network or networks currently in use.

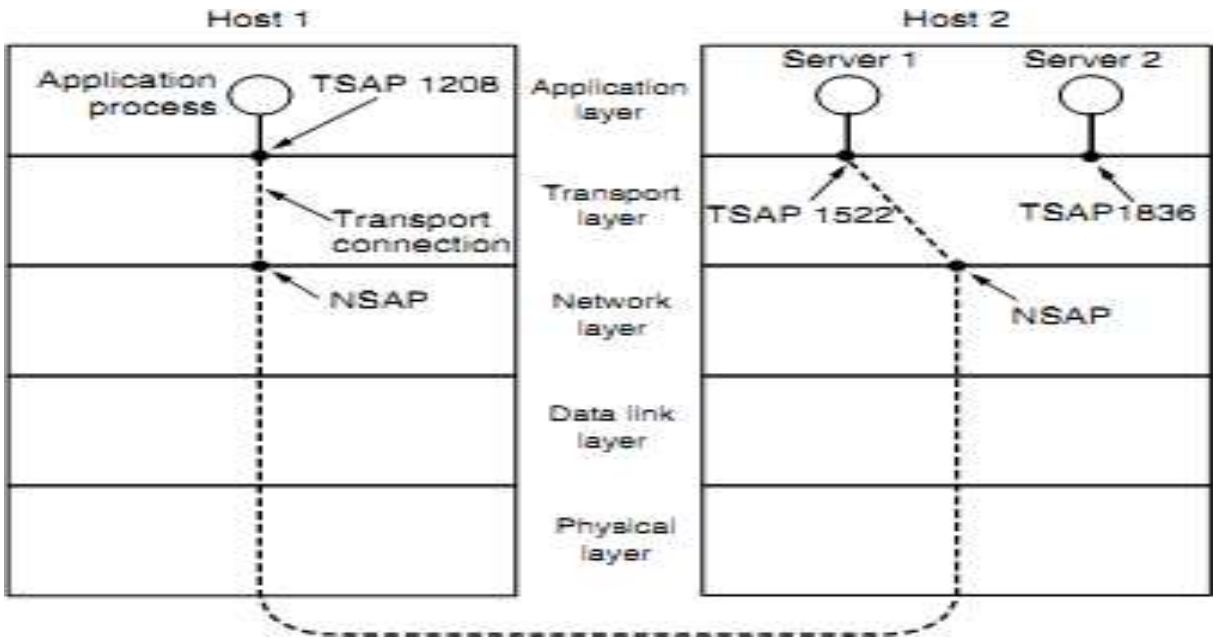

Transport Layer
Transport Layer
Transport Entity
TPDU
Transport protocol
Transport Entity
HOST-1
HOST-2

Elements in Transport Layer

The elements of transport protocols are:

1. ADDRESSING
2. Connection Establishment.
3. Connection Release.
4. Error control and flow control
5. Multiplexing.

Addressing


Host 1
Host 2
Application process
TSAP 1208
Transport connection
NSAP
Application layer
Transport layer
Network layer
Data link layer
Physical layer
Server 1
Server 2
TSAP 1522
TSAP1836
NSAP

• When an application (e.g., a user) process wishes to set up a connection to a remote application process, it must specify which one to connect to. The method normally used is to define transport addresses to which processes can listen for connection requests. In the Internet, these endpoints are called **ports.**

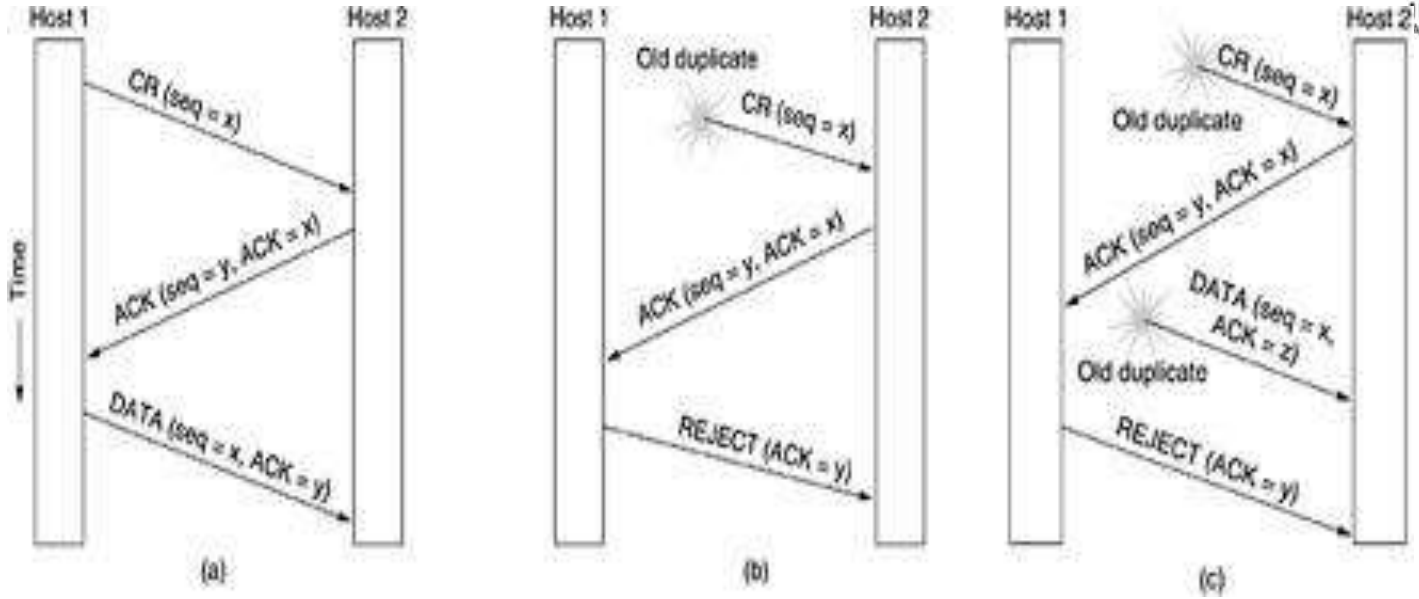
There are two types of access points.

TSAP (Transport Service Access Point) to mean a specific endpoint in the transport layer.

The analogous endpoints in the network layer (i.e., network layer addresses) are not surprisingly called

NSAPs (Network Service Access Points). IP addresses are examples of NSAPs..

Connection Establishment



Three protocol scenarios for establishing a connection using a three-way handshake. CR denotes CONNEC TION REQUEST (a) Normal operation. (b) Old duplicate CONNECTION REQUEST appearing out of nowhere. (c) Duplicate CONNECTION REQUEST and duplicate ACK .

Connection Release

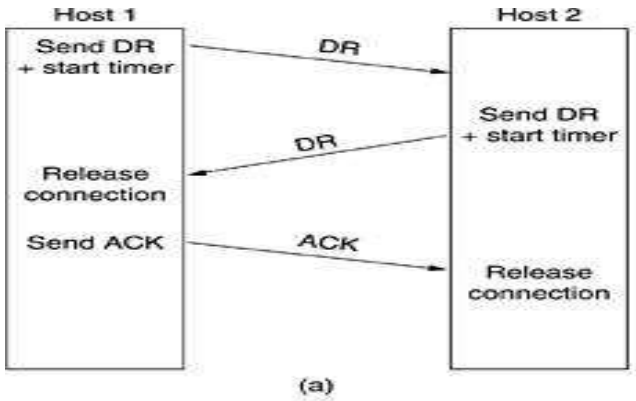
A connection is released using either asymmetric or symmetric variant. But, the improved protocol for releasing a connection is a 3-way handshake protocol.

There are two styles of terminating a connection:

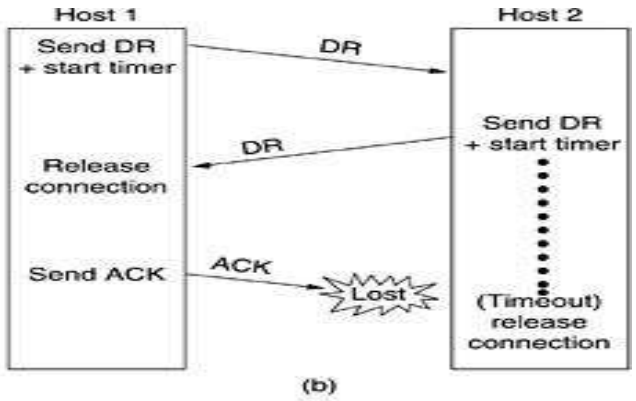
1) Asymmetric release and

2) Symmetric release.

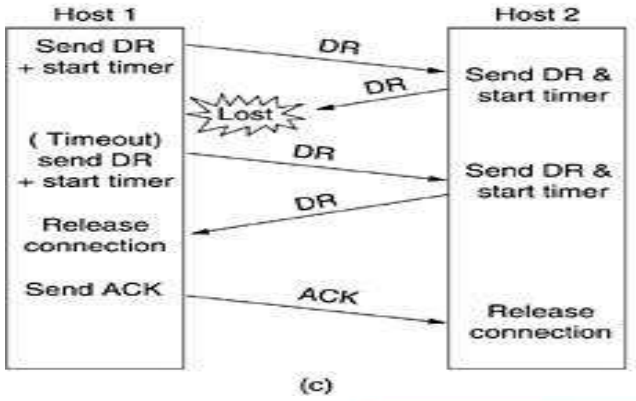
This disconnection can b done either by asymmetric variant (connection is released, depending on other one) or by symmetric variant (connection is released, independent of other one).



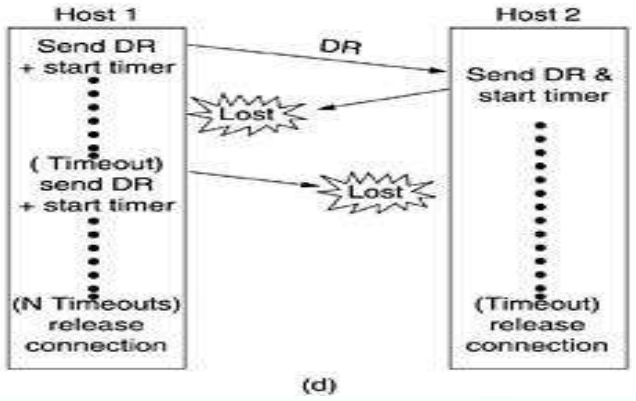
(a)



(b)



(c)



(d)

Computer Networks

Transport Layer Elements

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Transport Layer Elements

Computer Networks: MCA, I Year/II-Sem.

Outline

- Introduction to Transport Layer
- TPDU
- Elements in Transport Layer
- Addressing
- Connection Establishment
- Connection Release

Transport Layer

The network layer provides end-to-end packet delivery using data-grams or virtual circuits. The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine with a desired level of reliability that is independent of the physical networks currently in use.

•Transport Entity: The hardware and/or software which make use of services provided by the network layer, (within the transport layer) is called transport entity.

•Transport Service Provider: Layers 1 to 4 are called Transport Service Provider.

•Transport Service User: The upper layers i.e., layers 5 to 7 are called Transport Service User.

•Transport Service Primitives: Which allow transport users (application programs) to access the transport service.

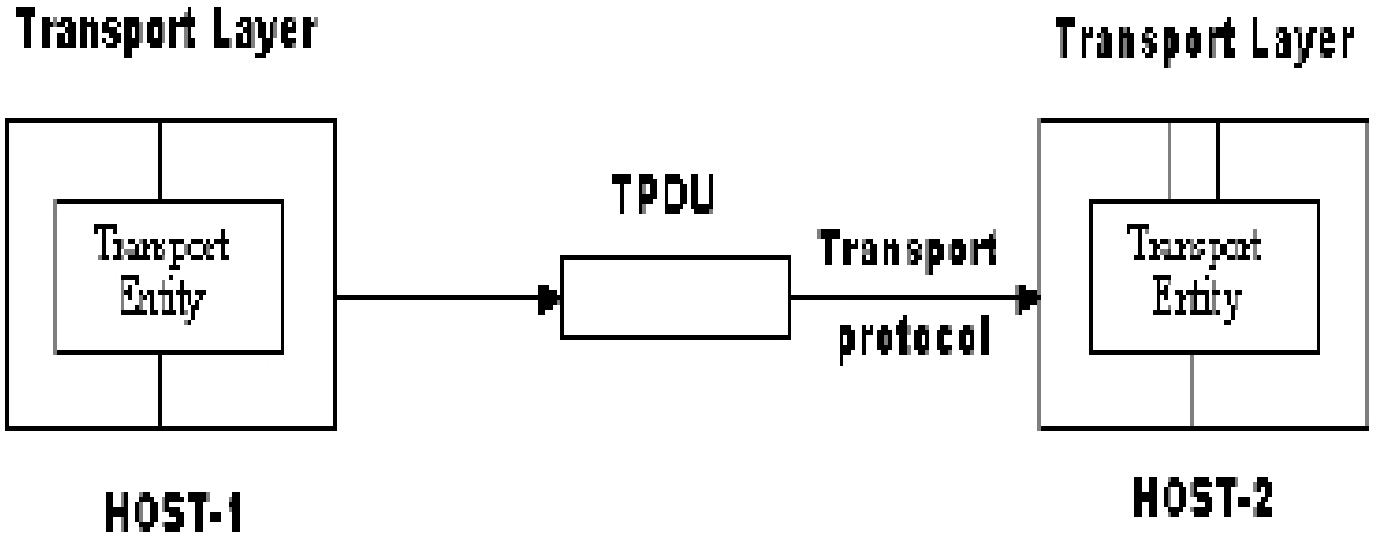
TPDU (Transport Protocol Data Unit)

Transmissions of message between 2 transport entities are carried out by TPDU.

•The transport entity carries out the transport service primitives by blocking the caller and sending a packet the service.

•Encapsulated in the payload of this packet is a transport layer message for the server's transport entity.

•The task of the transport layer is to provide reliable, cost-effective data transport from the source machine to the destination machine, independent of physical network or networks currently in use.

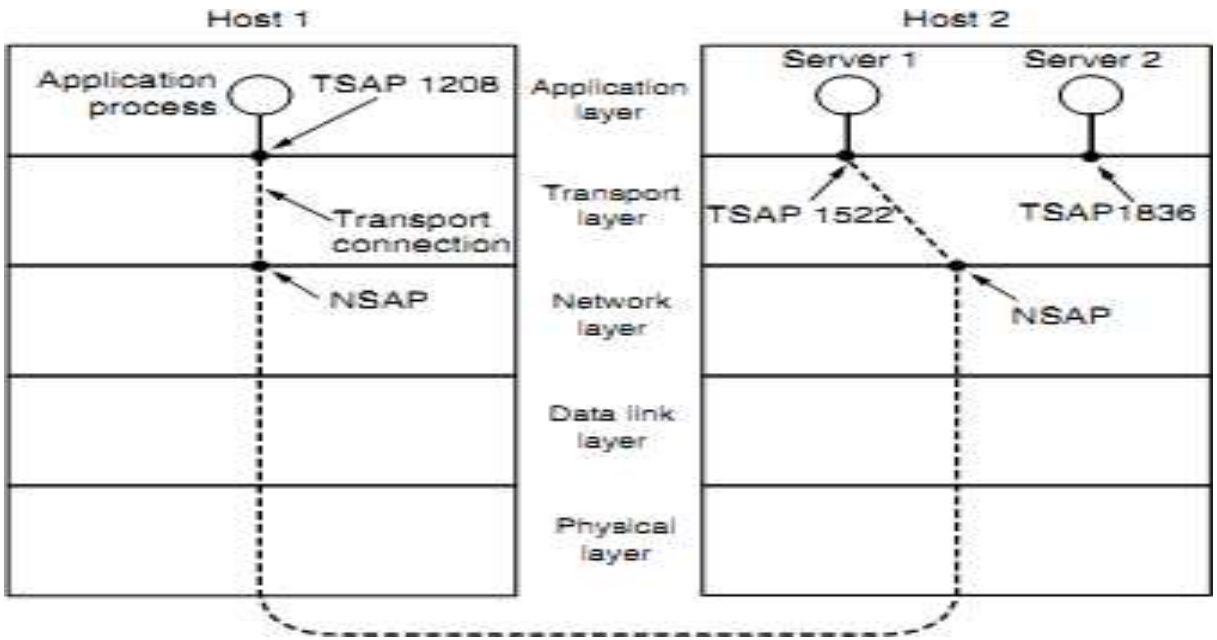

Transport Layer
Transport Layer
Transport Entity
TPDU
Transport protocol
Transport Entity
HOST-1
HOST-2

Elements in Transport Layer

The elements of transport protocols are:

1. ADDRESSING
2. Connection Establishment.
3. Connection Release.
4. Error control and flow control
5. Multiplexing.

Addressing


Host 1
Host 2
Application process
TSAP 1208
Transport connection
NSAP
Application layer
Transport layer
Network layer
Data link layer
Physical layer
Server 1
Server 2
TSAP 1522
TSAP1836
NSAP

• When an application (e.g., a user) process wishes to set up a connection to a remote application process, it must specify which one to connect to. The method normally used is to define transport addresses to which processes can listen for connection requests. In the Internet, these endpoints are called **ports.**

There are two types of access points.

TSAP (Transport Service Access Point) to mean a specific endpoint in the transport layer.

The analogous endpoints in the network layer (i.e., network layer addresses) are not surprisingly called

NSAPs (Network Service Access Points). IP addresses are examples of NSAPs..

Computer Networks

Transport Layer-TCP

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Transport Layer-TCP

Computer Networks: MCA, I Year/II-Sem.

Outline

- Introduction to Transport Layer
- TPDU
- TCP

Transport Layer

The network layer provides end-to-end packet delivery using data-grams or virtual circuits. The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine with a desired level of reliability that is independent of the physical networks currently in use.

•Transport Entity: The hardware and/or software which make use of services provided by the network layer, (within the transport layer) is called transport entity.

•Transport Service Provider: Layers 1 to 4 are called Transport Service Provider.

•Transport Service User: The upper layers i.e., layers 5 to 7 are called Transport Service User.

•Transport Service Primitives: Which allow transport users (application programs) to access the transport service.

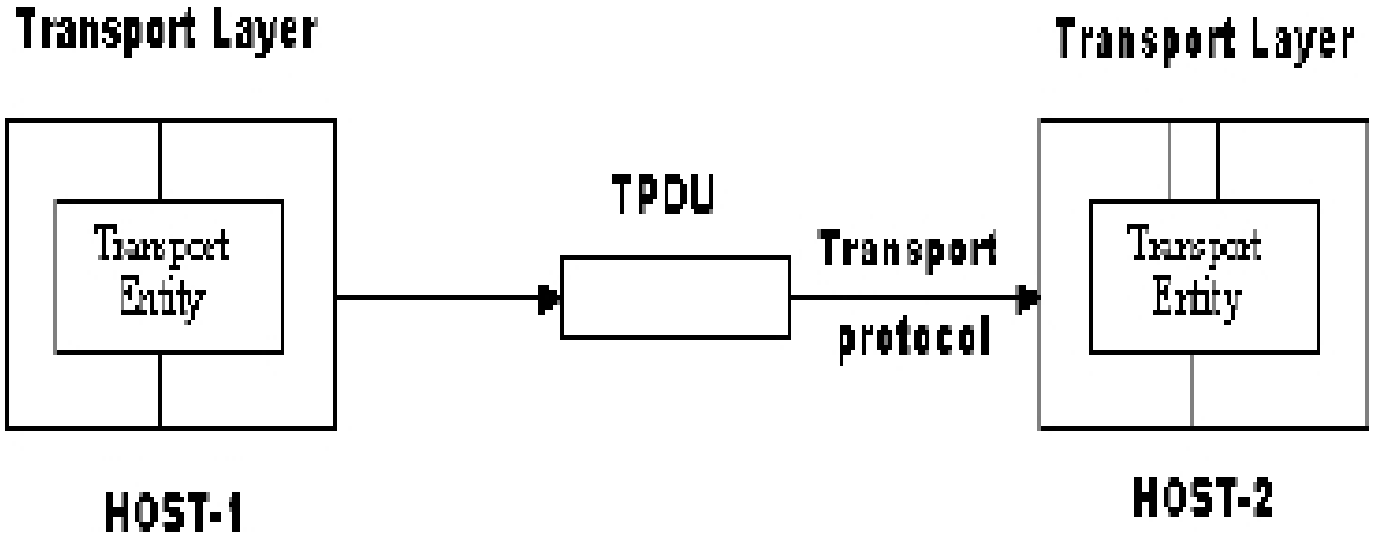
TPDU (Transport Protocol Data Unit)

Transmissions of message between 2 transport entities are carried out by TPDU.

•The transport entity carries out the transport service primitives by blocking the caller and sending a packet the service.

•Encapsulated in the payload of this packet is a transport layer message for the server's transport entity.

•The task of the transport layer is to provide reliable, cost-effective data transport from the source machine to the destination machine, independent of physical network or networks currently in use.

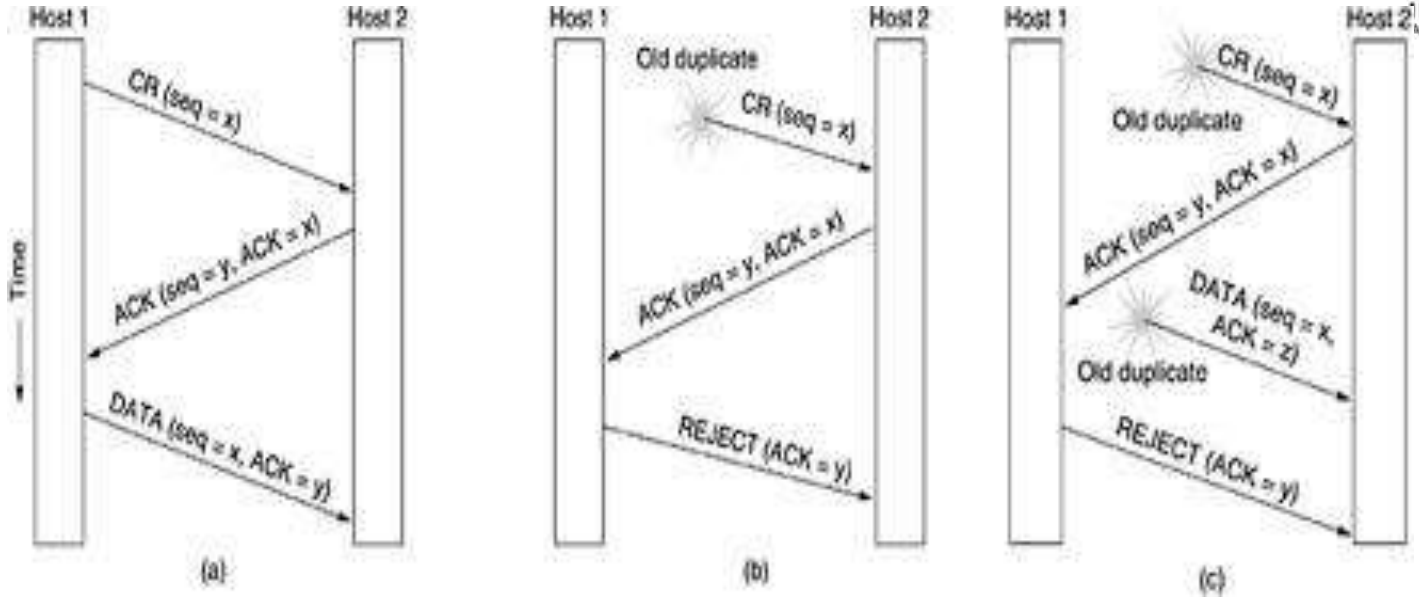

Transport Layer
Transport Layer
Transport Entity
TPDU
Transport protocol
Transport Entity
HOST-1
HOST-2

Elements in Transport Layer

The elements of transport protocols are:

1. ADDRESSING
2. Connection Establishment.
3. Connection Release.
4. Error control and flow control
5. Multiplexing.

Connection Establishment



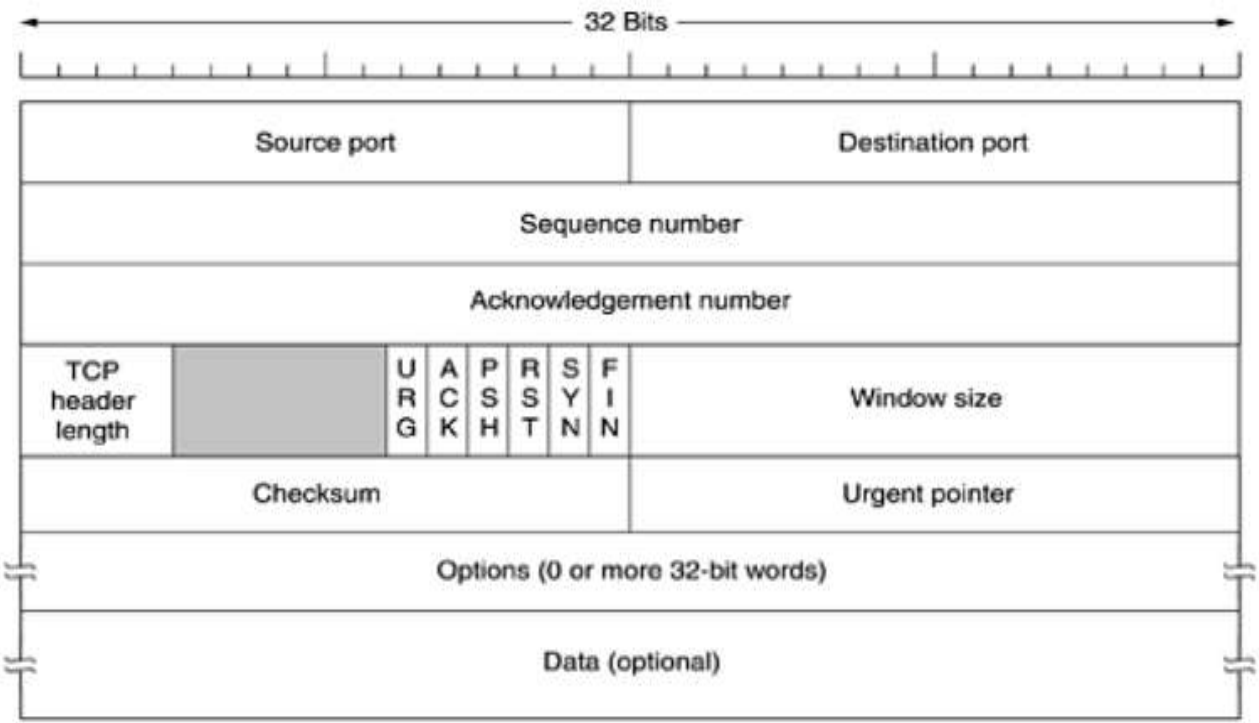
Three protocol scenarios for establishing a connection using a three-way handshake. CR denotes CONNEC TION REQUEST (a) Normal operation. (b) Old duplicate CONNECTION REQUEST appearing out of nowhere. (c) Duplicate CONNECTION REQUEST and duplicate ACK .

TCP Header Format

•Every segment begins with a fixed-format, 20-byte header. The fixed header may be followed by header options.

•After the options, if any, up to 65,535 - 20 - 20 = 65,495 data bytes may follow, where the first 20 refer to the IP header and the second to the TCP header.

•Segments without any data are legal and are commonly used for acknowledgements and control message



Computer Networks

Transport Layer-UDP

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Transport Layer-UDP

Computer Networks: MCA, I Year/II-Sem.

Outline

- Introduction to Transport Layer
- TPDU
- Elements in Transport Layer
- Addressing
- Connection Establishment
- Connection Release

Transport Layer

The network layer provides end-to-end packet delivery using data-grams or virtual circuits. The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine with a desired level of reliability that is independent of the physical networks currently in use.

•Transport Entity: The hardware and/or software which make use of services provided by the network layer, (within the transport layer) is called transport entity.

•Transport Service Provider: Layers 1 to 4 are called Transport Service Provider.

•Transport Service User: The upper layers i.e., layers 5 to 7 are called Transport Service User.

•Transport Service Primitives: Which allow transport users (application programs) to access the transport service.

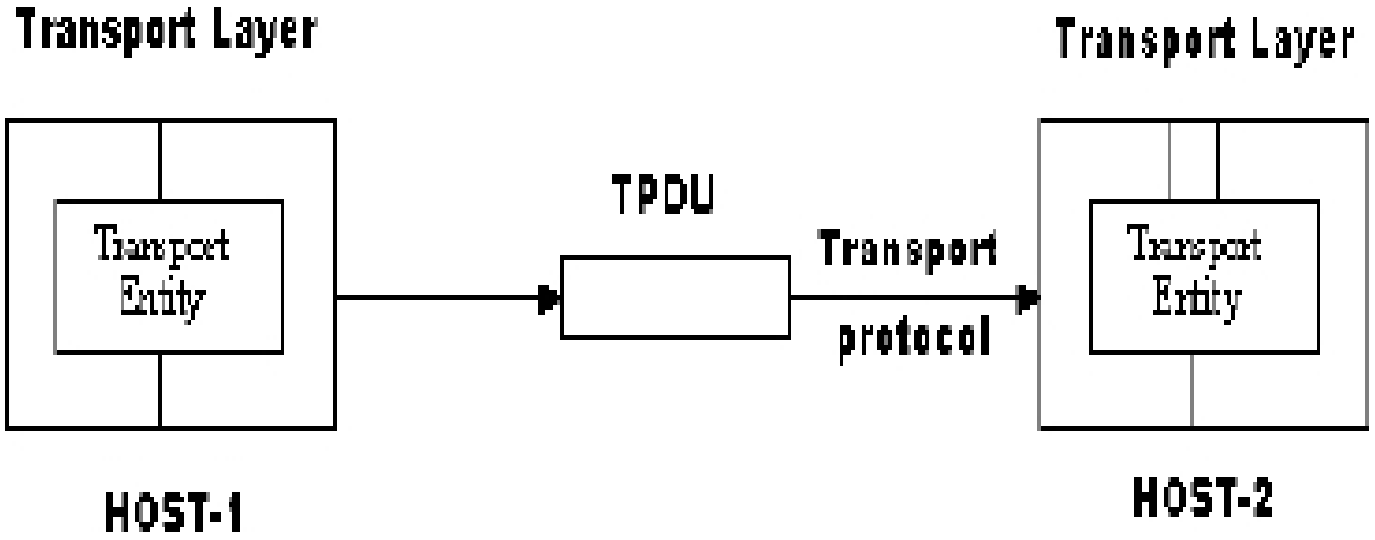
TPDU (Transport Protocol Data Unit)

Transmissions of message between 2 transport entities are carried out by TPDU.

•The transport entity carries out the transport service primitives by blocking the caller and sending a packet the service.

•Encapsulated in the payload of this packet is a transport layer message for the server's transport entity.

•The task of the transport layer is to provide reliable, cost-effective data transport from the source machine to the destination machine, independent of physical network or networks currently in use.


Transport Layer
Transport Layer
Transport Entity
TPDU
Transport protocol
Transport Entity
HOST-1
HOST-2

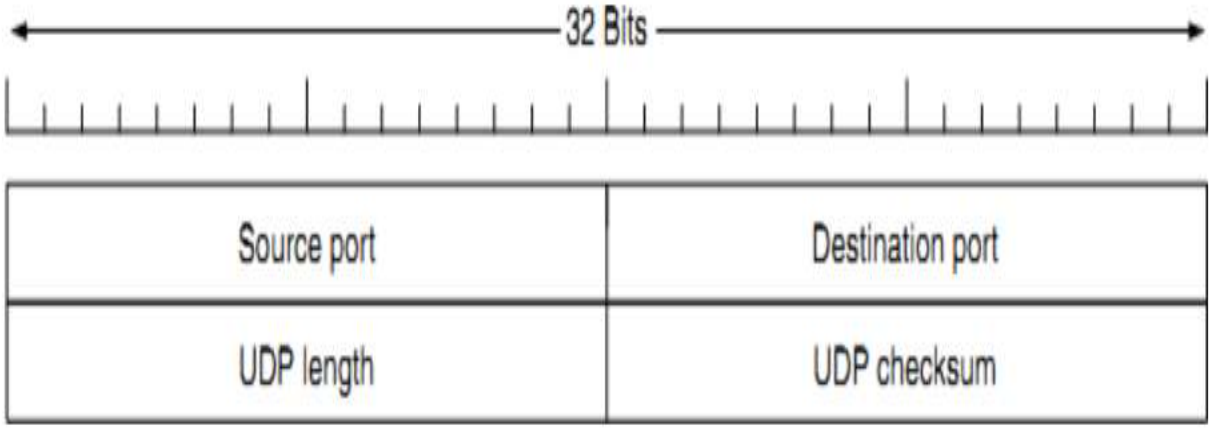
UDP (User Datagram Protocol)

A connectionless transport protocol called UDP (User Datagram Protocol). UDP provides a way for applications to send encapsulated IP datagrams without having to establish a connection.

➢ UDP transmits segments consisting of an 8-byte header followed by the pay-load. The two ports serve to identify the end-points within the source and destination machines.

➢ When a UDP packet arrives, its payload is handed to the process attached to the destination port.

UDP Header Format



Computer Networks

Introduction to Cryptography

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Introduction to Cryptography

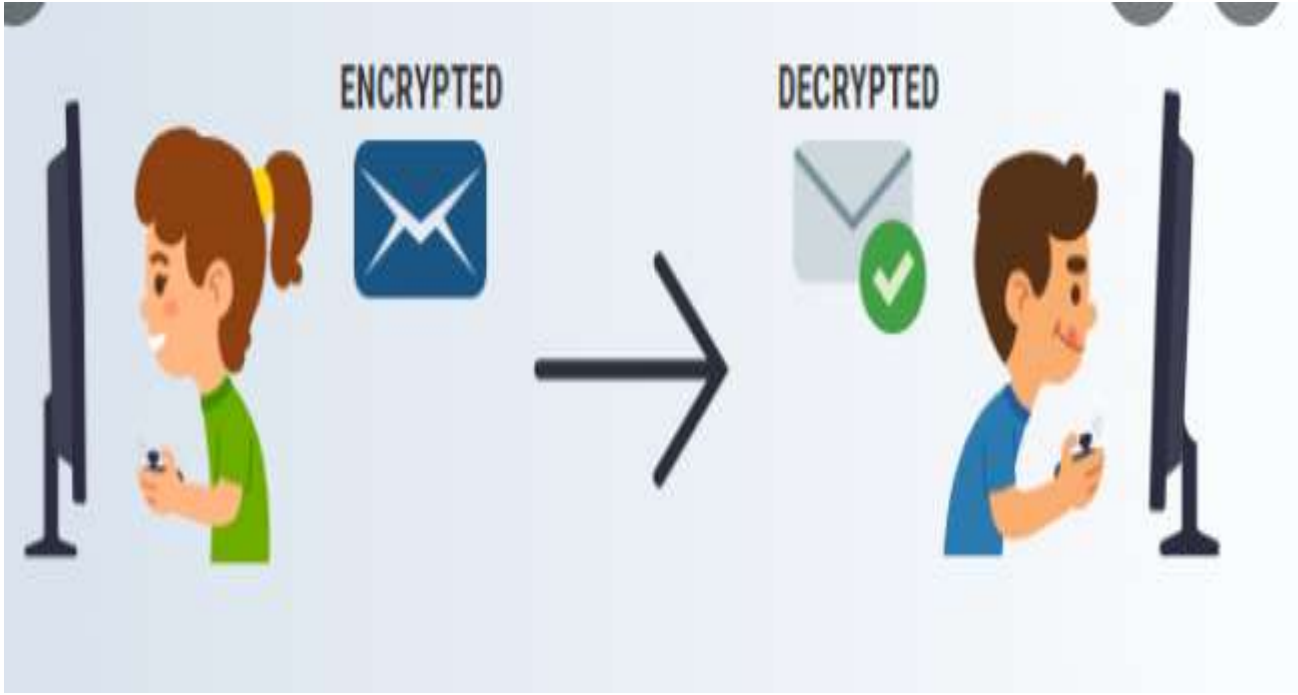
Computer Networks: MCA, I Year/II-Sem.

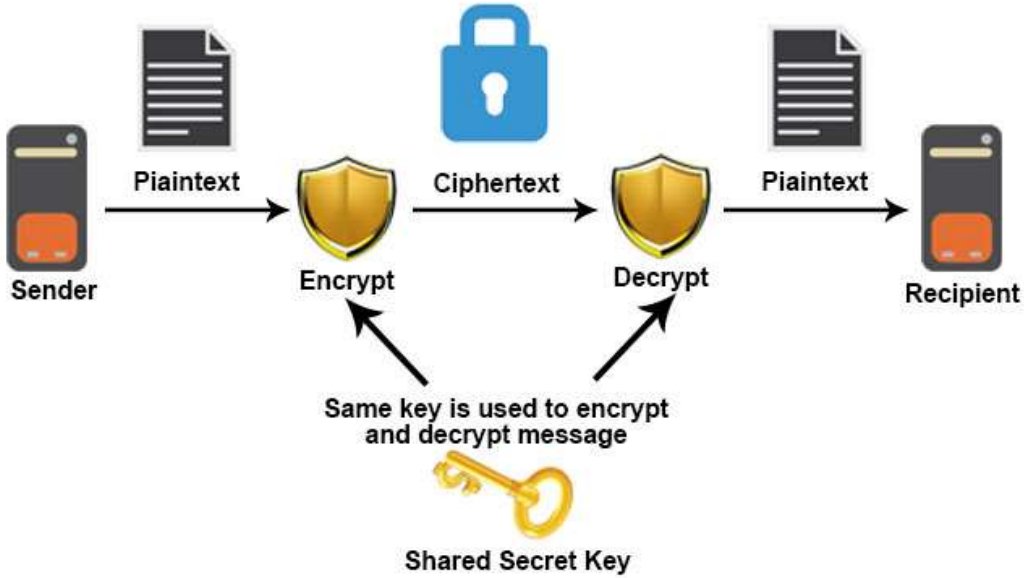
Cryptography

• Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.

• Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

• Cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption


ENCRYPTED
DECRYPTED


Piaintext
Ciphertext
Piaintext
Sender
Encrypt
Decrypt
Recipient
Same key is used to encrypt
and decrypt message
Shared Secret Key

Computer Networks

Cryptographic Algorithms-DES

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Cryptographic Algorithms-DES

Computer Networks: MCA, I Year/II-Sem.

Outline

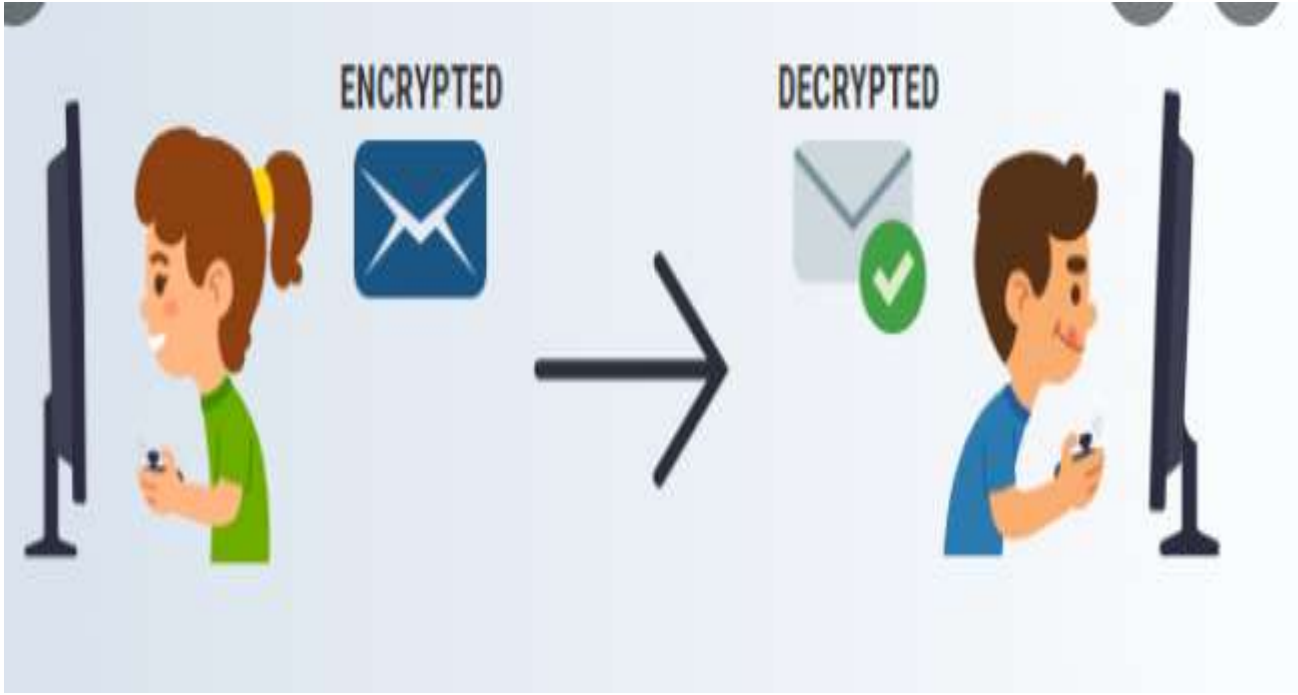
- What is Cryptography
- DES
- RSA
- Authentication Protocols

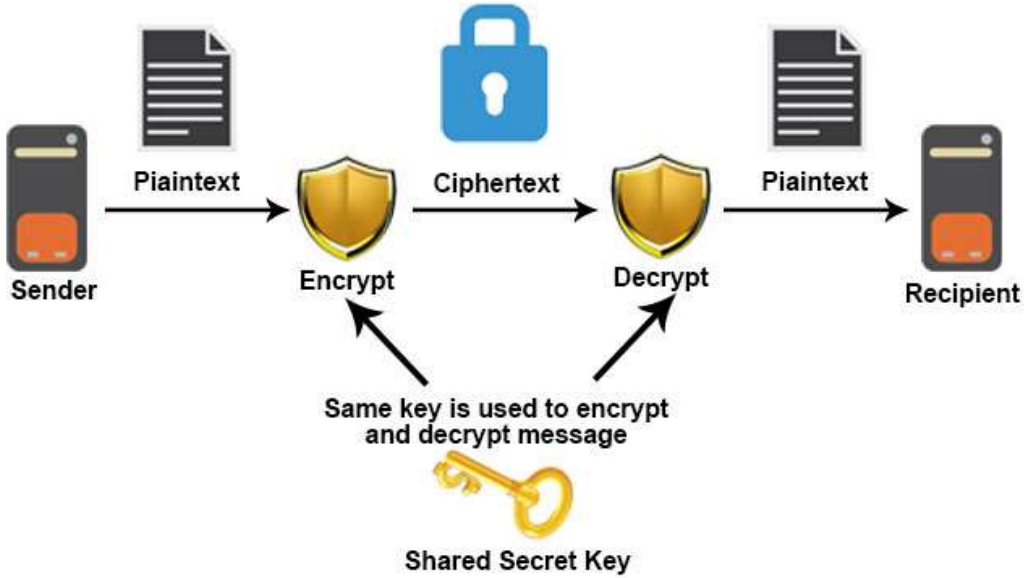
Cryptography

• Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.

• Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

• Cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption

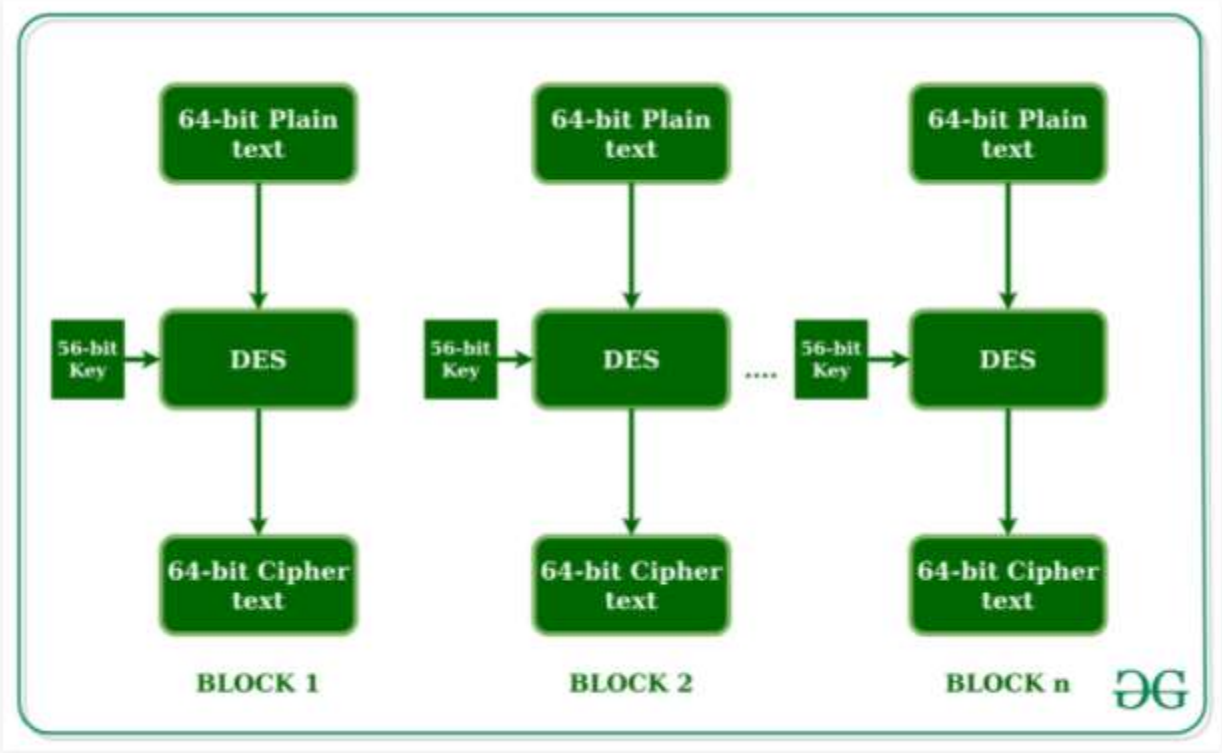

ENCRYPTED
DECRYPTED


Piaintext
Ciphertext
Piaintext
Sender
Encrypt
Decrypt
Recipient
Same key is used to encrypt
and decrypt message
Shared Secret Key

DES Algorithm

Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on decline. DES is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text.

The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.


64-bit Plain text
64-bit Plain text
64-bit Plain text
56-bit Key
DES
56-bit Key
DES
....
56-bit Key
DES
64-bit Cipher text
64-bit Cipher text
64-bit Cipher text
BLOCK 1
BLOCK 2
BLOCK n

•DES uses a 56 bit key. Actually, the initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56 bit key.

That is bit position 8, 16, 24, 32, 40, 48, 56 and 64 are discarded.

Steps in DES

• In the first step, the 64 bit plain text block is handed over to an initial Permutation (IP) function.

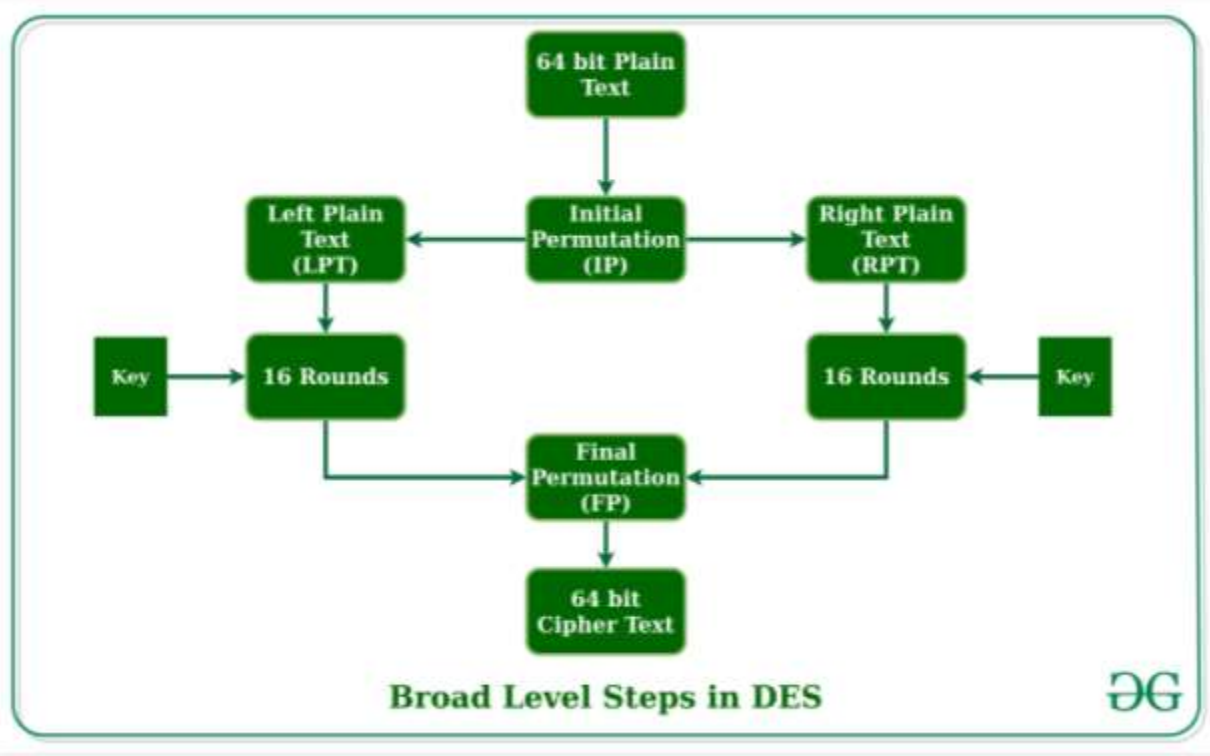
• The initial permutation performed on plain text.

• Next the initial permutation (IP) produces two halves of the permuted block; says Left Plain Text (LPT) and Right Plain Text (RPT).

• Now each LPT and RPT to go through 16 rounds of encryption process.

• In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block

• The result of this process produces 64 bit cipher text.


64 bit Plain Text
Initial Permutation (IP)
Left Plain Text (LPT)
Right Plain Text (RPT)
Key
16 Rounds
16 Rounds
Key
Final Permutation (FP)
64 bit Cipher Text
Broad Level Steps in DES

Computer Networks

Firewalls, DNS

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Firewalls, DNS

Computer Networks: MCA, I Year/II-Sem.

Outline

- What is a Firewall
- Types of Firewalls
- DNS

Firewall

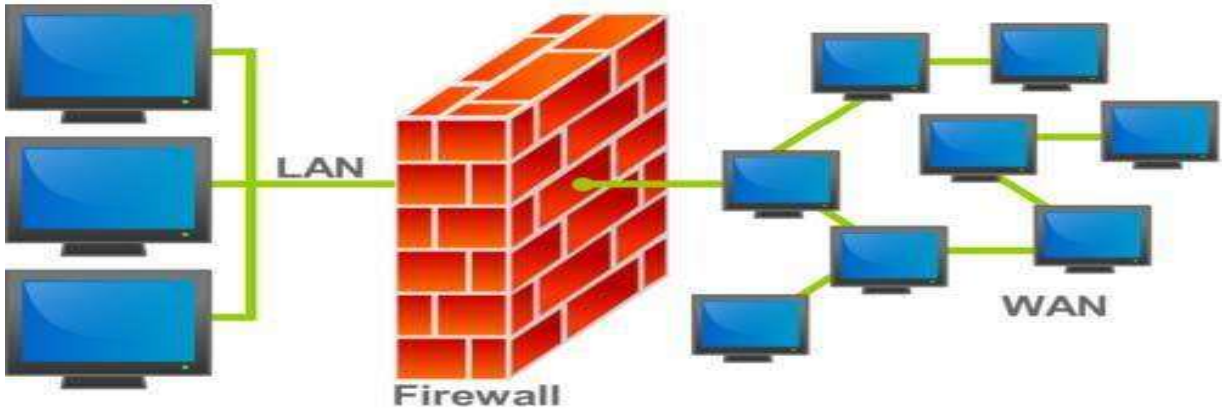
A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic

Reject : block the traffic but reply with an “unreachable error”

Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.


LAN
Firewall
WAN

Firewall is categorized into three basic types −

- Packet filter (Stateless & Statefull)
- Application-level gateway
- Circuit-level gateway

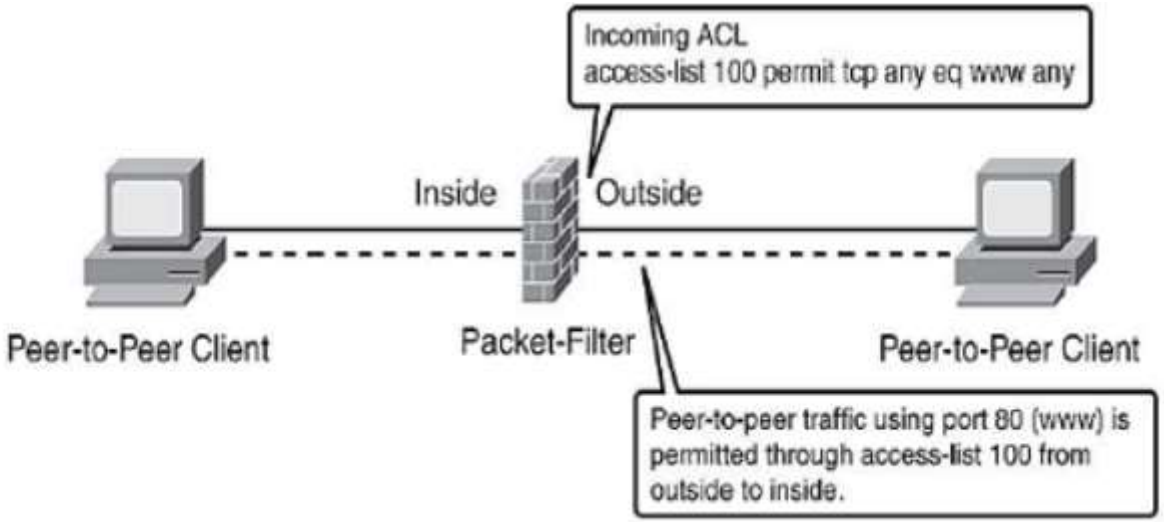
Packet filter Firewalls

Packet-filtering firewalls allow or block the packets mostly based on criteria such as source and/or destination IP addresses, protocol, source and/or destination port numbers, and various other parameters within the IP header.

The decision can be based on factors other than IP header fields such as ICMP message type, TCP SYN and ACK bits, etc.Packet filter rule has two parts −

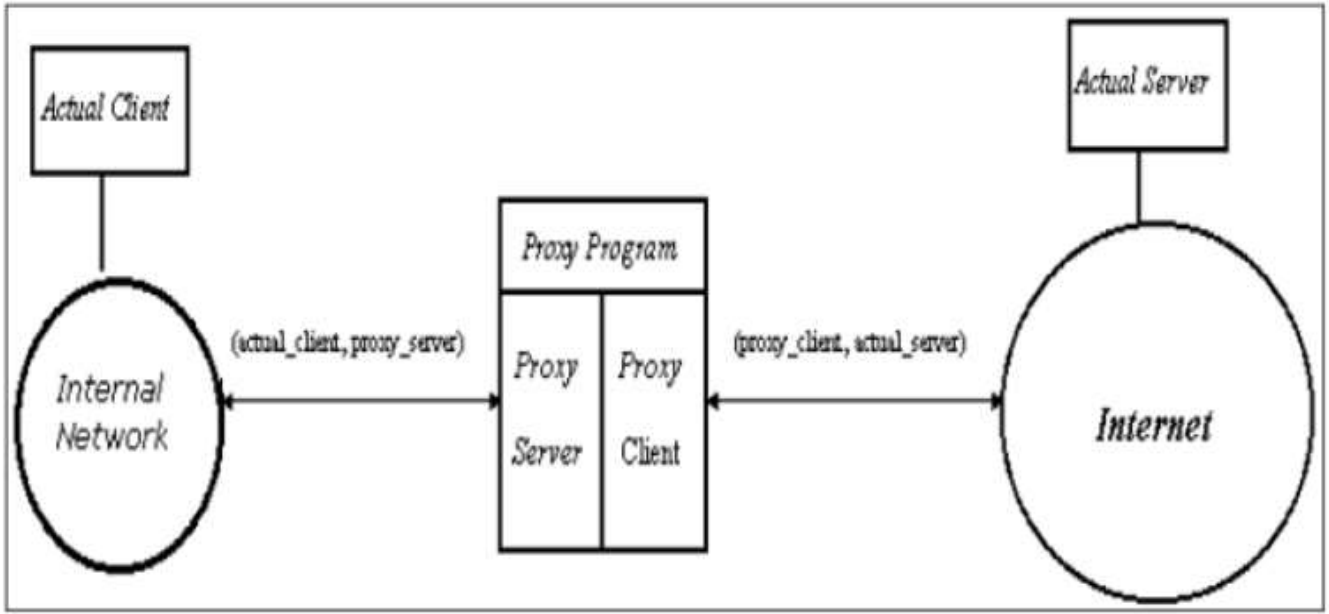
Selection criteria − It is a used as a condition and pattern matching for decision making.

Action field − This part specifies action to be taken if an IP packet meets the selection criteria. The action could be either block (deny) or permit (allow) the packet across the firewall.


Incoming ACL
access-list 100 permit tcp any eq www any
Inside
Outside
Peer-to-Peer Client
Packet-Filter
Peer-to-Peer Client
Peer-to-peer traffic using port 80 (www) is permitted through access-list 100 from outside to inside.

Application Gateways Firewalls

- An application-level gateway acts as a relay node for the application-level traffic.
- They intercept incoming and outgoing packets, run proxies that copy and forward information across the gateway, and function as a ***proxy server***, preventing any direct connection between a trusted server or client and an un-trusted host.
- The proxies are application specific. They can filter packets at the application layer of the OSI model.


Actual Client
Actual Server
Proxy Program
Internal Network
(actual_client, proxy_server)
Proxy Server
Proxy Client
(proxy_client, actual_server)
Internet

Circuit-Level Gateway

• The circuit-level gateway is an intermediate solution between the packet filter and the application gateway.

• It runs at the transport layer and hence can act as proxy for any application.

• Similar to an application gateway, the circuit-level gateway also does not permit an end-to-end TCP connection across the gateway.

• It sets up two TCP connections and relays the TCP segments from one network to the other. But, it does not examine the application data like application gateway. Hence, sometime it is called as ‘Pipe Proxy’

DNS(Domain Name System)

DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

Requirement

Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address


www.wikipedia.org?
91.198.174.192

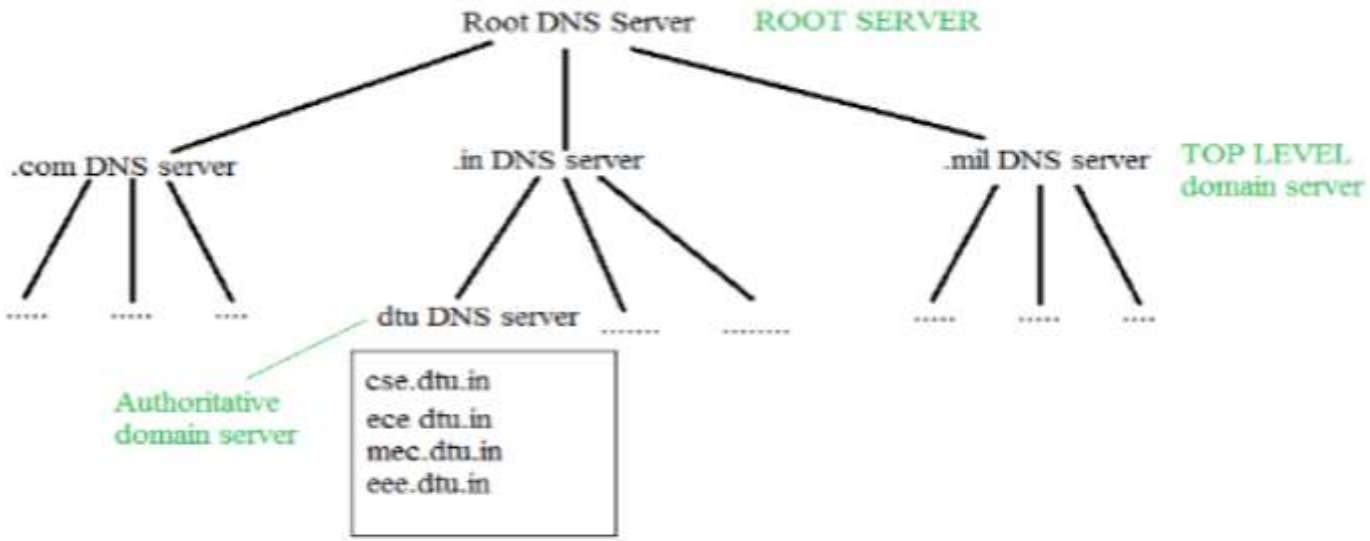
Domain :

There are various kinds of DOMAIN :

Generic domain : .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.

Country domain .in (india) .us .uk

Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping.So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type nslookup www.geeksforgeeks.org.


Root DNS Server
ROOT SERVER
.com DNS server
.in DNS server
.mil DNS server
TOP LEVEL
domain server
dtu DNS server
Authoritative
domain server
cse.dtu.in
ece dtu.in
mec.dtu.in
eee.dtu.in

Hierarchy of Name Servers

Root name servers –

It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.

Top level server –

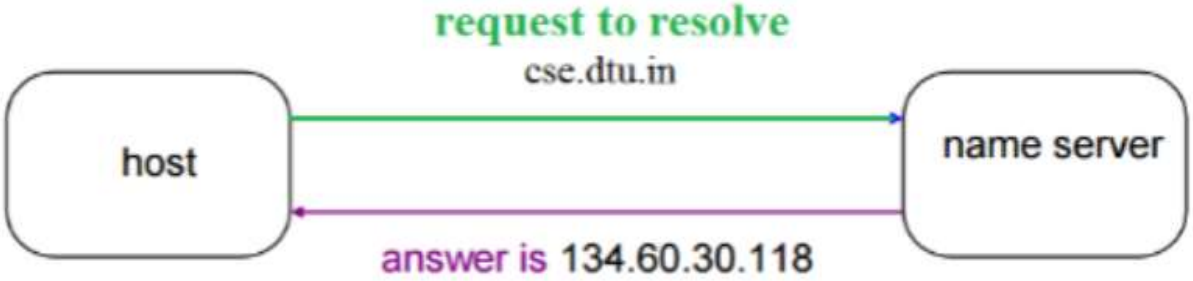
It is responsible for com, org, edu etc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the second level domains.

Authoritative name servers

This is organization’s DNS server, providing authoritative hostName to IP mapping for organization servers. It can be maintained by organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative ip address.

Name to Address Resolution

A host wants the IP address of cse.dtu.in



Namespace –

Set of possible names, flat or hierarchical . Naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value –

Name server –

It is an implementation of the resolution mechanism.. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree

Computer Networks

Cryptographic Algorithms-RSA

Presented By:

K. Praveen Kumar

Assistant Professor

MCA

GIET(A)

Lecture Details:

Topic : Cryptographic Algorithms

Computer Networks: MCA, I Year/II-Sem.

Outline

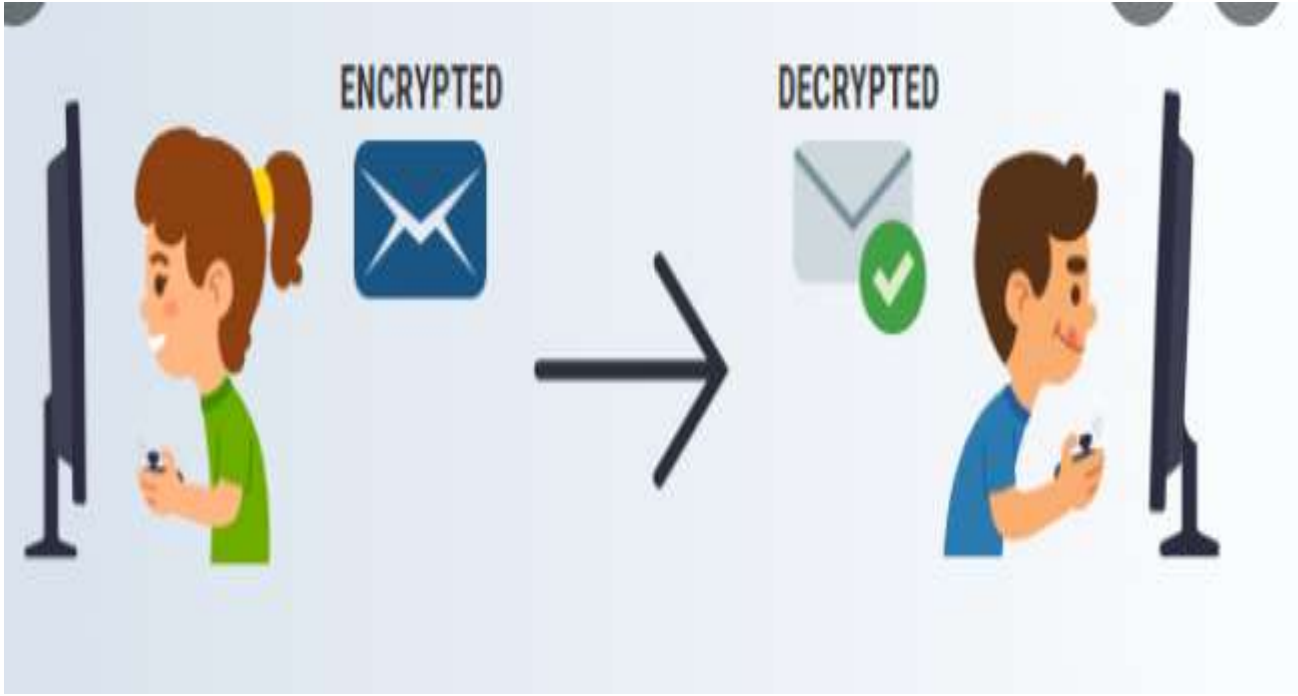
- What is Cryptography
- RSA
- Authentication Protocols

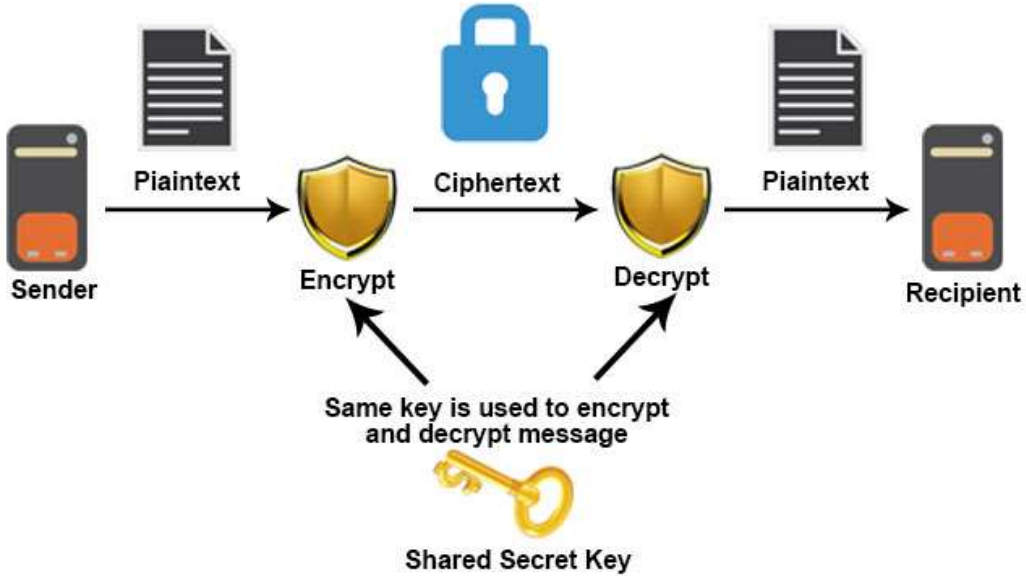
Cryptography

• Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.

• Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

• Cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption


ENCRYPTED
DECRYPTED


Piaintext
Ciphertext
Piaintext
Sender
Encrypt
Decrypt
Recipient
Same key is used to encrypt
and decrypt message
Shared Secret Key

RSA

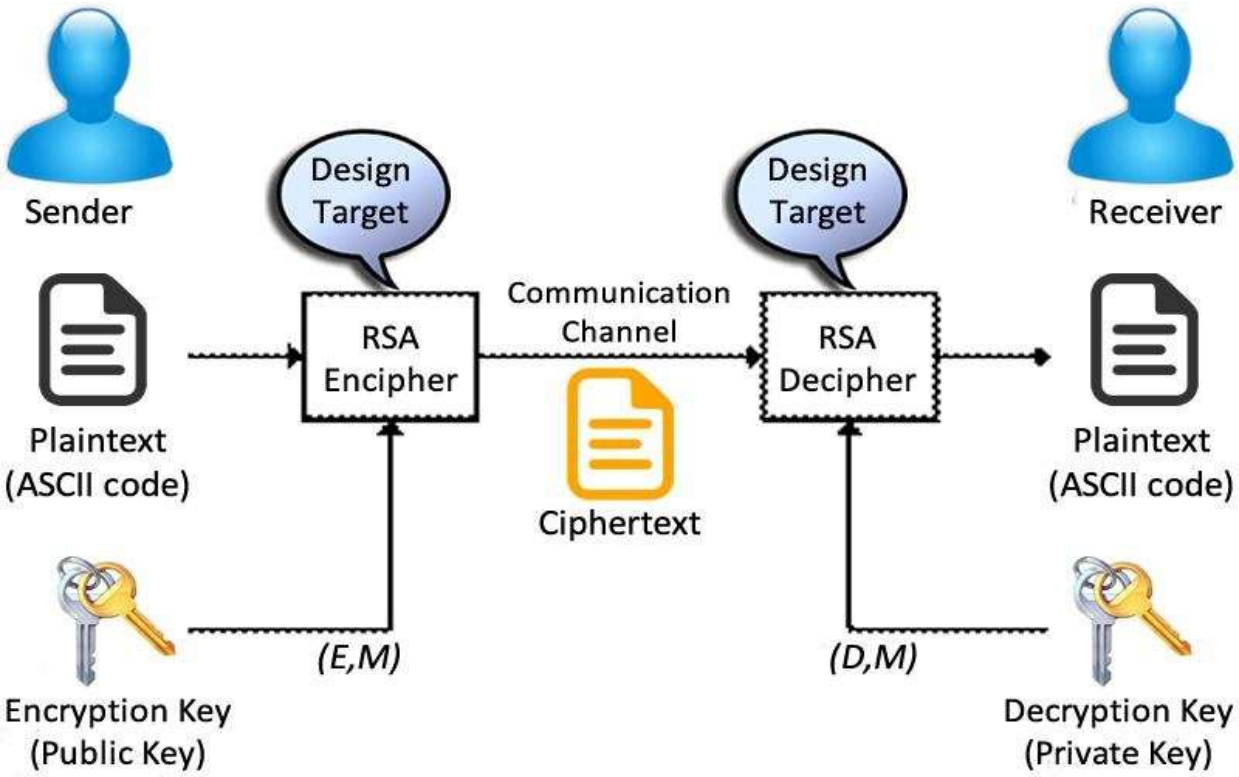
• RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.**

• As the name describes that the Public Key is given to everyone and Private key is kept private. **The idea!** The idea of RSA is based on the fact that it is difficult to factorize a large integer.

• The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers.

• So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially.

• RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task


Sender
Design Target
Design Target
Receiver
Plaintext (ASCII code)
RSA Encipher
Communication Channel
RSA Decipher
Plaintext (ASCII code)
Ciphertext
(E,M)
(D,M)
Encryption Key (Public Key)
Decryption Key (Private Key)

Key Generation

Select p, q	p, q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Authentication Protocols

User authentication is the first most priority while responding to the request made by the user to the software application. There are several mechanisms made which are required to authenticate the access while providing access to the data. In this blog, we will explore the most common authentication protocols and will try to explore their merits and demerits

Kerberos

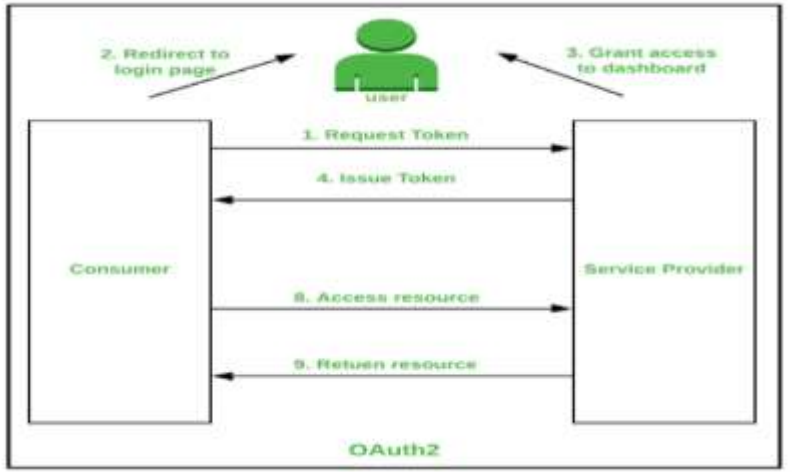
- Kerberos is a protocol that aids in network authentication.
- This is used for validating clients/servers during a network employing a cryptographic key
- It is designed for executing strong authentication while reporting to applications.
- The overall implementation of the Kerberos protocol is openly available by MIT and is used in many mass-produced products

Lightweight Directory Access Protocol (LDAP)

- LDAP refers to Lightweight Directory Access Protocol.
- It is a protocol that is used for determining any individuals, organizations, and other devices during a network regardless of being on public or corporate internet.
- It is practiced as Directories-as-a-Service and is the grounds for Microsoft building Activity Directory.

OAuth2

OAuth as the name suggests it is an authorization framework that promotes granting limited access to the user on its account through an HTTP service. When a user requests access to resources an API call is made and after the authentication token is passed.



Security Assertion Markup Language

• SAML stands for Security Assertion Markup Language which is based on XML-based authentication data format which provides the authorization between an identity provider and service provider. It serves as a product of the OASIS Security Services Technical Committee.