

Computer Network

for

Computer Science & Information Technology

By

Siddharth S. Shukla

(BE (CSE), ME(CTA))

- **12 Year teaching experience in CS & IT**
- **Ex. Faculty Bhilai Institute of Technology Durg**
(From 2004 to 2013)
- **Published a number of paper in National & International Journals**
- **150+ Student selected in IITs | IISc | IIITs under my guidance**

Copyright©,i-gate publication
Third edition 2021

All right reserved

No part of this book or parts thereof may be reproduced, stored in a retrieval system or transmitted in any language or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of the publisher.

Computer Network

Syllabus –

ISO/OSI stack

- Functionality of seven layers of OSI model
- Functionality of four layers of TCP/IP model

Internetworking devices

- Hubs
- Switches
- Gateways
- Routers

Flow control techniques:

Error Control Technique:

- Parity Check
- Checksum
- CRC

Sliding Window protocol

- Stop N Wait ARQ
- Go Back N ARQ
- Selective Repeat ARQ

LAN technologies (Ethernet,Token ring)

- Aloha system
- Ethernet: Persistent and non persistent CSMA/CD
 - Exponential Backoff algorithm
 - Efficiency
- Token ring:
 - Flow and error control techniques

TCP/UDP and sockets

- Header format of TCP
- TCP connection management
- TCP transmission policy
- TCP optimization
- TCP congestion control mechanism
- TCP timer management
- State transition diagram of TCP
- Header format of UDP
- Protocols used for TCP
- Protocols used for UDP

Routing algorithms

- Dijkstra's algorithm
- Distance vector routing protocol
- Link state routing protocol

IP(v4)

- Frame format
- Different class (A,B,C etc.) addressing
- Supernetting

- Subnetting
- IPv4 - Reserved Addresses

IP(V6)

Application layer protocols

- ICMP
- DNS
- SMTP
- POP
- FTP
- HTTP

Network security

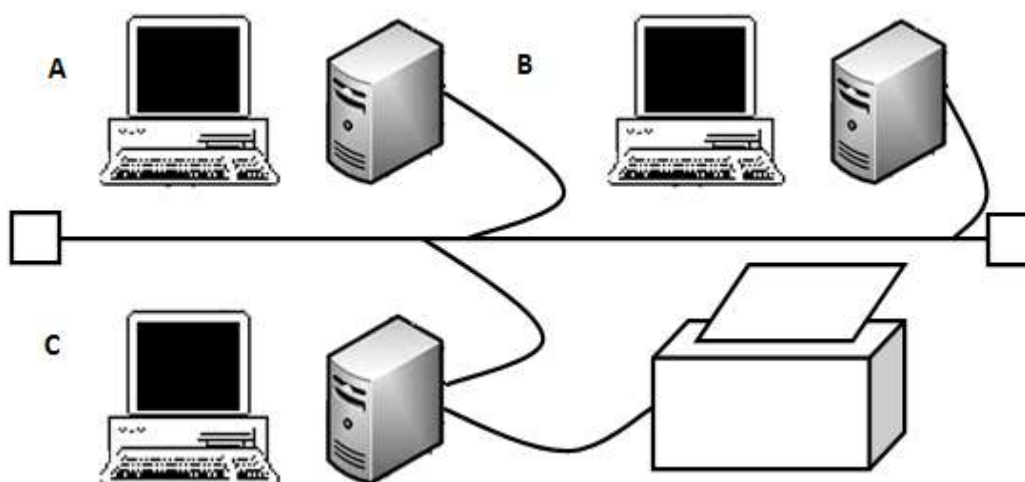
- Basic concepts of public key and private key cryptography
- Digital signature
- firewalls

Textbooks : “Computer Network”

- “Computer Network” - Peterson & Davie
 - “Algorithms” by Dr. M. N. Seetaramanth Tata McGraw Hill publication
 - Introduction Algo:CLRS, Dasgupta, Vazirani
 - “Data Communications and Networking”-William Stallings
-

Computer Network

- Connecting of several computing device together by data communication system.
- A network is basically a communication system for computers
- Computer network connects two or more autonomous computers
- The computers can be geographically located anywhere.
- Network in small geographical Area (Room, Building or a Campus) is called LAN (Local Area Network)
- Network in a City is call MAN (Metropolitan Area Network)
- Network spread geographically (Country or across Globe) is called WAN (Wide Area Network)



Goals/ Applications of computer Networking

1. Program and file sharing

Software resources can also be used more effectively over a network. With stand-alone computer (o. e; not connected to network), the software used on the computer must be present on each computer's hard disk. It is also difficult and time consuming to install and configure the software individually on every computer. With a network one can centrally install and configure the software, which can be accessed at the entire connected computer.

2. Network Resource sharing

Network resources include printers, plotters, Fax, modems, scanners, floppy disks, CD-ROMS and storage devices (i.e. Hard disks) which can be shared by terminals connected to network. For example the sharing of a resource such as a storage device.

3. Database sharing

A database program is an ideal application for a network. A network feature called record locking lets multiple users simultaneously access a file without corrupting the data. Record locking insures that no two users edit the same record at the same time.

4. Economical Expansion of the PC Base

Networks provide an economical way to expand the number of computers in an organization.

5. Ability to network software

A class of software called Groupware is designed specifically for networks. It lets users interact and coordinate their activities.

Note: Not all software will use a network even if one is installed. You should check the software documentation to see what features, if any, the software provides in a network environment.

6. Ability to use electronic mail

Electronic mail lets users easily communicate with one another. Messages are dropped in “mailboxes” for the recipients to read at a convenient time.

7. Creation of workgroups

Groups are important in networks. They can consist of users who work in a department or who are assigned to special project. With Netware, one can assign users to groups and then give each group access to special directories and resources not accessible by other users. This saves the trouble to assigning access to each individual user.

8. Centralized Management

Because Netware user’s dedicated servers can be grouped in on location, along with the shared resource attached to them, for easier management.

Hardware upgrades, software backups, system maintenance and system protection are much easier to handle when these devices are in a location.

9. Security

A network provides more secure environment for a company’s important information. Security starts with the login procedure to ensure that a user accesses the network using his or her own account. This account is tailored (i.e. made according to the user requirements) to give the user access only to authorized areas of the server and the network. Login restrictions can force a user a log in at one specific station and only during specific time frame or period.

10. Access to more than one operating system

Netware provides connections for many different operating system, including DOS, OS/2, UNIX, and Apple Talk. Users of these system can access files on the Netware server.

11. Enhancement of the corporate structure

Networks can change the structure of an organization and the way it is managed. Users who work in a specific department and for a specific manager no longer need to be in the same

physical area. Their offices can be located in areas where their expertise is most needed. The network ties them to their department managers and systems. This arrangement is useful for special project in which individuals from different departments, such as research, production and marketing, need to work closely with each other.

Layer Architecture Model

- Layer architecture simplifies the network design.
- It is easy to debug network applications in a layered architecture network.
- The network management is easier due to the layered architecture.
- Network layers follow a set of rules, called protocol.
- The protocol defines the format of the data being exchanged, and the control and timing for the handshake between layers.

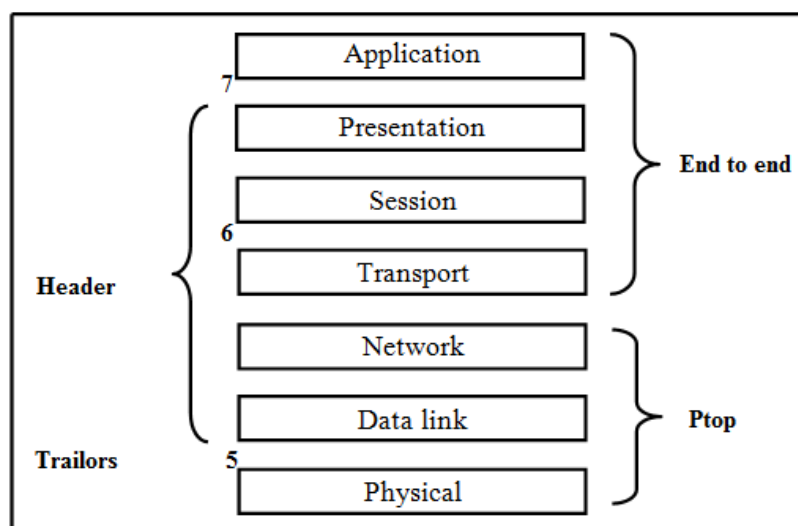


Figure OSI model

Open System Interconnection (OSI)

- International standard organization (ISO) established a committee in 1977 to develop an architecture for computer communication.
- Open Systems Interconnection (OSI) reference model is the result of this effort.
- In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.
- Term “open” denotes the ability to connect any two systems which conform to the reference model and associated standards.
- The Open Systems Interconnection (OSI) model is a reference tool for understanding data communications between any two networked systems.
- It divides the communications processes into seven layers depend on the functionality and responsibilities of the layers.

- Each layer both performs specific functions to support the layers above it and offers services to the layers below it.
- The three lowest layers focus on passing data from end to end communication.
- The top four layers come into play in the end system to complete the process.



- The process of breaking up the functions or tasks of networking into layers reduces complexity.
- Each layer provides a service to the layer above it in the protocol specification.
- Each layer communicates with the same layer's software or hardware on other computers.
- The lower 3 layers (network, data link and physical —Layers 3, 2, and 1) are concerned with the flow of data from end to end through the network.
- The lower 3 layers (network, data link and physical —Layers 3, 2, and 1) are hardware oriented layers.
- The layer 4 transport layer is use to provide interface between lower 3 layers and upper 3 layers.
- The upper 3 layers of the OSI model (application, presentation and session—Layers 7, 6 and 5) are orientated more toward services to the applications.
- The upper 3 layers of the OSI model (application, presentation and session—Layers 7, 6 and 5) are user oriented layers.
- Data is encapsulated with the necessary protocol information as it moves down the layers before network transit.

Physical Layer

- Responsibilities:
 1. Bit Presentation
 2. Transmission Mode
 3. Link Configuration
 4. Topological Configuration
 5. Data Rate
- Provides physical interface for transmission of information.

- Defines rules by which bits are passed from one system to another on a physical communication medium.
- Covers all - mechanical, electrical, functional and procedural - aspects for physical communication.
- Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.

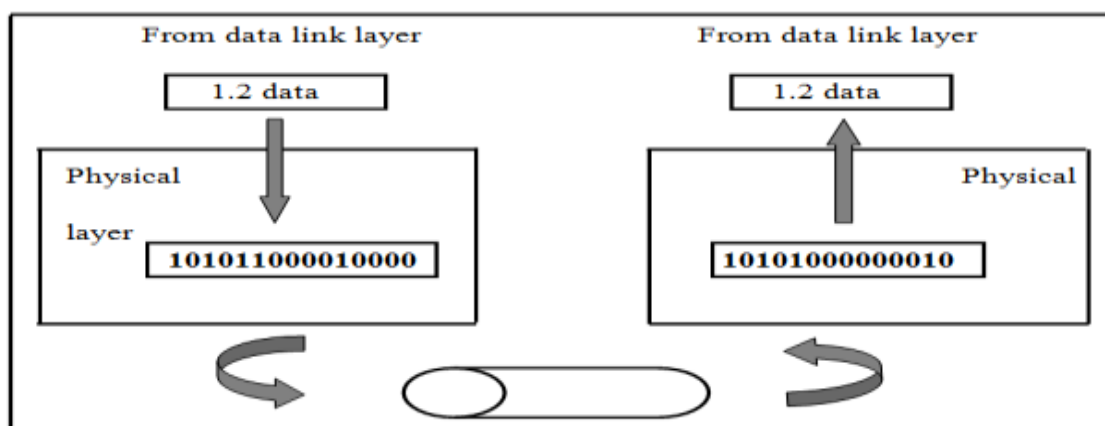


Figure Physical layer

Data Link Layer

- Responsibilities:
 - Error Control
 - Flow Control
 - Access Control
 - Framing
 - Physical Addressing System
- The data link layer transmits frames of data from computer to computer on the same network segment.

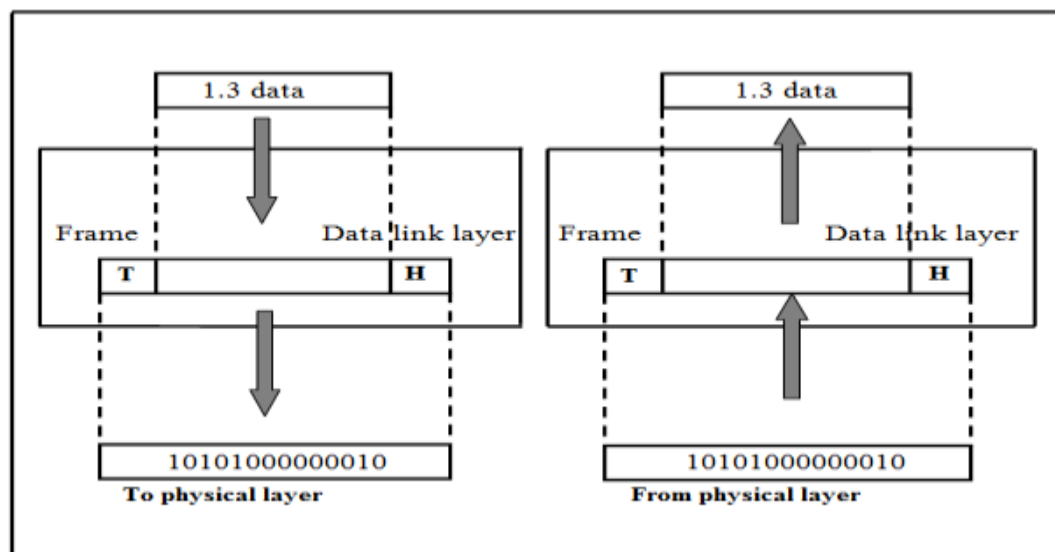


Figure Data link layer

- The data link layer is divided into two sub layers:
 1. MAC layer
 2. LLC layer
- The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer.
- The MAC sub layer controls. How a computer on the network gains access to the data and permission to transmit it.
- The LLC layer controls frame synchronization, flow control and error checking.

Network Layer

- Responsibilities:
 - Logical addressing system
 - Routing
 - Congestion
 - Feedback Message

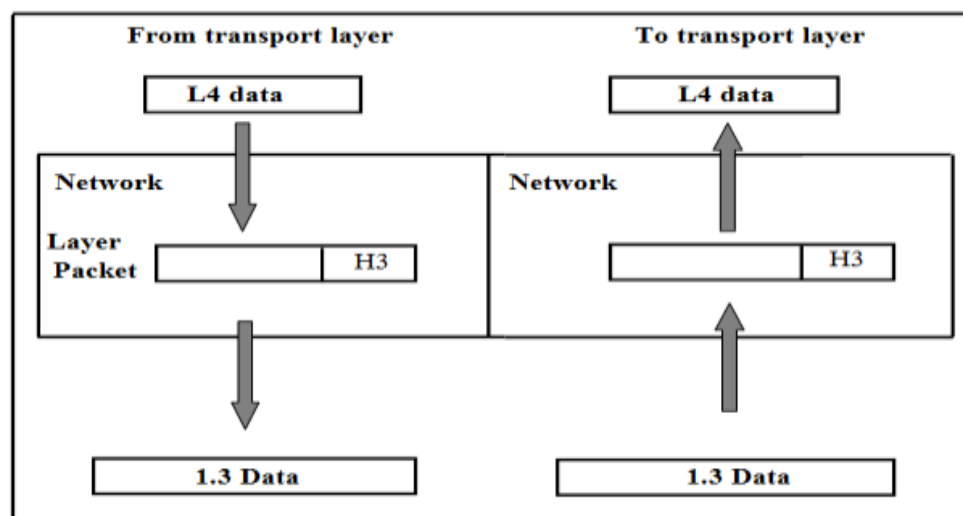


Figure Network Layer

- Implements routing of frames (packets) through the network.
- Defines the most optimum path the packet should take from the source to the destination
- Defines logical addressing so that any endpoint can be identified.
- The Internet Protocol (Ip) addresses make networks easier to both set up and connect with one another.
- The Internet uses IP addressing to provide connectivity to millions of networks around the world.
- Handles congestion in the network.
- Facilitates interconnection between heterogeneous networks (Internetworking).
- The network layer also defines how to fragment a packet into smaller packets to accommodate different media.
- All reassembly of fragmented packets happens at the network layer of the final destination system.

Transport Layer

- Responsibilities:
 - Error Control
 - Flow Control
 - Segmentation and reassembly
 - Multiplexing and demultiplexing
 - Service point addressing system (Port Number)
- Purpose of this layer is to provide a reliable mechanism for the exchange of data between two processes in different computers.
- Ensures that the data units are delivered error free.
- Ensures that data units are delivered in sequence.
- Ensures that there is no loss or duplication of data units.
- Provides connectionless or connection oriented service.
- Provides for the connection management.
- Multiplex multiple connection over a single channel
- Depending on the application, the transport layer either offers reliable, connection-oriented or connectionless, best-effort communications..
- The most common transport layer protocols are the connection-oriented TCP
- Transmission Control Protocol (TCP) and the connectionless UDP User Datagram Protocol (UDP).

Specific responsibilities of the transport layer include the following:

- **Service-point addressing:** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not from one computer

to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header therefore must include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

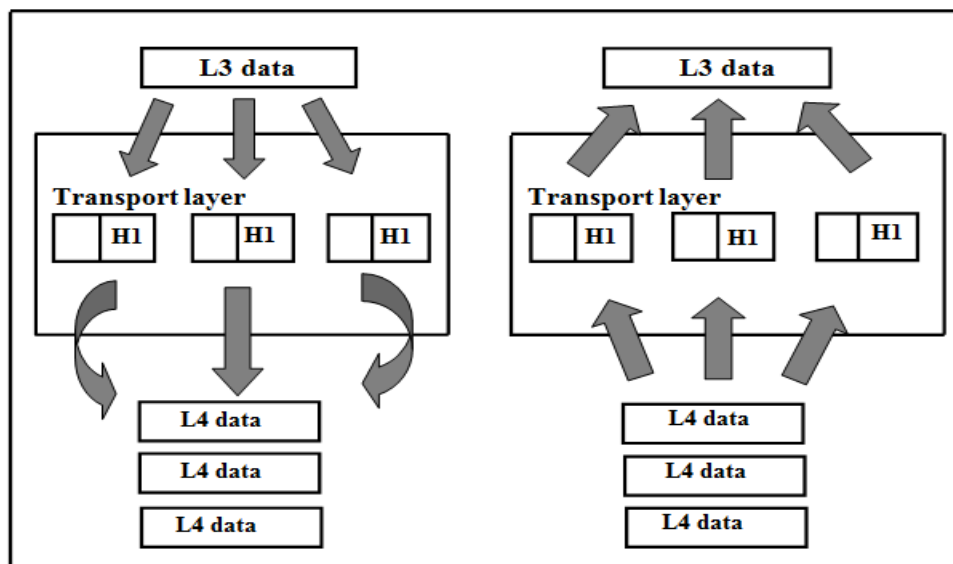


Figure Transport layer

- **Segmentation and reassembly:** A message is divided into transmittable segments, each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in the transmission.
- **Connection control:** The transport layer can be either connectionless or connection-oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
- **Flow control:** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- **Error control:** Like the data link, the transport layer is responsible for error control. However, error control at this layer is performed end-to-end rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error. (damage, loss, or duplication). Error correction is usually achieved through retransmission.

Example

In below figure shows an example of transport layer. Data coming from the upper layers have service-point (port) addresses j and k (j is the address of the sending

application and k is the address of the receiving application). Since the data size is larger than the network layer can handle, the data are split into packets, each packet retaining the service-point addresses (j and k). Then in the network layer, network addresses (A and P) are added to each packet. The packets may travel on different paths and arrive at the destination either in order or out of order. The two packets are delivered to the destination network layer, which is responsible for removing the network layer headers. The two packets are now passed to the transport layer, where they are combined for delivery to the upper layers.

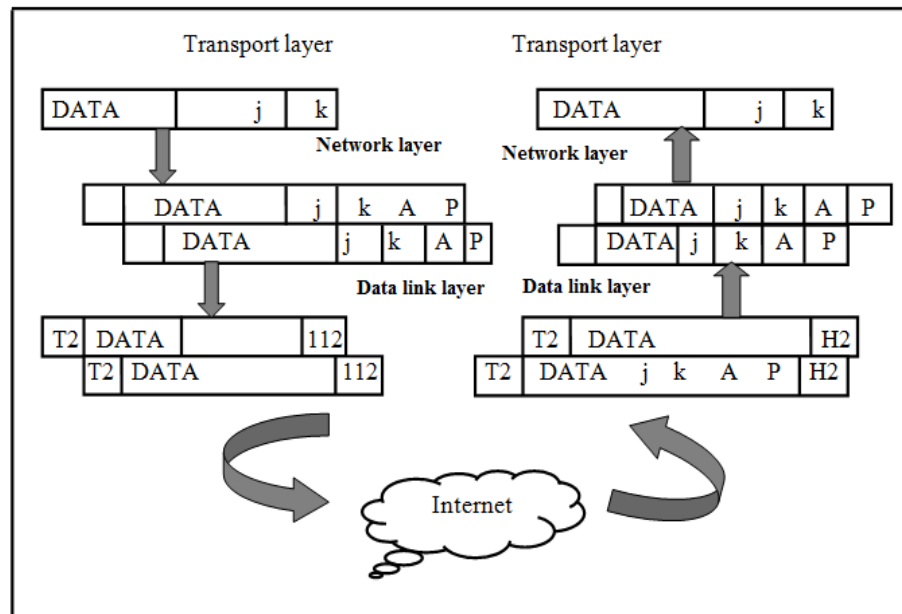


Figure Transport layer (Example)

Session Layer

- Responsibilities:
 - Dialog Control
 - Managing Check Point
 - Grouping of operations
- Session layer provides mechanism for controlling the dialogue between the two end systems. It defines how to start, control and end conversations (called sessions) between applications.
- This layer requests for a logical connection to be established on an end-user's request.
- Any necessary log-on or password validation is also handled by this layer.
- Session layer is also responsible for terminating the connection.
- This layer provides services like dialogue discipline which can be full duplex or half duplex.
- Session layer can also provide check-pointing mechanism such that if a failure of some sort occurs between checkpoints, all data can be retransmitted from the last checkpoint.

Synchronization

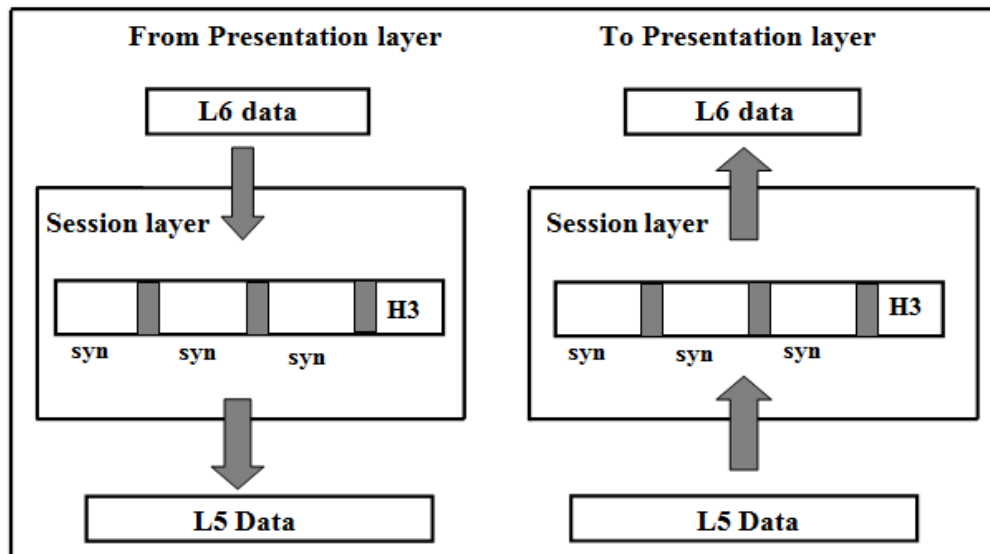


Figure Session layer

Presentation Layer

- The presentation layer, is responsible for how an application formats the data to be sent out onto the network.
- The presentation layer basically allows an application to read (or understand) the message.
- Examples of presentation layer functionality include:
 - Encryption and decryption of a message for security
 - Compression and expansion of a message so that it travels efficiently
 - Graphics formatting
 - Content translation
 - System-specific translation

Below Figure shows the relationship between this layer and the application layer and session layer,

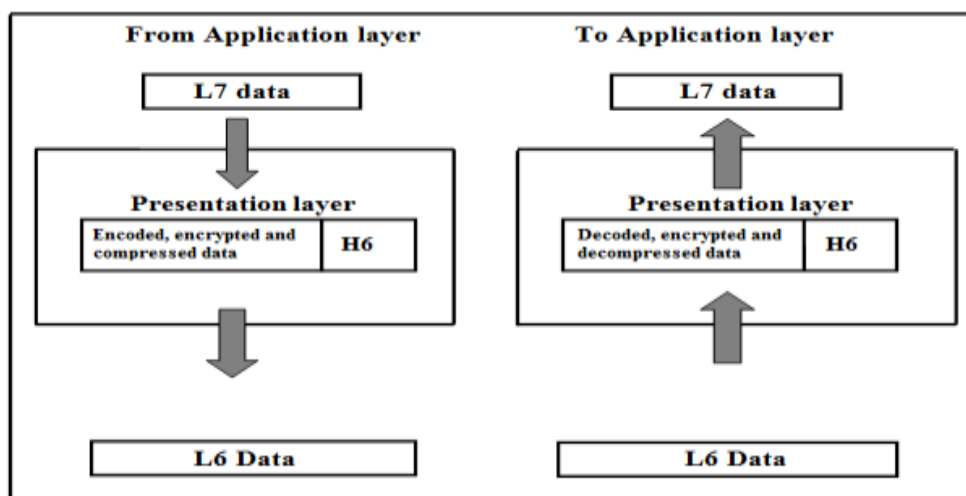


Figure Presentation layer

Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as email, remote file access and transfer, shared database management and other type of distributed information services.

Figure shows the relationship of the application layer to the user and the presentation layer.

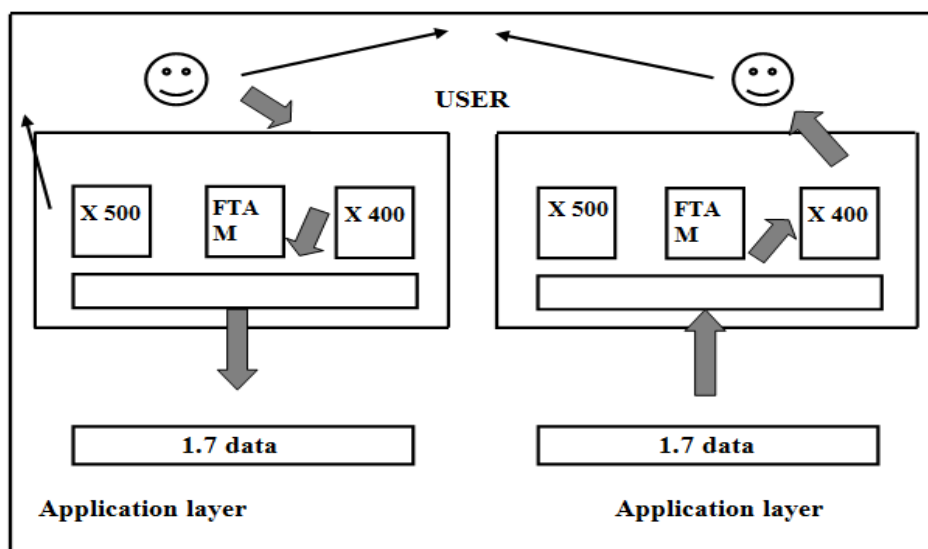


Figure Application Layer

- Examples of application layer functionality include:
 - Support for file transfers
 - Ability to print on a network
 - Electronic mail
 - Electronic messaging
 - Browsing the World Wide Web
- HTTP(for the secure transfer of web page related to file)
- FTP(file transfer protocol)
- SMTP(simple mail transfer protocol)
- Notes:
 - Biggest Layer is transport layer.
 - Complex layer is network layer
 - Optional layer is session layer

Summary of Layer Functions

The function of the seven layers are summarized in below Figure

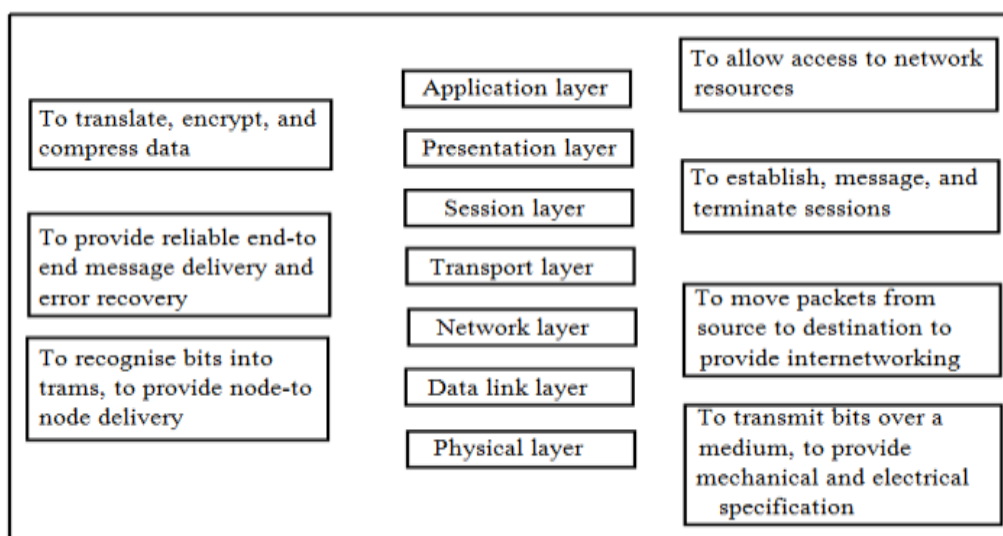
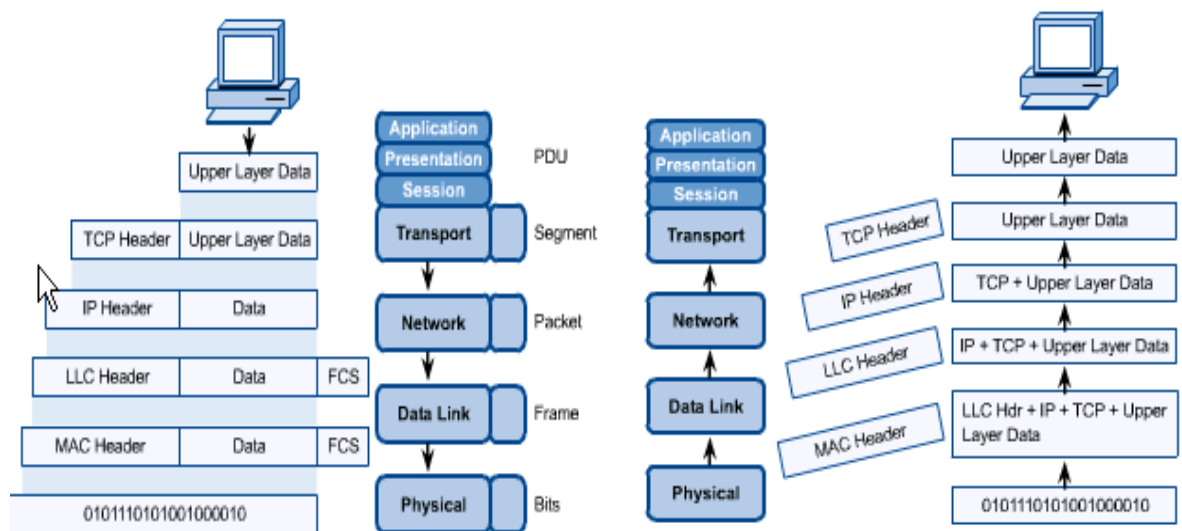


Figure Summary of layer functions

Layer	Common Protocols	Devices
Application	DNS; FTP;TFTP; BOOTP; SNMP;RLOGIN;SMTP; MIME; NFS; FINGER;TELNET;NCP; APPC;AFP; . 5MBSSH telnet FTP	Gateway
Presentation	HTTP,SMTP,SNMP	Gateway, Redirector
Session	RPC, Named Pipes, NETBIOS	Gateway
Transport	TCP UDP	Gateway, Brouter
Network	IP IGMP ICMP	Brouter Router
Data Link	Logical Link Control: 802.1 OSI model 802.2 toot cal Link Control Media Access Control: 802.3 CSMMCD (Ethernet), 802.4 (Token Bus) 802.5 (Token Ring)	Bridge, Switch
Physical	IEEE 802, IEEE 802.2, ISDN	Repeater, Multiplexer , Hubs, Amplifier

OSI in Action:

- A message begins at the top application layer and moves down the OSI layers to the bottom physical layer.
- As the message descends, each successive OSI model layer adds a header to it.
- A header is layer-specific information that basically explains what functions the layer carried out.
- Conversely, at the receiving end, headers are striped from the message as it travels up the corresponding layers.



TCP/IP

- **TCP/IP Application Layer (layer 4):**

The TCP/IP application layer handles all high level protocols that the Application, Presentation and Session layers of the OSI model handle, including encoding and dialogue control issues.

- **TCP/IP Transport Layer (layer 3):**

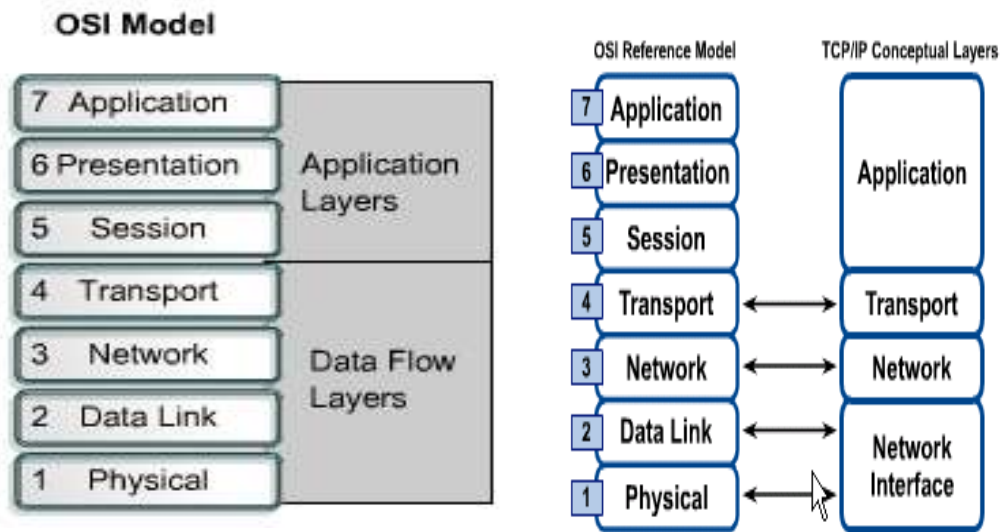
The TCP/IP transport layer uses two protocols, Transport Control Protocol (TCP) and User Datagram Protocol (UDP), which deal with connection-oriented and connection-less communication respectively. TCP provides reliable, low-error network communication using packet switching, while UDP provides a low overhead connection-less alternative.

- **TCP/IP Internet Layer (layer 2):**

The internet layer of TCP/IP is based entirely around one protocol, the Internet Protocol (IP). This layer has very Similar functions to the OSI Network Layer. Its primary function is to negotiate the best path to a destination.

- **TCP/IP Network Layer (layer 1):**

The TCP/IP network layer combines the tasks of the OSI Physical and Data Link Layers into one layer.



Advantage:

- It is use divide and conquer principle therefore maintenance and administration easy.
- It is use OO principle abstraction and encapsulation

Disadvantage:

- Duplication of functionalities.
- Interdependency among the layers.

OSI Vs TCP/IP:

OSI	TCP/IP
It consist seven layers.	It consist 5 layers but in latest TCP/IP 4 layes.
No definition for multicasting in OSI	It is clearly define in TCP/IP
No flexibility	Flexibility
Not Practical	TCP/IP practical std.

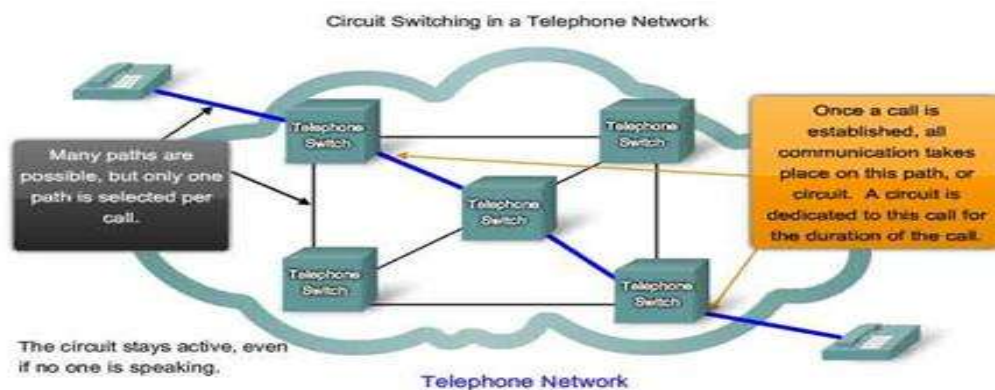
Switching Networks:

They are of two types

- **CIRCUIT SWITCHED NETWORK**
- **PACKET SWITCHED NETWORK**
- Packet-switched and circuit-switched networks use two different technologies for sending messages and data from one point to another.

Circuit Switching:

- Circuit switching was designed in 1878 in order to send telephone calls down a dedicated channel.
- This channel remains open and in use throughout the whole call and cannot be used by any other data or phone calls.



- Dedicated communication path exists between two stations
- There are three phases in circuit switching:
 - Establish
 - Transfer
 - Disconnect
- The telephone message is sent all together; it is not broken up.
- The message arrives in the same order that it was originally sent.
- In modern circuit-switched networks, electronic signals pass through several switches before a connection is established.
- During a call no other network traffic can use those switches.
- The resources remain dedicated to the circuit during the entire data transfer and the entire message follows the same path.
- Circuit switching can be analog or digital.
- With the expanded use of the Internet for voice and video, analysts predict a gradual shift away from circuit-switched networks.
- A circuit-switched network is excellent for data that needs a constant link from end-to-end, for example, real-time video.
- Must have switching capacity and channel capacity to establish connection
- Circuit switching takes place at the physical layer.
- Before starting transmission the station must make a reservation for the resources to be used during transmission.
- Data transfer between two stations is in the form of signals (not in the form of packet) as it works on physical layer.
- There are three phases of transfer setup → data transfer → teardown (connection released signal is generated in this phase).

Advantage:

- Circuit is dedicated to the call – no interference, no sharing
- Guaranteed the full bandwidth for the duration of the call
- Guaranteed quality of service

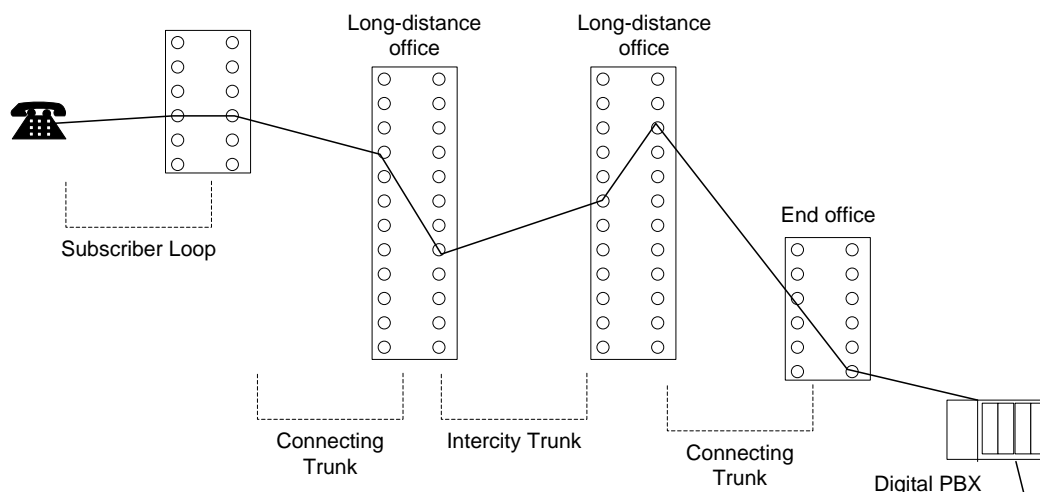
Disadvantage:

- Inefficient – the equipment may be unused for a lot of the call; if no data is being sent, the dedicated line still remains open.
- It takes a relatively long time to set up the circuit.
- During a crisis or disaster, the network may become unstable or unavailable.
- It was primarily developed for voice traffic rather than data traffic.

Circuit Switching Application:

- Inefficient
 - Channel capacity dedicated for duration of connection
 - If no data, capacity wasted
- Set up (connection) takes time
- Once connected, transfer is transparent
- Developed for voice traffic (phone)

Public Circuit Switched Network:



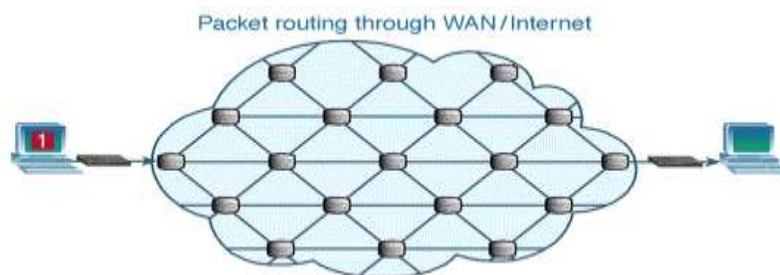
- Circuit switching designed for voice
 - Resources dedicated to a particular call
 - Much of the time a data connection is idle
 - Data rate is fixed
- Both ends must operate at the same rate

Packet Switching:

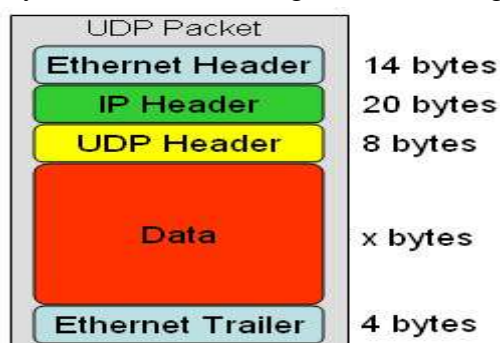
Packet Switching Principles: (no resource reservation is done, they are allocated on demand)

Basic Operation:

- In packet-based networks, the message gets broken into small data packets.
 - These packets are sent out from the computer and they travel around the network seeking out the most efficient route to travel as circuits become available.
 - This does not necessarily mean that they seek out the shortest route.
 - Each packet may go a different route from the others.
-
- Data transmitted in small packet.
 - Longer messages split into series of packets
 - Each packet contains a portion of user data plus some control information
 - Control information
 - Routing (addressing) information
 - Packets are received, stored briefly (buffered) and passed on to the next node
 - Store and forward



- Each packet is sent with a 'header address' which tells it where its final destination is, so it knows where to go.
- The header address also describes the sequence for reassembly at the destination computer so that the packets are put back into the correct order.
- One packet also contains details of how many packets should be arriving so that the recipient computer knows if one packet has failed to turn up.
- If a packet fails to arrive, the recipient computer sends a message back to the computer which originally sent the data, asking for the missing packet to be resent.



UDP = User Datagram Protocol

Advantage:

- Line efficiency
 - Single node to node link can be shared by many packets over time
 - Packets queued and transmitted as fast as possible
- Data rate conversion
 - Each station connects to the local node at its' own speed
 - Nodes buffer data if required to equalize rates
- Packets are accepted even when network is busy
 - Delivery may slow down
- Priorities can be used
 - Security
 - Bandwidth used to full potential
 - Devices of different speeds can communicate
 - Not affected by line failure (redirects signal)
 - Availability – no waiting for a direct connection to become available
 - During a crisis or disaster, when the public telephone network might stop working, e-mails and texts can still be sent via packet switching

Disadvantage:

- Under heavy use there can be a delay
- Data packets can get lost or become corrupted
- Protocols are needed for a reliable transfer
- Not so good for some types data streams (e.g. real-time video streams can lose frames due to the way packets arrive out of sequence)

Circuit Vs Packet Switching:

- It is easier and less expensive to double the capacity of a packet switched network—a circuit network is heavily dependent on the number of channels available.
- Circuit-switched technologies, which take four times as long to double their performance/cost, force ISPs to buy that many more boxes to keep up.
 - This is why everyone is looking for ways to get Internet traffic off the telephone network.
 - The alternative of building up the telephone network to satisfy the demand growth is economically out of the question.

- The battle between circuit and packet technologies has been around a long time, and it is starting to be like the old story of the tortoise and the hare.

-In this case, the hare is circuit switching—fast, reliable and smart. The hare starts out fast and keeps a steady pace, while the tortoise starts slow but manages to double his speed every 100 meters.

-If the race is longer than 2 km (1.2 miles), the power of compounding favors the tortoise (packet switching).

Classification Of Networks

Networks are classified upon the geographical area they span and can fall into the following categories:

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN)

LAN

A LAN generally consists of the following:

1. Two or more computers
2. Software to control the operation of the computers.
3. Peripheral devices such as modems, printers, plotters etc.
4. Coaxial or fibre optic cables are usually used to connect the computers and other devices.
5. A plug-in board to handle the data transmissions.

The number of computers in LAN varies from small LAN's that connect 2 to 25 computers, to large LAN's that may connect more than 10,000 computers. Normally LANs are owned by single organization. The speed of data transfer ranges from several thousand bit per second to several Mbps (Mega bits per second).

LAN Topologies:

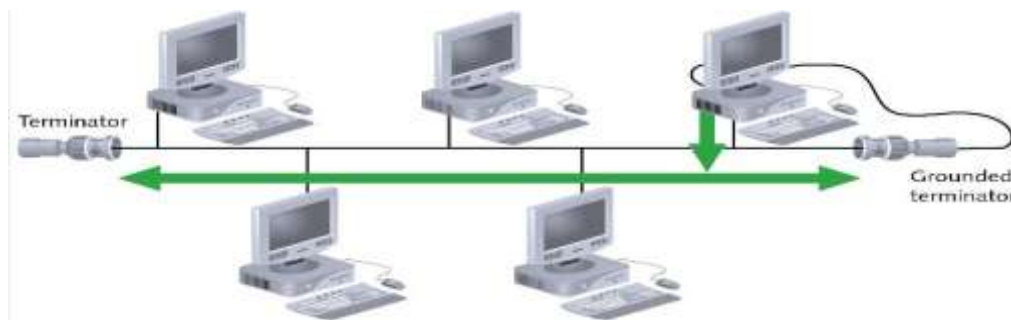
- Each computer or device in a network is called a node.
- The geometrical arrangement of computer resources, remote device, and communication facilities is known as network topology.

All network topologies derived from two basic types: The bus and the point-to-point and a network can be made in one of the two different:

1. Bus Network
2. Ring network

Bus

- This type of network was widely used in the 1980's
- In this configuration every computer (node) shares the networks total bus capacities.
- In this configuration adding more computers will reduce the access speed on the network.
- Each computer communicates to other computers on the network independently this is referred to as PEER-TO-PEER networking



How a Bus Peer to Peer Network Works

- All computers on a network have a distinct address just like your house does.
- A message would be send from one computer with the address of another computer attached to the message.
- The message is broadcasted to all the computers on the network until the addressed PC accepts the message

Advantages of Bus Topology

- Works well for small networks
- Relatively inexpensive to implement
- Easy to add to it
- Resilient Architecture

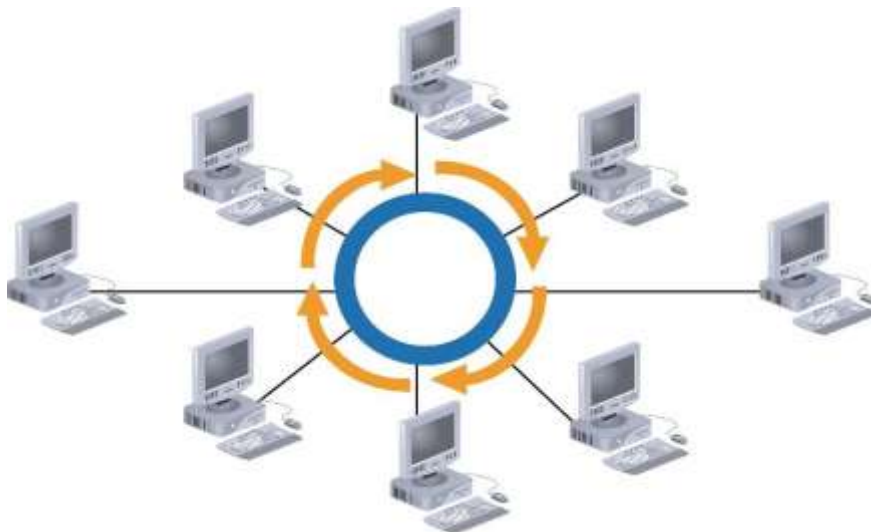
Disadvantages of Bus Topology

- Management costs can be high
- Potential for congestion with network traffic
- Fault diagnosis is difficult
- Fault isolation is difficult
- Repeater configuration
- Nodes must be intelligent

Ring Topology

- Ring topology
 - Each node is connected to the two nearest nodes so the entire network forms a circle
 - One method for passing data on ring networks is **token passing**

- Active topology
 - Each workstation transmits data



- A node has information to send to another computer on the network so it sends the information out on the network to the PC it is connected to, if the information is for this PC (the recipients NIC address is attached to the message, which is like putting an address on an envelope) then the PC accepts the data
- otherwise it passes the information on to the next PC by repeating the data back out on the line
- This method of repeating the data helps keep the integrity of the data readable by other computers .

How it Works

- As it is better to have computers take turns using the connecting Data cable, Ring topologies incorporated a system called Token passing.
- In this topology, to transmit on the wire your computer must have control of the token or wait for the token to be free.
- Larger Token Ring networks use multiple tokens.

Advantages of Ring Topology

- Easier to manage; easier to locate a defective node or cable problem.
- Well-suited for transmitting signals over long distances on a LAN.
- Handles high-volume network traffic.
- Enables reliable communication.

Disadvantages of Ring Topology

- Expensive
- Requires more cable and network equipment at the start
- Not used as widely as bus topology
 - Fewer equipment options

- Fewer options for expansion to high-speed communication
- Node failure causes network failure
- Difficult to diagnose faults

Metropolitan Area Network (MAN)

- A man is basically a bigger version of a LAN and normally uses similar technology.
- A MAN can support both data and voice and might be even related to the local cable television (CATV) network.

A special standard has been adopted for MAN is called DQDB (Distributed Queue Dual Bus). DQDB consists of two unidirectional buses (cables) to which all computer are connected as shown in figure below each bus has a head-end, a device that initiates transmission activity.

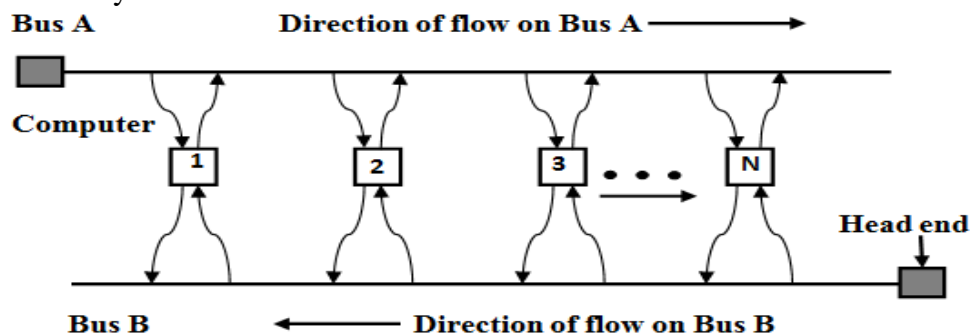


Figure MAN (DQDB architecture)

Traffic for right side uses the upper bus i.e. if computer 1 wants to send some message to computer 3, it will use the upper bus A. traffic to the left use the lower one.

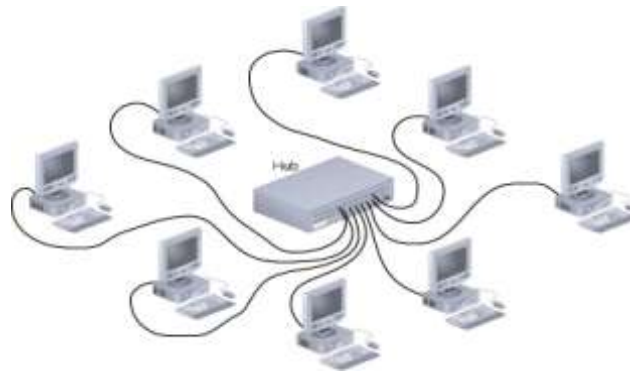
A key aspect of a MAN is that there is broadcast medium to which all the computer are attached.

A network can be made in one of the two different topologies:

1. Star Network
2. Tree Network
3. Mesh Network

Star topology

- In a Star topology every node is connected through a central device such as a Hub, Switch or Router
- In a star network, devices or computers are connected to one centralized computer.
- The disadvantage of star network is that none of the other computers can communicate with each other if the central computer breaks down.
- Compared to a Ring or Bus topology a Star topology requires that more thought be put into its setup



Advantages of Star Topology

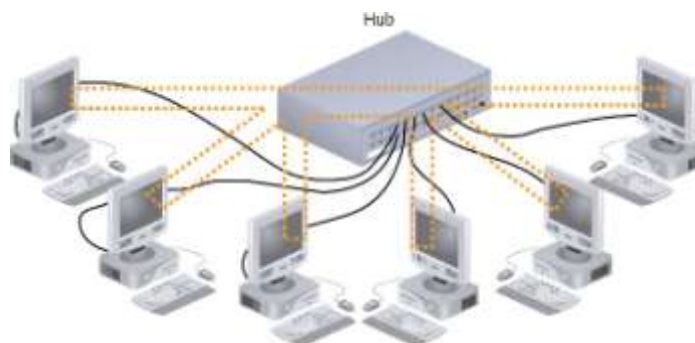
- Good option for modern networks
- Low startup costs
- Easy to manage
- Offers opportunities for expansion
- Most popular topology in use; wide variety of equipment available

Disadvantages of Star Topology

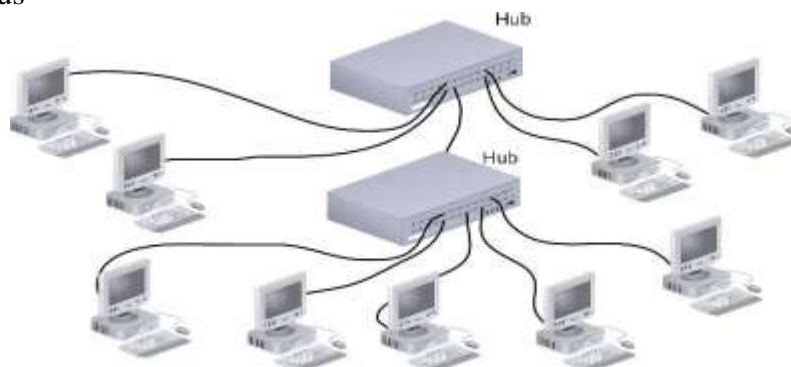
- Hub is a single point of failure
- Requires more cable than the bus

Hybrid Physical Topologies:

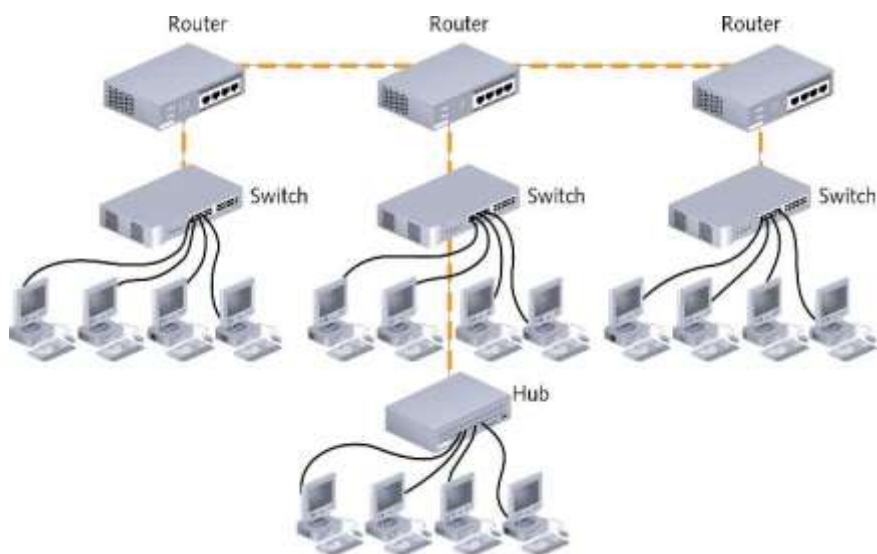
Star-Wired Ring



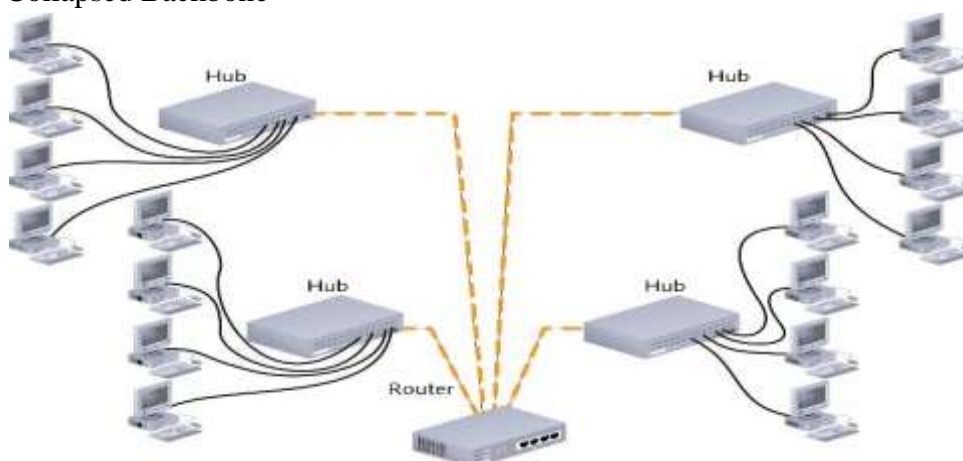
Star-Wired Bus



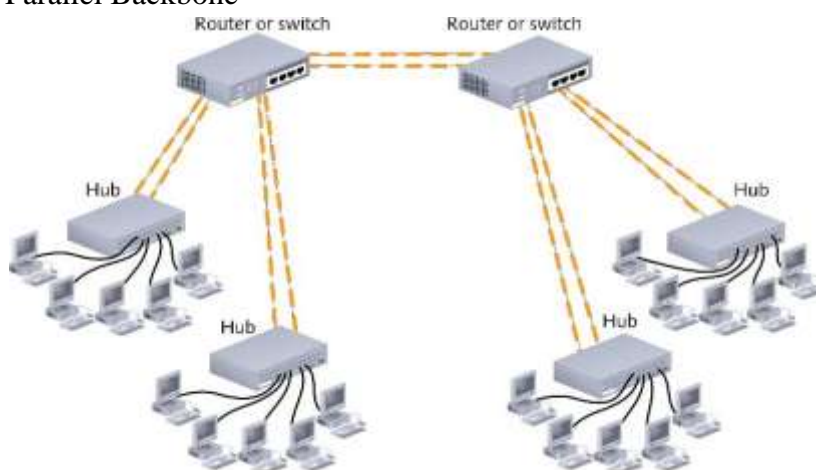
Distributed Backbone



Collapsed Backbone



Parallel Backbone



Tree Network

- In a tree network, several devices or computers are linked hierarchical fashion. Tree network is also known as hierarchical network.
- This type of distribution system is commonly used in the organization where headquarters communicate with regional offices and regional offices communicate with distinct offices and so on (below)

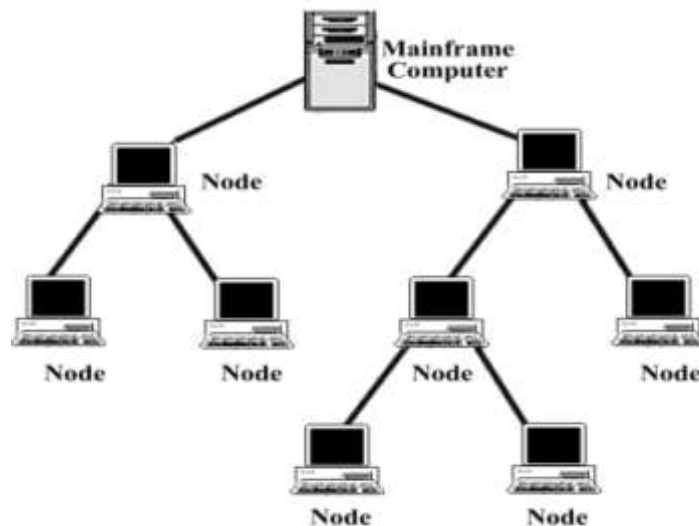


Figure Tree Network

Advantages of Tree Network:

- (a) Easy to extend
- (b) Fault isolation

Disadvantages of tree Network:

- (a) Dependent on the root

Mesh Network

A mesh network has point –point connections between every device in the network. Each device requires an interface for every other device on the network, mesh topologies are not usually considered practical.

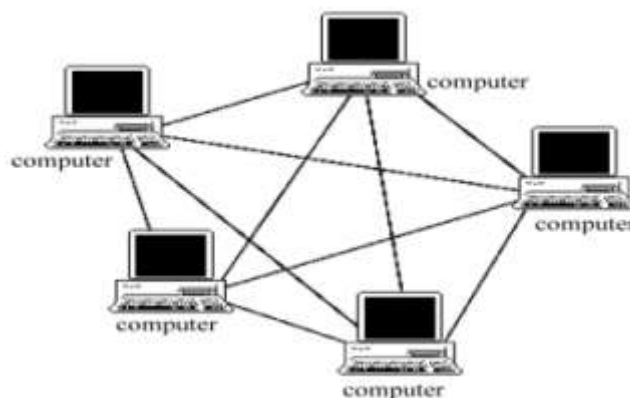


Figure Mesh Network

Advantages and Disadvantages of Mesh Network:

- (a) **Units Affected by Media Failure:** Mesh topology resist media failure better than topologies. Implementations that include more than two devices will always have multiple paths to send signals from one device to another. If one path fails, the transmission signal can be routed the failed link.
- (b) **Ease of installation:** Mesh network are relatively difficult to install because each device must be linked directly to all other devices. As the number of devices increases, the difficulty of installation increases geometrically.
- (c) **Ease of Troubleshooting:** Mesh topologies are easy to troubleshooting because each medium link is independent of all others. You can easily indentify faults and can rectify it.
- (d) **Difficulties of Reconfiguration:** Mesh topologies are difficult to reconfigure for the same reasons that they are difficult to install.

Wide Area Network(WAN)

- A WAN spans a large geographical area, often a country or continent.
- It contains a collection of machines intended for running user programs, these machines are called hosts.
- The hosts are connected by a communication subnet or just subnet.
- The job of subnet is to carry message from host to host just as the telephone system carries words from speaker to listener.
- In most wide area networks, the subnet consists of two distinct components: transmission lines and switching elements.
- Transmission lines moves bits between machines.
- The switching elements are specialized computers used to connect two or more transmission lines.
- When the data arrive on an incoming line, the switching element must choose an outgoing line to forward them on. These switching elements are popularly called routers. The collection of communication lines and routers form the subnet, Figure Show the relations between hosts and the subnet.

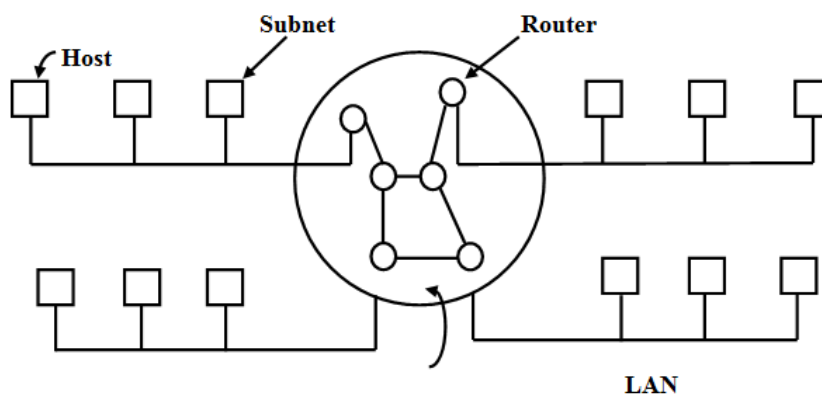
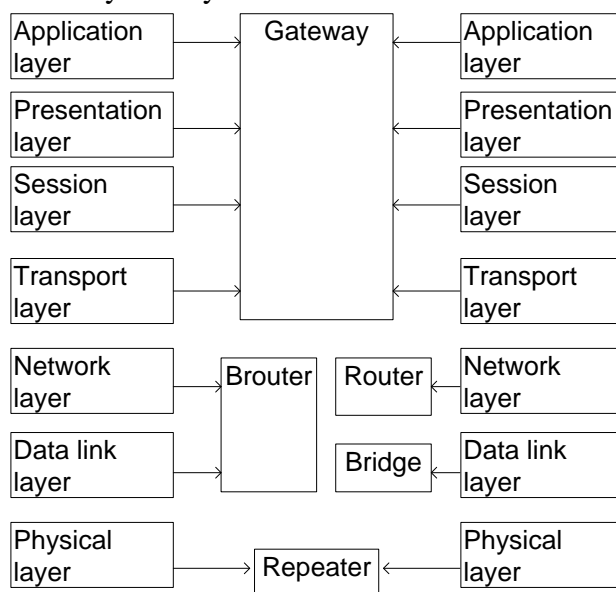


Figure Communication

INTERNETWORKING DEVICE

Object available in computer network are:

- Workstation or server—7 Layers
- Hub—Physical Layer
- Switch—DLL and physical layer
- Bridge—DLL and Physical layer
- Router—network, DLL and physical layer
- BRouter—network, DLL and Physical
- Gateway—7Layer



Repeater:

- It is used physical layer.
- Due to properties of medium and other reasons, the signal gets weak they travel long distances. Weakening of signals limits the distance any medium can carry data. Adding a device that amplifies the signal, can allow it to travel further, increasing the size of the network. Devices that amplify signals in this way are called repeaters.
- Due to properties all into two categories: amplifiers and signal- regenerating repeaters. Amplify the entire incoming signal i.e. they amplify both the signal noise.
- Signal-regenerating repeaters differentiate between data noise, and retransmitting only the desired information.
- This reduces the noise. The original signal is duplicated, boosted to its original strength, and sent.
- A simple repeater connects similar type of segments: for example an Ethernet to Ethernet (simple).
- It doesn't perform any error checking.
- A two port repeater has two bi-directional ports, and two amplifiers.
- A multi port repeater is used to connect multiple segments.

- They may connect different types of cable, but use the same data link and network Protocol
- Internetwork commonly uses special devices called repeaters, bridges, routers and gateways to connect independent networks.

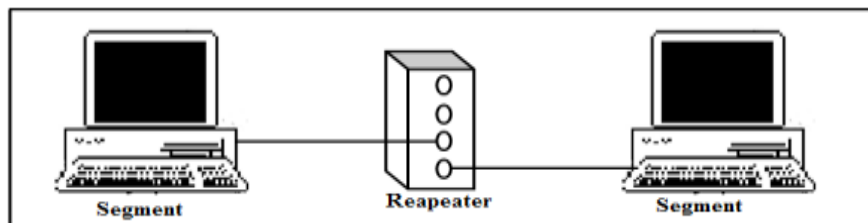


Figure shows the arrangement of repeater

Hub:

- It is DLL layer device.
- It is used to connect two similar LANs, such as two CSMA LANs.
- It is used to connect multiple workstation and servers.
- It is passive device.
- It is broadcasting device.
- Traffic is very high in hub communication and causing unnecessary distribution at various stations.
- Cost of hub is less and operation is simple.
- All networks require a central location to bring media segment (i.e. computer) together. These central locations are called hubs.
- The easiest way to understand this concept is to think of the necessity of connection multiple cables. If you just connect the media segments together by soldering them, the signals would interface with each other and create problem.
- A hub organizes the cables and relays signals to the media segments. Figure below shows a hub-arrangement.

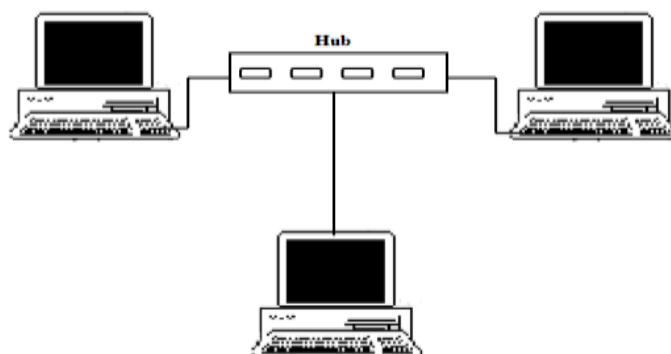


Figure Hub

There are three categories of hubs:

- **Passive hubs:** A passive hub simply combines the signals of network segment. There is no signal processing or regeneration, Because it does not boost the signal and, in

fact, absorbs some of the signals. Also, with a passive hub, each computer receives the signals sent from all other computer connected to hub.

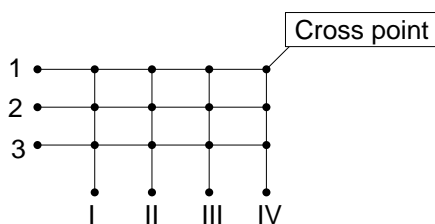
- **Active hubs:** Active hubs are like passive hubs except that they have electronic components that regenerate or amplify signals. Because of this, the distance between devices can be increased. They are also much more expensive than passive hubs.
- **Intelligent hubs:** In addition to signal regeneration, intelligent hubs perform some network management and intelligent path selection. Many switching hubs can choose alternative path will be the quickest and send the signal that way.

Switch:

- Switch is also used to connect multiple workstation & server.
- A switch is a combination of a hub and a bridge
- A switch can allow simultaneous access to multiple servers, or multiple simultaneous connections to a single server
- Active device associative with s/w.
- Traffic is less and no unnecessary traffic.
- Maintenance lookup table to see the route.
- Cost is 3 to 5 times server.

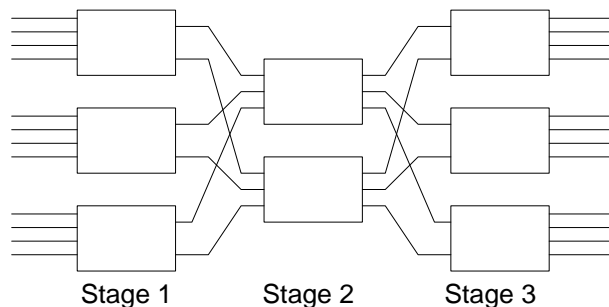
Cross-bar switch:

- A cross-bar switch connects n inputs to m output in a grid, using electronic micro switches at each cross-point.
- The major limitation of this design is the number of cross-points required.
- Connecting n inputs to m outputs using a cross-bar switch requires $n \times m$ cross-points. For example, to connect 1000 inputs to 1000 outputs requires a cross-bar with 1,000,000 cross points.
- A crossbar with this number of cross points is impractical. Such a switch is also inefficient because statistics show that, in practice, fewer than 25 percent of the cross point are in use at any given time. The rest are idle.

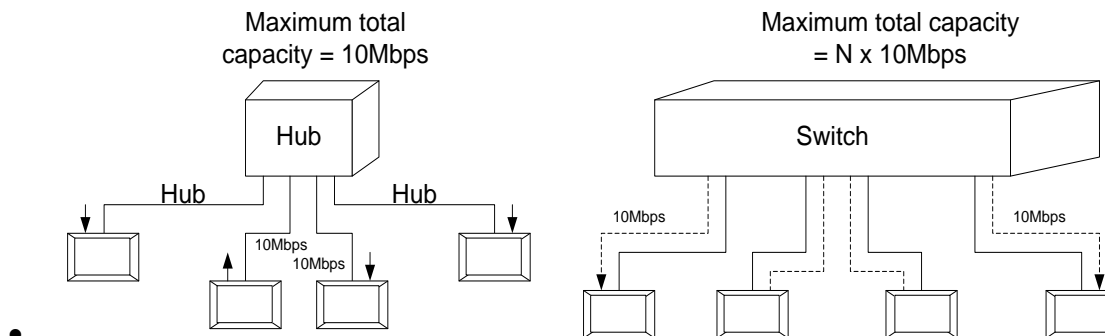


Multistage Switch:

- The solution to the limitations of the cross-bar switches is several stages. In multistage switching, devices are linked to switches that, in-turn, are linked to other switches.
- The design of a multistage switch depends on the number of stages and the number of switches required in each stage.
- Normally, the middle stages have fewer switches than do the first and last stages.

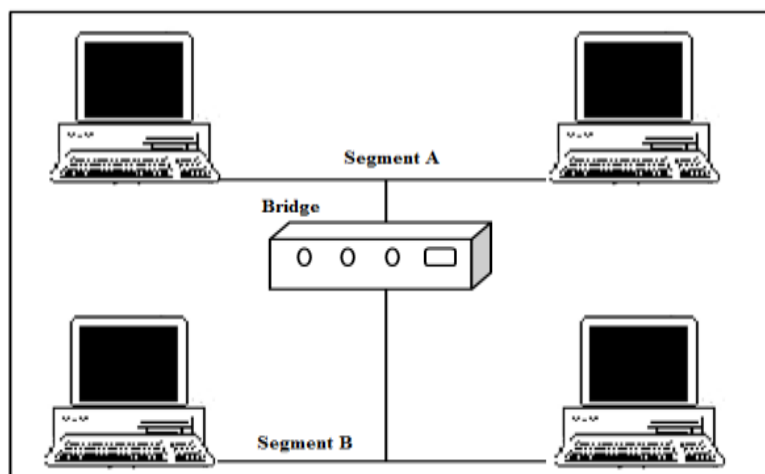


Switches vs. Hubs:



Bridge:

- It is used to connect multiple LAN and multiple subnets.
- Filtering and forwarding is design criteria.
- It is also an active device associated with software and maintenance lookup table to keep track LAN.



We cannot use bridges to connect LANs of different type and protocols. This is because each network type uses different physical addressing.

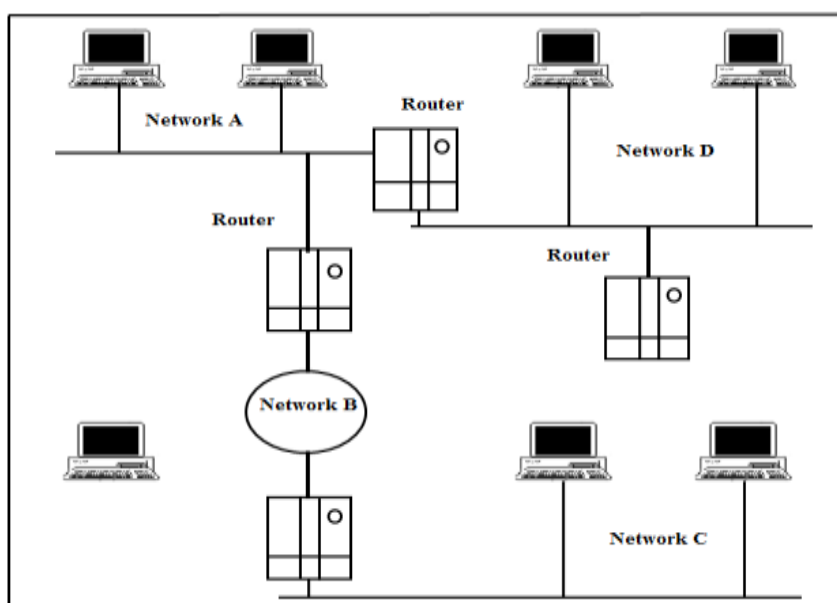
There are two basic types of bridges:

- **Transparent bridges:** The keeps a table of addresses in memory to determine where to send data.

- **Source-routing bridges:** That requires the entire route to be included in the transmission and do not route packets intelligently. IBM Token Ring networks use this type of bridge.

Router:

- It is used to connect different similar network.
- It is sophisticated device requires lot of configuration.
- Routing algorithm are running in router.
- Cost is very high.
- Routers use logical and physical addressing to connect two or more logically separate networks. They accomplish this connection by organizing the large network into logical network segments (sometime called subnet-works or subnets). Each of these subnets is given a logical address. This allows the networks to separate but still access each other and exchange data when necessary. Data is grouped into packets, or block of data. Each packet in addition having a physical device address, has a logical network address.



• **Fig. 1.25 Network connected by routers**

The network address allows routers to more accurately and efficiently calculate the optimal path to a workstation or computer. Routers perform function very similar to that of a bridges but routers keep the network separate. Because, they must check both the device address and network address, router processing is generally slower than bridge processing.

Brouter:

- Combination of bridge and router.
- They operate at both the data link & network layers
- They can connect both same and different link type network LAN segments
- It is two in one device has the capability of both bridge and router.

Gateway:

- Used to connect different dissimilar network.
- Also called as protocol converter.

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.

A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing

Syntax: The term *syntax* refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

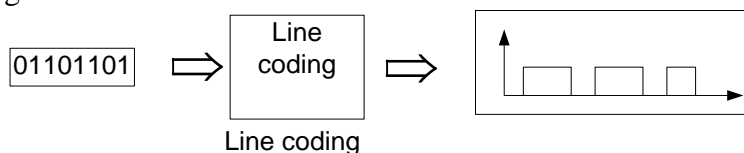
Semantics: The word *semantics* refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?

Timing: The term *timing* refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

DATA ENCODING

Line coding:

Line coding a process of converting binary data, a sequence of bits, to a digital signal. Data, text, numbers, images, all are stored as sequences of bits. Line coding converts a .sequence of bits to a digital signal.

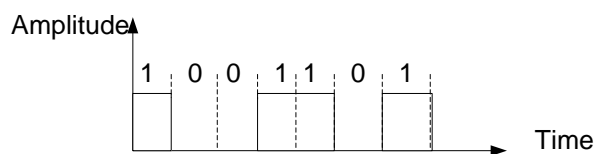


Characteristics:

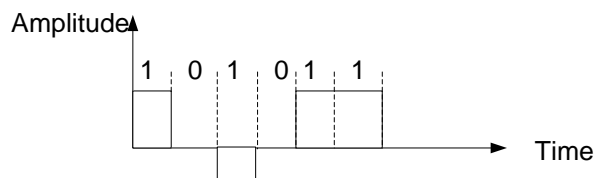
- Signal level and data level:

The number of values allowed in a particular signal is referred as signal levels.

The number of values used to represent data is referred as data levels.



2 signal level, 2 data level



3 signal level, 2 data level

- Pulse rate and bit rate:

The pulse rate defines the number of pulse per second.

A pulse is the minimum amount of time required to transmit a symbol.

The bit rate defines the number of bits per second.

$$\text{Bit rate} = \text{Pulse rate} \times \log_2 L$$

L is the number of data levels of the signal.

Example:

A signal has two data levels with pulse duration of 1 ms. calculate the pulse rate and bit rate.

$$\text{Pulse rate} = \frac{1}{1 \times 10^{-3}} = 1000 \text{ pulses/s}$$

$$\text{Bit rate} = \text{pulse rate} \times \log_2 L = 1000 \times \log_2 2 = 1000 \text{ bps}$$

- DC Components:

Some line coding schemes leave a residual direct-current component. This component is not desirable.

- Self-synchronization:

To correctly interpret the signals received from the sender, the receiver's bit intervals must correspond exactly to the sender's bit intervals.

Assignment:

1. Match the following:

List I

- A. Bridge
- B. Router
- C. Gateways

List II

- P. Operate at the 3 layer of OSI
- Q. Operate at the bottom layer of OSI
- R. Operate at the network layer of the OSI model

Codes:

- | | | |
|-------|---|---|
| A | B | C |
| (A) P | R | Q |
| (B) Q | R | P |
| (C) R | P | Q |
| (D) R | Q | P |

- 2. How much bandwidth is there in 0.1 micron of spectrum at a wave length of 1 macron?
(A) 30000 MHz (C) 30000 KHz
(B) 30000 GHz (D) 30000 Hz
- 3. The number of cross points needed for 12 lines in a cross point switch which is full duplex in nature and there no self connection is
(A) 66 (C) 132
(B) 78 (D) 144
- 4. A terminal multiplexer has four 1800 bps terminals and 'n' 200 bps terminals connected to it the outgoing line is 9600. What is the maximum value of 'n'?
(A) 4 (C) 12
(B) 8 (D) 16
- 5. Which of the following has the highest processing delay?
(A) Repeater (C) Router
(B) Bridge (D) Gateway
- 6. A sine wave completes 2 cycles in 8 seconds. What is its frequency?
(A) 0.25 Hz (C) 1.21 Hz
(B) 0.01 Hz (D) 2.20 Hz
- 7. A digital signal generated from a device has a bit rate of 1000 bps. Identify the bit interval.
(A) 0.001 second (C) 0.1 second
(B) 0.01 second (D) 0.0001 second
- 8. A transmission network is designed. Identify the delay for utilization values of 25% Assume that the network delay is 20 ms.
(A) 36.66 ms (C) 26.66 ms

- (B) 80 ms (D) 100 ms
9. How long does it take to transmit x KB over a y Mb/sec. link Ignore propagation delay. Write down the answer as a ratio of x and y
- (A) $7.23 \frac{x}{y}$ ms (C) $8.20 \frac{x}{y}$ ms
(B) $7.92 \frac{x}{y}$ ms (D) $8.19 \frac{x}{y}$ ms
10. A system has an h layer protocol hierarchy. Let the message generated at the application level be of length M Bytes. Let each layer generate a k byte header which gets added to the message as the message moves down to the layer. What fraction of the network bandwidth is filled with headers?
- (A) $\frac{hk}{m+hk}$ m (C) $\frac{k}{m}$
(B) $\frac{h}{m}$ (D) $\frac{m}{hk}$
11. The University of Athens is interested to interconnect all the departments through a mesh network. Assuming that it has to interconnects 210 computers identify the number of connections required.
- (A) 21429 (C) 21945
(B) 2046 (D) 4096
12. Segmentation is done in
- (A) Transport layer (C) Data link layer
(B) Network layer (D) Physical layer
13. Network layer activities are
- (A) Logical addressing (C) Access control
(B) Port addressing (D) All of the above
14. Hop-to-Hop delivery is related to
- (A) Data link layer (C) Transport layer
(B) Network layer (D) All of the above
15. Process to process delivery is related to
- (A) Data link layer (C) Transport layer
(B) Network layer (D) All of the above
16. Which of the following OSI layer performs error checking of data?
- (A) Network (C) Data link
(B) Transport (D) Physical
17. Routing is done in
- (A) Network layer (C) Data link layer
(B) Physical layer (D) Transport layer

18. Prot number is
(A) Process number (C) Both A and B
(B) Computer address (D) None of the above
19. A mesh network has one coordinator and six devices. Determine the number of channels.
(A) 21 (C) 36
(B) 22 (D) 31
20. Ban rate means
(A) Number of bits transmitted per unit time
(B) Number of signal units per second to represent bits
(C) Number of pulse transmitted per unit time
(D) Number of bits received per unit time
21. How many connections are possible in a point to point network with 10 devices ?
(A) 100 (C) 45
(B) 55 (D) 90
22. A company is interested in establishing a point to network with its 6 branches. Identify the number of connections.
(A) 36 (C) 21
(B) 15 (D) 18

GATE Questions CS:

1. Match the following:

P. SMTP	1. Application layer
Q. BGP	2. Transport layer
R. TCP	3. Data link layer
S. PPP	4. Network layer
	5. Physical layer

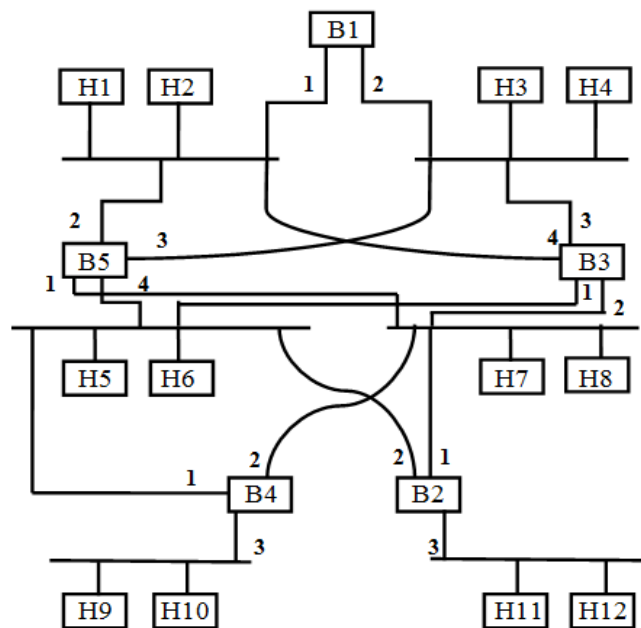
- (A) P-2, Q-1, R-3, S-5, (C) P-1, Q-4, R-2, S-5
(B) P-1, Q-4, R-2, S-3 (D) P-2, Q-4, R-1, S-5

[GATE-CS-2007]

Statement for Linked Answer Questions 2 and 3:

Consider the diagram shown below where a number of LANs are connected by (transparent) bridges. In order to avoid packets looping through circuit in the graph, the bridge organize themselves in a spanning tree. First, the root bridge is identified as the bridge with the least serial number. Next, the root bridge out (one or more) data unit units to enables the setting up of the spanning tree of shortest paths from the root bridge to each bridge. Each bridge identifies a port (the root port) through which it will forward frames to the root bridge. Port conflict are always resolve in favour of the port with the lower index value. When there is a possibility a multiple bridge forwarding to the same LAN (but not through the root port), ties

are broken as broken as follows: bridge closest to the root get preference and between such bridge, the one with lowest serial number is preferred.



2. For the given connection of LANs by bridges, which one of the following choices represents the depth first traversal of the spanning tree of bridge?
- (A) B1, B5, B3, B2 (C) B1, B5, B2, B4
(B) B1, B3, B2, B4 (D) B1, B3, B4, B2

[GATE-CS-2006]

3. Consider the correct spanning tree for the previous question. Let host H1 send out a broadcast ping packet which of the following options represents the correct forwarding table on B3?

(A)

Hosts	Port
H1, H2, H3, H4	3
H5, H6, H9, H10	1
H7, H8, H11, H12	2

(B)

Hosts	Port
H1, H2	4
H3, H4	3
H5, H6,	1
H7, H8, H9, H10	2
H11, H12	

(C)

	Hosts	Port
	H1, H2, H3, H4	3
(D)	H5, H6, H9, H10	1
	H7, H8, H11, H12	2
	H1, H2, H3, H4	3
	H5, H7, H9, H10	1
	H7, H8, H11, H12	4

[GATE-CS–

2006]

4. Suppose the round trip propagation delay for a 10 Mbps Ethernet having 48-bit jamming signal is 46.4 us.

(A) 94 (C) 464
 (B) 416 (D) 512

[GATE-CS–2005]

5. In a packet switching network, packets are routed from source to destination along single path having two intermediate nodes. If the message size is 24 bytes and packet contains a header of 3 bytes, then the optimum packet size is:

(A) 4 (C) 7
 (B) 6 (D) 9

[GATE-CS–2005]

6. In a network of LANs connected by bridge, packets are sent from one LAN to another through intermediate bridge. Since more than one path may exist between two LANs, packets may have to be routed through multiple bridges. Why is the spanning tree algorithm used for bridge-routing?

(A) For shortest path routing between LANs
 (B) For avoiding loops in the routing paths
 (C) For fault tolerant
 (D) For minimizing collisions

[GATE-CS–2005]

7. Which of the following is NOT true with respect to a transparent bridge and a router?

(A) Both bridge and router selectively forward data packets
 (B) A bridge uses IP addresses while a router uses MAC addresses
 (C) A bridge builds up its routing table by inspecting incoming packets
 (D) A router can connect between a LAN and WAN

[GATE-CS–2004]

8. Choose the best matching between Group 1 and Group 2.

Group -1

Group – 2

P. Data link layer

1. Ensures reliable transport of data over a physical point-to-point link

Q. Network layer

2. Encodes/ decodes data for

physical transmission

R. Transport layer

3. Allow end-to-end communication between two processes

4. Routes data from one network node to the next

(A) P-1, Q-4, R-3

(C) P-2, Q-3, R-1

(B) P-2, Q-4, R-1

(D) P-1, Q-3, R-2

[GATE-CS-2004]

GATE Question IT:

1. A group of 15 routers are interconnected in a centralized complete binary tree with a router at each tree node. Router i communicate with router j by sending a message to the tree. The root then sends the message back down to router j. the mean number of hops per message, assuming all possible router pairs are equally likely is

(A) 3

(C) 4.53

(B) 4.26

(D) 5.26

[GATE-IT-2007]

2. Let us consider a statistical time division multiplexing of packets. The number of sources is 10. In a time unit, a source transmits a packet of 1000 bits. The number of sources sending data for the first 20 time units is 6, 9, 3, 7, 2, 2, 2, 3, 4, 6, 1, 10, 7, 5, 8, 3, 6, 2, 9, 5 respectively. The output capacity of multiplexer is 5000 bits per time unit. Then the average number of backlogged of packets per time unit during the given period is

(A) 5

(C) 3.45

(B) 4.45

(D) 0

[GATE-IT-2007]

3. Which of the following statements is FALSE regarding a bridge

(A) Bridge is a layer 2 device

(B) Bridge reduces collision domain

(C) Bridge is used to connect two or more LAN segments

(D) Bridge reduces broadcast domain

[GATE-IT-2005]

4. Which of the following statement is FALSE?

(A) Packets switching leads or better utilizations of bandwidth resources than circuit switching.

(B) Packet switching results in less variations in delay than circuit switching

(C) Packet switching requires more per-packet processing than circuit switching

(D) Packet switching can lead to reordering unlike in circuit switching

[GATE-IT-2004]

Answer Keys

Assignment:

1 B 2 B 3 A 4 C 5 D 6 A 7 A 8 C 9 D 10 A
 11 C 12 A 13 A 14 B 15 C 16 C 17 A 18 A 19 A 20 B
 21 C 22 B

GATE Questions CS:

1 B 2 A 3 A 4 C 5 D 6 B 7 B 8 A

GATE Questions IT:

1 D 2 C 3 D 4 B

Explanations:
Assignment:
1. [Ans. B]

Bridge → operate at the bottom two layer of OSI

Router → operate at the network layer of the OSI model

Gate way → operate at the top 3 layer OSI

2. [Ans. B]

Bandwidth = 30000 GHz

3. [Ans. A]

$$\begin{aligned} \text{Number of cross point} &= \frac{n(n-1)}{2} \\ &= \frac{12 \times 11}{2} = 66 \end{aligned}$$

4. [Ans. C]

Maximum value of n is = 12

5. [Ans. D]

Gateway has the highest processing delay.

6. [Ans. A]

Let t be the period and f be the frequency. Period is the amount of time it takes to complete one cycle. Frequency is the number of cycles per second. So in the above case the period.

$$\text{Period} = 2/8 = 4; f = 1/T = 1/4 = 0.25 \text{ Hz}$$

7. [Ans. A]

We know that bit interval is defined as bit interval is defined as

$$\text{bit interval} = \frac{1}{\text{bit rate}}$$

$$\text{Substituting the available values we get bit interval} = \frac{1}{1000} = 0.001 \text{ second}$$

8. [Ans. C]

We know that the effective delay of a network can determined using the formula

$$D = \frac{1}{(1-u)}$$

Given 1 = 20 ms

When Utilization is 25%

$$D = \frac{20}{(1-25)} = \frac{20}{(.75)} = 26.66 \text{ ms}$$

9. [Ans. D]

$$\begin{aligned}x \text{ KB} &= 8 * 1024 * x \text{ bits} \\y &= y * 10^6 \text{ bps} \\ \frac{x}{y} &= \frac{8 * 1024 * x \text{ bits}}{y * 10^6 \text{ bps}} = 8.19 \frac{x}{y} \text{ ms}\end{aligned}$$

10. [Ans. A]

With n layers and k bytes added to each layer, the total number of header bytes per message is equal to hk.

Relative space wasted on headers will then be $\frac{hk}{m}$

11. [Ans. C]

$$\frac{210 * 209}{2} = 21945 \text{ connections}$$

12. [Ans. A]

Transport layer is responsible for segmentation

13. [Ans. A]

Network layer performs logical addressing

14. [Ans. B]

Network layer provides hop-to-hop delivery

15. [Ans. C]

Process to delivery is related to transport layer.

16. [Ans. C]

Data link layer perform error checking

17. [Ans. A]

Network layer perform routing.

18. [Ans. A]

Port numbers identify process.

19. [Ans. A]

Total No. of device in the network is = (1 + 6) = 7 number of channels of a network with n nodes is = $\frac{7(7-1)}{2} = 21$

20. [Ans. B]

Band rate means number of signal units per second to represent bits.

21. [Ans. C]

We know that the number of direct connections = $\frac{(n^2-n)}{2}$ Substituting the value 10 in the above equation, we get 45 connections.

22. [Ans. B]

We know that the number of direct connection = $\frac{(n^2-n)}{2}$ Substituting the value 6 in the above equation, we get 15 connections.

GATE Question CS:

1. [Ans. B]

SMTP -----Application layer
 BGP -----Network layer
 TCP -----Transport layer
 PPP -----Data link layer

2. [Ans. A]

For the given connection if LANs by bridge the depth first traversed is B1, B5, B3, B4, and B2.

3. [Ans. A]

Correct forwarding table on B3

Hosts	Port
H1, H2, H3, H4,	3
H5, H6, H9, H10,	1
H7, H8, H11, H12,	2

4. [Ans. C]

Propagation delay = 46.4×10^{-6}

Then the minimum frame size is $10 \times 10^6 \times 46.4 \times 10^{-6} = 464$ bits

5. [Ans. D]

We consider optimum packet size which required minimum number of packet and does not waste any space.

Header size = 3 byte

\therefore Packet size = $9 - 3 = 6$ is data size

$24/6 = 4$ are the required packet

For case L \rightarrow 24 packet and are required

6. [Ans. B]

For avoiding loops in the routing paths

7. [Ans. B]

Bridge ----- IP Address

Router ----- MAC address

8. [Ans. A]

Data link layer – Ensure reliable transport of data over a physical point to point link

Network layer – Router data from one network node to the next

Transport layer – Allow end – to – end communication

GATE Questions IT:

1. [Ans. D]

Mean Number of hop = 5.26

2. [Ans. C]

Total No. of source = 10

Packet size = 1000 bits

Output capacity of multiplexer = 5000 bits

\therefore Average number of back logged of packet = 3.45

3. [Ans. D]

When ever station sends broadcast, then it is received by all station of LAN at does not matter on which segment they are

4. [Ans. B]

Packet switching results in less variation in delay than circuit switching

The Data Link Layer

(Flow and error control techniques)

Data Link Layer Design Issues

The data link layer has number of specific function to carry out. These function include providing a well defined service, interface to a network layer, determining how the bits of the physical layer are grouped into frames, dealing with transmission errors, regulating the flow of frame so that flow of frame so that slow receivers are not swamped by fast sender, and general link management.

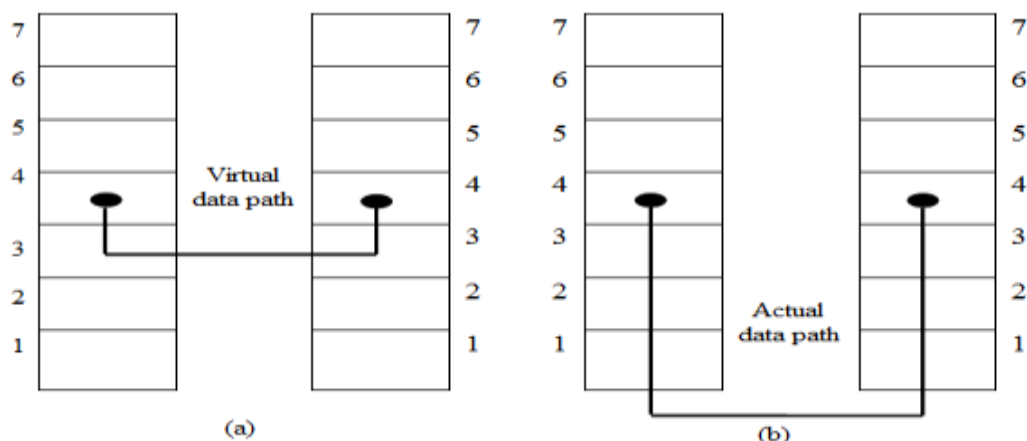
Service Provided to the Network Layer

The function of the data link layer is to provide services to Network layer.

The principal service is transferring data from network layer on source machine to network layer on the destination machine.

The job of data link layer is to transmit the bits to the destination machine, so they can be handed over to the network layer there as shown in figure (a)

The actual transmission follows the path of figure (b), but it is easier to think in terms of two data link layer process communicating using a data link protocol.



Figure

The data link layer can be designed to offer various services.

1. Unacknowledged connectionless services.
2. Acknowledged connection less services.
3. Connection oriented service.

Unacknowledged connectionless service consists of having the sources machine send the independent frames to the destination machine without having the destination machine acknowledge them.

No connection is established beforehand or released afterwards. If the frame is lost due to noise on the line, no attempt is made to recover in the data link layer. This class of service is appropriate when the errors rate is very low and recovery is let to the higher layers.

The most sophisticated service the data link layer provide to the network layer is connection oriented service. With this service, the source and destination machine establish connection before the data are transferred. Each frame sent over the connection is numbered, and the data link layer guarantees that each frame sent is indeed received.

When connection oriented services is used, transfer have three distinct phases.

In the first phase the connection is established by having both sides initialized variables and counter needed to keep track of which frame have been received and which one have not.

In the second phase one or more frames are actually transmitted.

In the third and final phase, the connectio0n is released, freeing up the variable, buffers and other resources and other resources used to maintain the connection.

Framing

In order to provide services to the network layer, the data link layer must use the service provided to it by physical layer.

What the physical layer does it accept the raw bit stream and attempt to deliver it to the destination.

This bit stream is not guaranteed to be error free. The number of bits received must be less than, equal to, or more than the number of bits transmitted, and they have different values.

It is up to data link layer to detect, and if necessary correct the errors.

The usual approach is for data link layer to break the bit stream up into discrete frames and compute the checksum for each frame.

When a frame arrives at destination the checksum is recomputed. If a newly computed checksum is different from the one contained in the frame, the data link layer knows that an error has occurred and takes step to deal with it.

Breaking the bit stream up into frames is more difficult than it at first appears.

Here, we will look at three commonly used methods:

1. Character count
2. Starting and ending character with character stuffing.
3. Starting and ending with bit stuffing.

Character Count

The **first framing** method uses the field the header to specify the number of character in the frame, when the data link layer at the destination sees the character count, it knows how many character follow, and hence the end of the frame is, this technique is shown in below figure (a) for four frames of sizes 5, 5, 8 and 9 characters respectively.

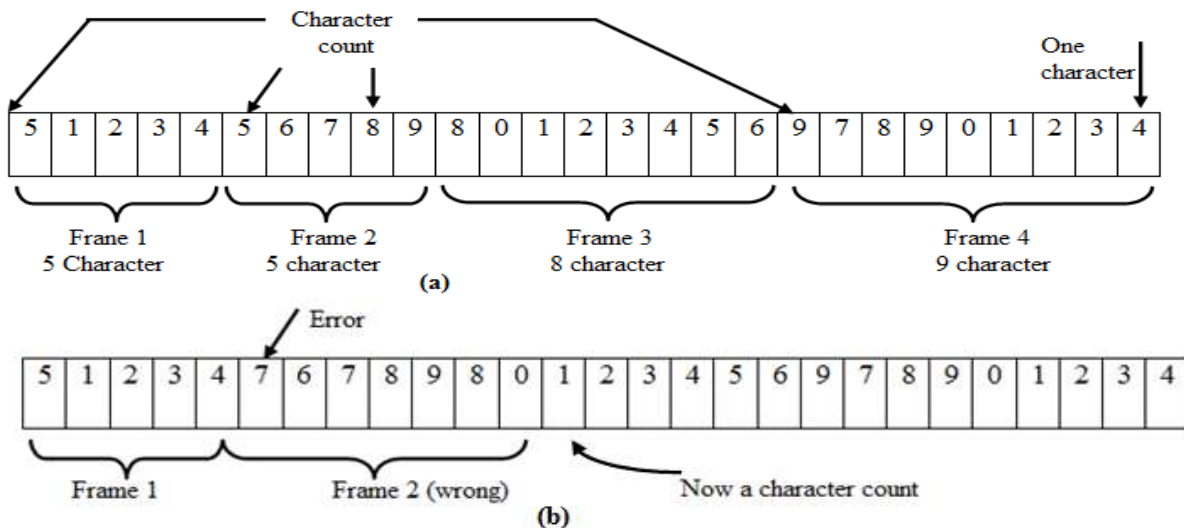


Fig ure A character stream (a) without error (b) with error

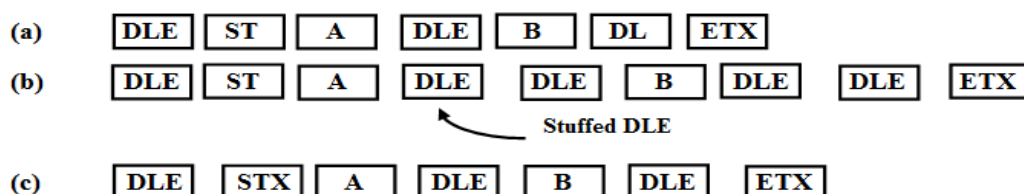
The trouble with this algorithm is that the count can be garbled by a transmission error.

Starting and ending character with character stuffing

The **second framing** method gets around the problem of re-synchronization after an error has occurred, by having each frame start with the ASCII character sequence DLESTX and end with sequence DLEETX (DLE is data link escape, STX is start of Text, ETX is End of Text). In this way, if the destination ever loses the track of frame boundary all it has to do is look for DLESTX or DLEETX character to figure out where it is.

A serious problem occurs with this method when binary data, such as object programs or floating point numbers, are being transmitted, it may easily happen that the character for DLESTX or DLRETX occur in the data, which will interface with the framing, one way to solve this problem is to have sender data link layer insert on ASCII DLE character just before each "accidental" DLE character in the data, the data link layer in the receiving end removes the DLE before the data are given to the network layer.

This technique is called '**character stuffing**'. Thus framing DLESTX or DLEETX can be distinguished from one in the data by absence or presence of single DLE. DLEs in the data are always doubled below figure gives an example data stream before stuffing, and after destuffing.



- (a) Data sent by network layer
- (b) Data after being character stuffed by data link layer
- (c) Data passed to the network layer to the receiving side

Starting and ending with bit stuffing

The third technique allows the frames to contain any arbitrary bits and allows the character codes with an arbitrary numbers of bits per character.

It works like this, each frame begins and ends with specific bit pattern, 01111110, called the flag byte.

Whenever the sender's data link layers encounter five consecutive ones in the data, it automatically stuffs the 0 bit into the outgoing bit stream.

This bit stuffing is analogous to character stuffing, in which the DLE is stuffed into the outgoing character stream before DLE in the data.

Whenever the receiver sees five consecutive 1 bits, followed by zero bit, it automatically destuffs (i.e. deletes) the 0 bit, if the user data contains the flag pattern, 01111110, this flag is transmitted as 011111010 but stored in the receiver memory as 01111110 below figure gives an example of bit stuffing.

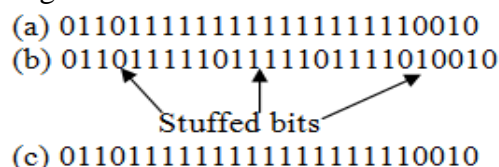


Figure: bit stuffing (a) The original data (b) The data as they appears on line. (c) The data as they are stored in receivers memory after de-stuffing.

Flow Control

Another important design issue that occurs in data link layer (and higher layers as well) is that what to do with the sender data that systematically want to transmits frames faster than the receiver can accept them.

This situation can easily occur when the sender is running on faster computer and receiver is running on slow machine. The sender keeps pumping the frames out at the higher rate until the receiver is completely swapped and at a certain point the receiver will start losing frames.

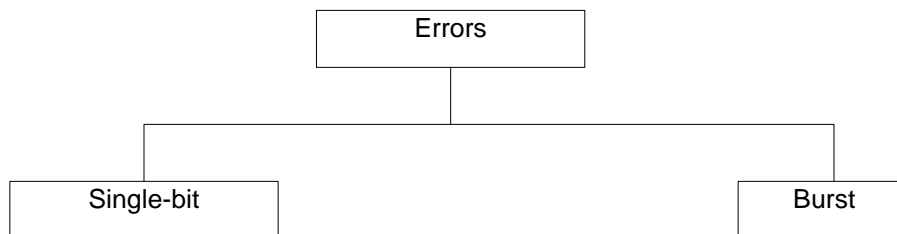
The usual solution is to introduce flow control throttle (force) the sender into sending no faster than the receiver can handle the traffic. This throttling generally requires a feedback mechanism, so the sender can come to know whether the receiver is full or not.

Error detection and correction

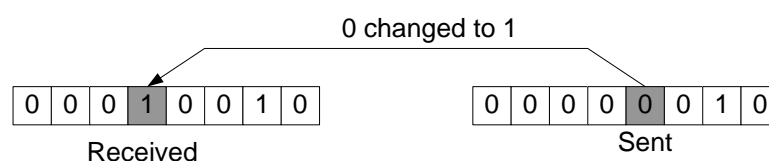
Data can be corrupted during transmission. For reliable communication, error must be detected and corrected

Error Detection and Correction are implemented either at the data link layer or the transport layer of the OSI model

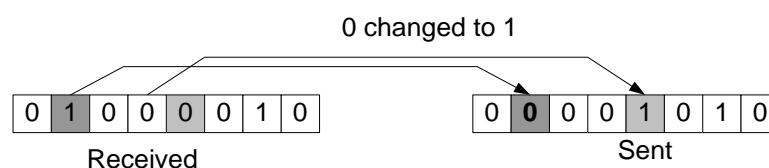
Type of Errors:



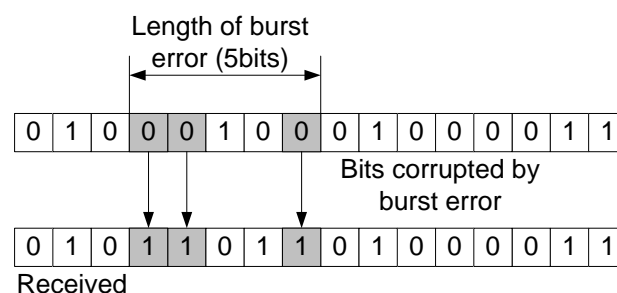
Single-Bit error: When only one bit in the data unit has changed



Multiple-Bit error: When two or more nonconsecutive bits in the the data unit have changed



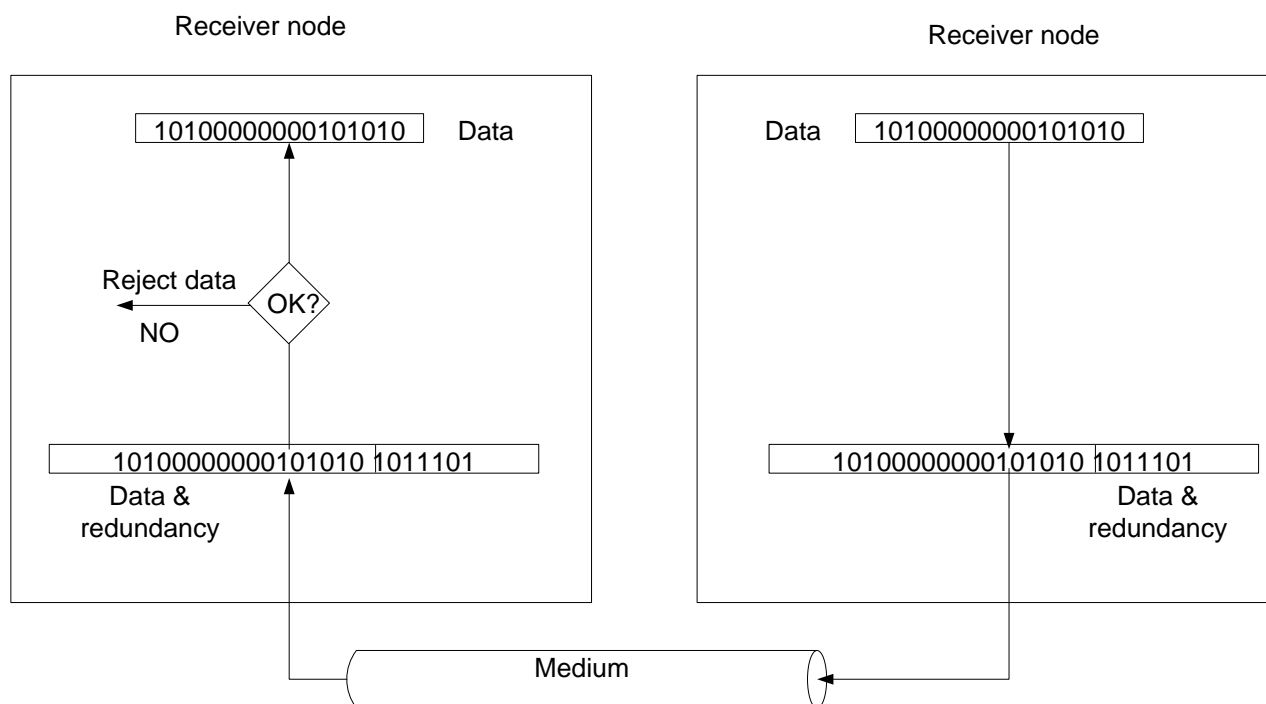
Burst error: Means that 2 or more consecutive bits in the data unit have changed



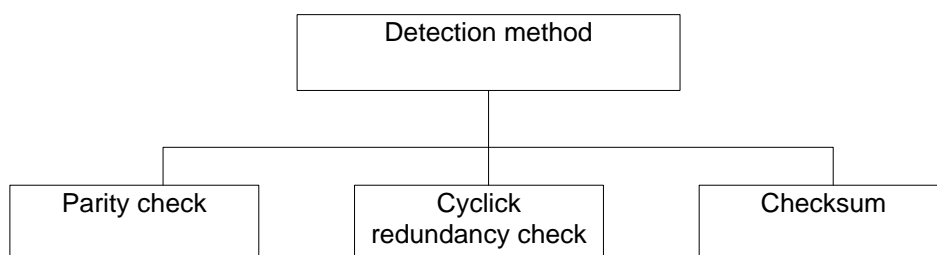
Error detection:

Error detection uses the concept of redundancy, which means **adding extra bits** for detecting errors at the destination

Redundancy:



Detection methods:



PARITY CHECK

A parity bit is added to every data unit so that the total number of 1s (including the parity bit) becomes even for even-parity check or odd for odd-parity check

Most of errors result in change of a bit from 0 to 1. One of the simplest error detection code which is used in common called as parity bit.

Parity bit is used to check data for the communication purpose. This can be done by counting number of 1's in message string. There are two types of **parity bit**:

- 1) **Even parity bit:** If in a string number of 1's are even than it is called even parity bit e.g. 101000 has even parity bit (since, there are two 1's)
- 2) **Odd parity bit:** If in a message string number of 1's are odd than it is called odd parity bit e.g. 101100 has odd parity bit (since, there are three number 1's)

How parity bit detects error?

Let us understand the principle of working of parity bit with suitable example. Basically, If we pass the received bits and send bits through exclusive OR gate, we will get the resultant all zeros if received and sent bit are same. Otherwise we will get 1 bit at the position where the bit have changed in transition.

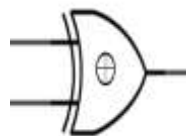
say for e.g.

Sent bits 11001010
 Received bits 1000



Due to transition the bit have changed from 1 to 0

After passing these bits through X-OR gate we get



01000000 i.e. 11001010

10001011

01000000

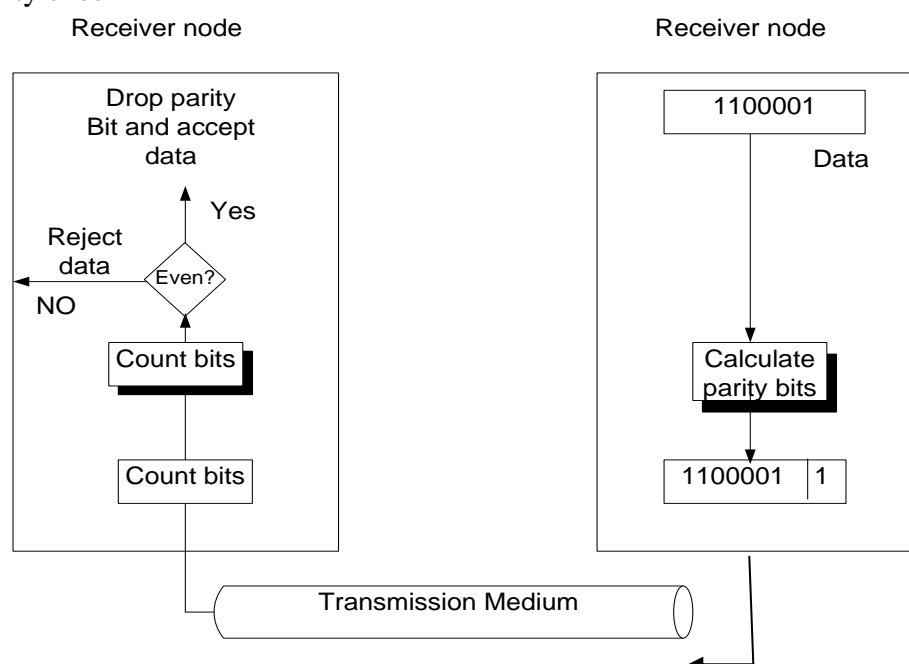
↑ Here bit have changed

Also, if the send and the received bit are same, than the resultant would be zero's.

i.e. 1 1 0 0 1 0 1 0 (sent)
 1 1 0 0 1 0 1 0 (received)
 0 0 0 0 0 0 0 0

All zero's indicates that there is no error in the transaction

- Simple parity check



Examples:

Suppose the sender wants to send the word "world". In ASCII the five characters are coded as
1110111 1101111 1110010 1101100 1100100

The following shows the actual bits sent,

11101110 11011110 11100100 11011000 11001001

Now suppose the word "world" in corrupted in transmission.

11101110 11011110

Example 1 is received by the receiver without being

11100100 11011000 11001001

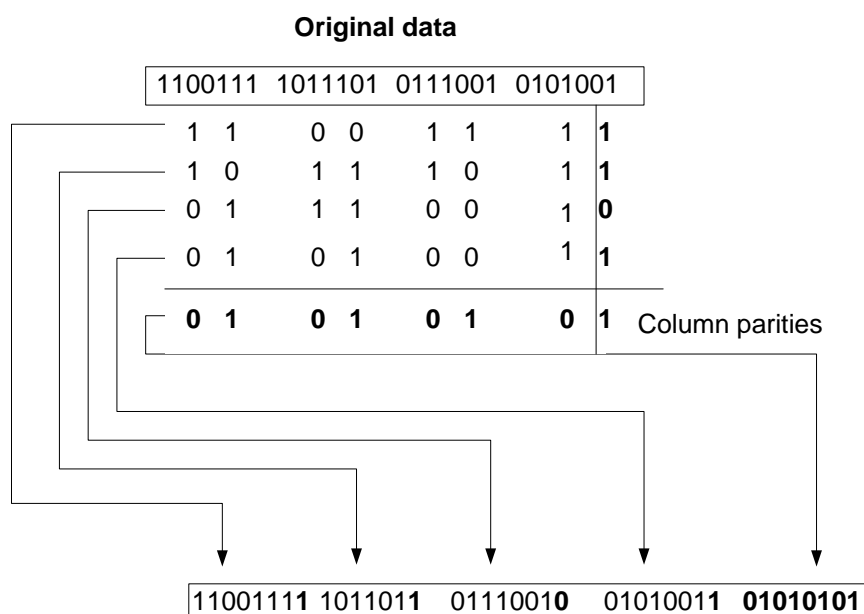
The receiver counts the 1s in each character and comes up with even numbers (6, 6, 4, 4, 4). The data are accepted.

Now suppose the word "world" in Example. 1 is corrupted during transmission.

11111110 11011110 11101100 11011000 11001001

The receiver counts the 15 in each character and comes up with even and odd numbers (7, 6, 5, 4, 4). The receiver knows that the data are corrupted, discards them, and asks for retransmission.

Two -Dimensional Parity Check:



Example:

Suppose the following block is sent:

10101001 00111001 11011101 11100111 10101010

However, it is hit by a burst noise of length 8, and some bits are corrupted.

10100011 10001001 11011101 11100111 10101010

HAMMING CODE

In parity bit, we can only detect error in data or message, we cannot rectify the data or message. But in case of hamming code we can check and rectify the error.

In this code we use number of parity bits for generating code. Suppose our data is of length n then we use k parity bits for generating hamming code of $n + k$ bits length.

We generate code according to the following steps:

1. we number $(n+k)$ data from 1.
2. the positions of the parity bit are power of 2. It means $2^0 = 1, 2^1 = 2, \dots$
3. Each parity bit assigned a number of bits to check their parity. This allotment of bit must go through all parity bits, who's sum is m . Supposes m^{th} bit is passing through

P_1, P_2, \dots, P_r bit then sum if $P_1 + P_2 + P_3 + \dots + P_r = m$

Now, let us understand the working of hamming code with the help of a suitable example,

Suppose we are sending the following bits:

1101 1011 1110 0011 (16 bits)

Step 1 Find the value of k (i.e. the parity bits)

Here, $n = 16, (16 = 2^x)$

$$2^x = 2^4$$

$$x = 4$$

Now, $k = x + 1$

$$= 4 + 1 = 5$$

Therefore $k = 5$ (parity bits)

Step 2 Hamming code = Actual code + parity bits

$$= n + k$$

$$= 16 + 5$$

$$= 21 \text{ bits}$$

Hence, we will make the hamming code of length 21 bits

Step 3 Before making the hamming code we have to decide about the parity whether it is even or odd. If even parity, the number of 1's including parity bit will be even and if odd parity then the number of 1's will be odd including the parity bit.

In this case we assume even parity.

Step 4 Place these parities on the power of 2's i.e. $2^0 = 1^{\text{st}}$ position, $2^1 = 2^{\text{nd}}$ position will be a parity bit position and so on till $2^4 = 16^{\text{th}}$ position. On rest of the positions place the original bits (i.e. number)

<input type="text"/>	<input type="text"/>	1	<input type="text"/>	1	0	1	<input type="text"/>	1	0	1	1	1	1	1	<input type="text"/>	0	0	0	1	1
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

→ Parity bit position (the powers of 2)

Structure of hamming code is ready, now we have to find out the values of parity bits.

Step 5 Parity bits will check the following positions:

1 → 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21

2 → 2, 3, 6, 7, 10, 11, 14, 15, 18, 19

4 → 4, 5, 6, 7, 12, 13, 14, 15, 20, 21

8 → 8, 9, 10, 11, 12, 13, 14, 15

16 → 16, 17, 18, 19, 20, 21

Here, for example, parity bit 1 will check the bits from 1 onwards leaving one bit in between i.e. 1, 3, 5, 7, 9 etc. Also, parity bit 2 will check the bits from 2 onwards. The two –two bits, leaving 2 bit in between i.e., 2, 3, 6, 7, 10, 11,etc. leaving 4, 5 and 8, 9 in between and so on.

As we have assumed the even parity, so if the number of 1's on these positions comes to be even, then we will put 0 in the parity box, otherwise if the number of 1's are not coming out to be even, then we will put 1 in the parity box and make it even.

So, with parity bits, we will get the following hamming code.

<input type="text"/>	<input type="text"/>	1	<input type="text"/>	1	0	1	<input type="text"/>	1	0	1	1	1	1	1	<input type="text"/>	0	0	0	1	1
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

Hence, the complete hamming code.

Step 6 Now let us introduce some error in hamming code say at position or bit

Replace the 0 bit to 1 bit. So the hamming code will look like this:

<input type="text"/>	<input type="text"/>	1	<input type="text"/>	1	0	1	<input type="text"/>	1	0	1	1	1	1	1	<input type="text"/>	0	0	0	1	1
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

Now, again we will check the positions of bits according to their parity bits i.e. the parity bit 1 will check whether 0 is correct or not, the number of 1's on position 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21 are even, hence the parity bit 1 is correct and so on.

Therefore,

Parity bit 1 → √
Parity bit 2 → √
Parity bit 4 → ×
Parity bit 8 → √
Parity bit 16 → √

Except bit 4, all the parity bits are correct. Therefore the error is found on bit 4 (i.e. detection) and now we will change this 1 to 0 (i.e. rectification), which is then the correct code.

Another error: Assume the error is in position bit 11. Hence, the hamming code will be

<u>0</u>	<u>1</u>	1	<u>1</u>	1	0	1	<u>0</u>	1	0	0	1	1	1	1	<u>0</u>	0	0	0	1	1
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

Check all the bits again (for even parity).

Hence,

Parity bit 1 → ×
Parity bit 2 → √
Parity bit 4 → ×
Parity bit 8 → ×
Parity bit 16 → √

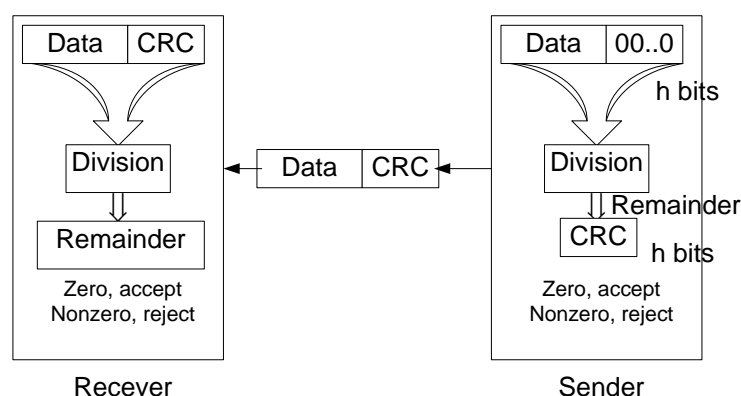
Hence, parity bit 1, 2, and 8 found to be wrong, add them, we get

$$1 + 2 + 8 = 11$$

Position 11 is having error.

CYCLIC REDANDCY CHECK(CRC)

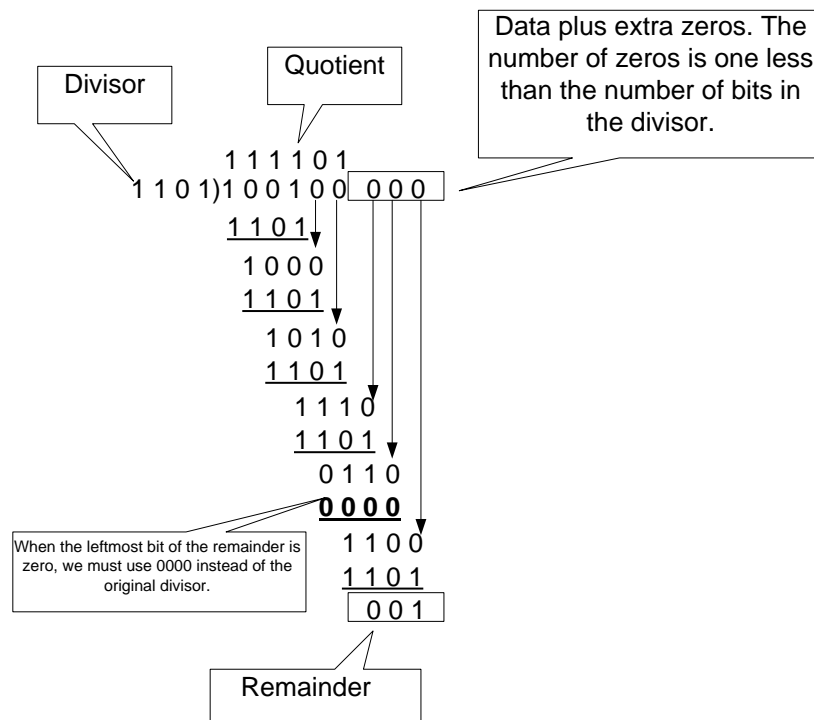
It is based on binary division.



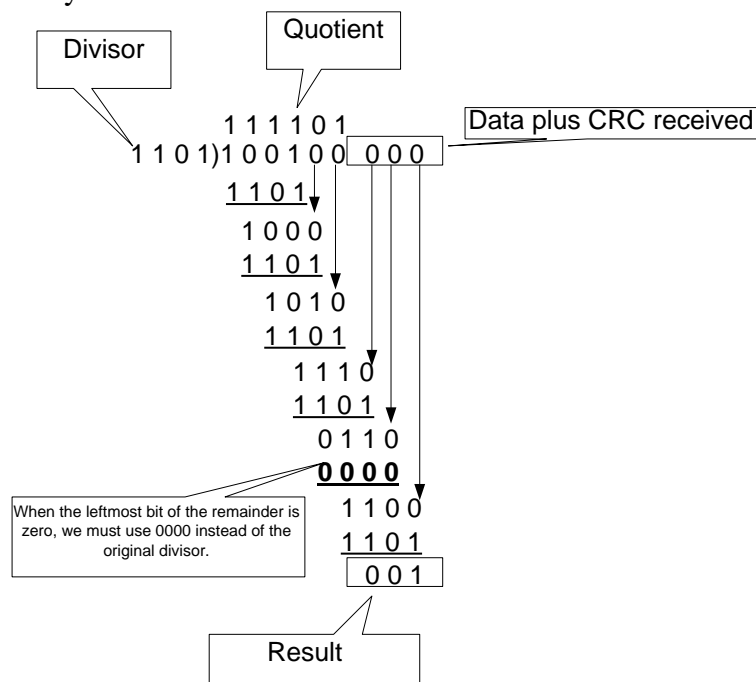
CRC generator: uses modular-2 division.

Binary Division

In a CRC Generator



CRC checker: Binary Division in a CRC Checker



Polynomials

The CRC generator (the divisor) is most often represented not as a string of 1s and 0s, but as an algebraic polynomial as shown in below. The polynomial format is useful for two reasons: it is short, and it can be used to prove the concept mathematically

$$x^7 + x^5 + x^2 + x + 1$$

Figure: A Polynomial

The relationship of a polynomial to its corresponding binary representation is shown in figure

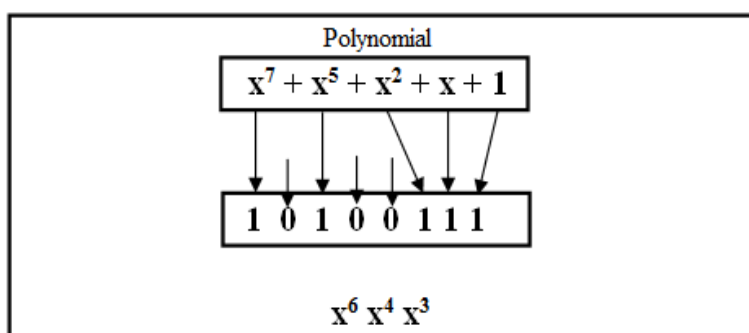


Figure: Polynomial representing a divisor

A polynomial should be selected to have at least the following properties:

- It should not be divisible by x .
- It should be divisible by $(x + 1)$.

The first condition guarantees that all burst errors of length equal to the degree of the polynomial are detected. The second condition guarantees that all burst errors affecting an odd number of bits are detected.

Example:

It is obvious that we cannot choose x (binary 10) or $x^2 + x$ (binary 110) as the polynomial because both are divisible by x . However, we can choose $x + 1$ (binary 11) because it is not divisible by x . But it is divisible by $x + 1$. We can also choose $x^2 + 1$ (binary 101) because it is divisible by $x + 1$ (binary division).

The standard polynomials used by popular protocols for CRC generation are shown in below figure.

The numbers 12, 16 and 32 refer to the size of the CRC remainder. The CRC divisors are 13, 17 and 33 bits respectively.

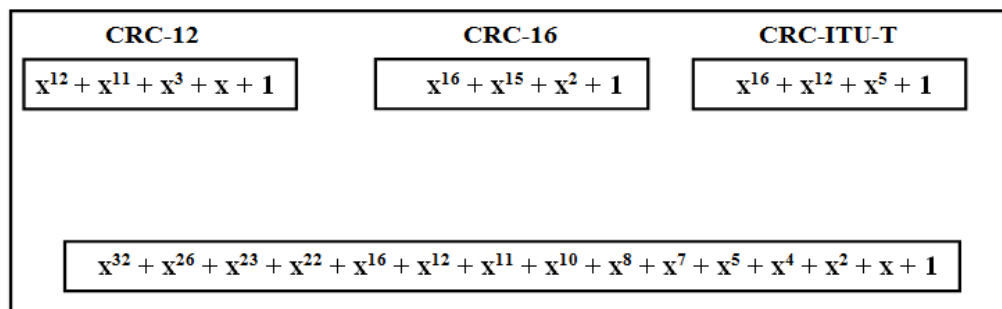


Figure: Standard polynomials

Performance

CRC is a very effective error detection method. If the divisor is chosen according to the previously mentioned rules.

- CRC can detect all burst errors that affect an odd number of bits.
- CRC can detect all burst errors of length less than or equal to the degree of the polynomial.
- CRC can detect with a very high probability burst errors of length greater than the degree of the polynomial.

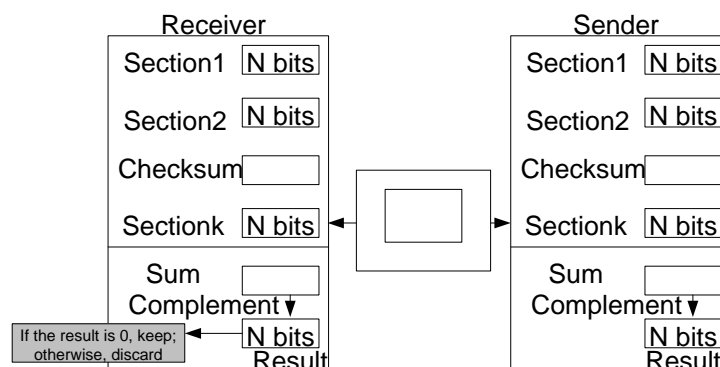
Example:

The CRC-12 ($x^{12} + x^{11} + x^3 + x + 1$). Which has a degree of 12, will detect all burst errors affecting an odd number of bits, will detect all burst errors with a length less than or equal to 12, and will detect 99.97 percent of the time burst with a length of the time burst errors with a length of 12 or more.

Checksum

- used by the higher layer protocols
- is based on the concept of redundancy (VRC, LRC, 'CRC)

Checksum Generator:



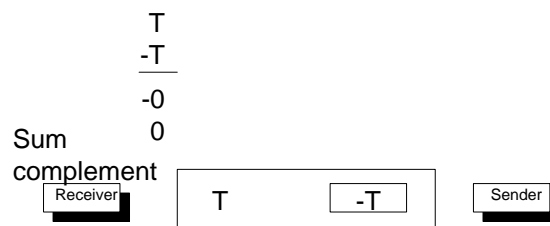
- To create the checksum the sender does the following:**

The unit is divided into K sections, each of n bits.

Section 1 and 2 are added together using one's complement.
 Section 3 is added to the result of the previous step.
 Section 4 is added to the result of the previous step.
 The process repeats until section k is added to the result of the previous step.
 The final result is complemented to make the checksum.

• **Data unit and checksum:**

The receiver adds data unit and the checksum field. If the result is all 1s, the data unit is accepted; otherwise it is discarded.



Example:

Original data: 10101001 00111001

```

10101001
00111001
-----
11100010   Sum
00011101   Checksum
10101001 00111001 00011101 <= Sent data
  
```

At receiver side:

```

Received data: 10101001 00111001 00011101
10101001
00111001
00011101
-----
11111111 <= Sum

00000000 <= Complement
  
```

Error. Correction:

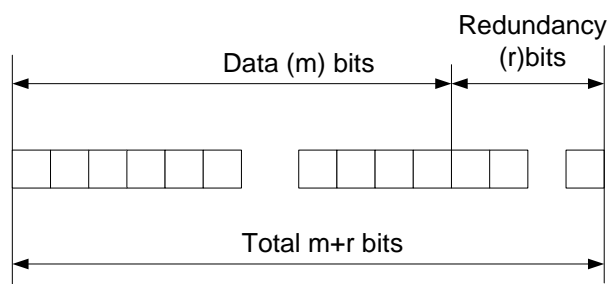
- Can be handled in two ways
- When an error is discovered, the receiver can have the sender retransmit the entire data unit.
- A receiver can use an error-correcting code, which automatically corrects certain errors.

Single-Bit error correction:

- Parity bit
- The secret of error correction is to locate the invalid bit or bits
- For ASCII code, it needs a three-bit redundancy code (000-111)

Redundancy bits:

- To calculate the number of redundancy bits (R) required to correct a given number of data bit (M)



- If the total number of bits in a transmittable unit is $m+r$, then r must be able to indicate at least $m+r+1$ different states ; $2^r \geq m+r+1$

For example:

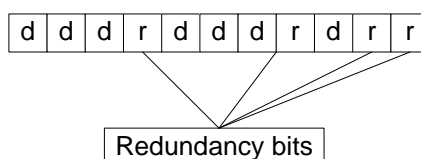
For value of m is 7(ASCII), the smallest r value that can satisfy this equation is 4 ($2^4 \geq 7+4+1$)

•Relationship between data and redundancy bits:

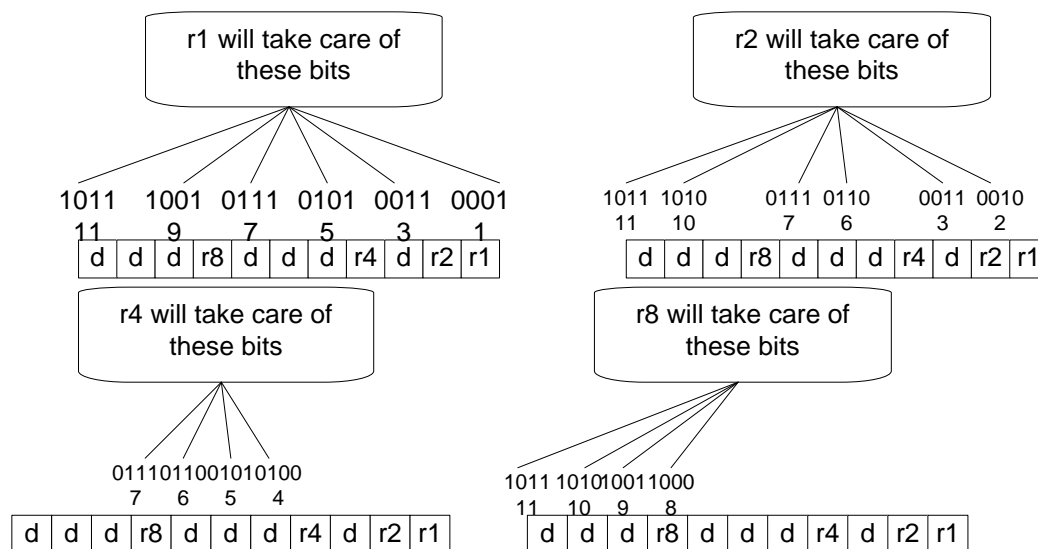
Number of Data Bits (m)	Number of Redundancy Bits (r)	Total Bits (m+r)
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11

Redundancy bits calculation:

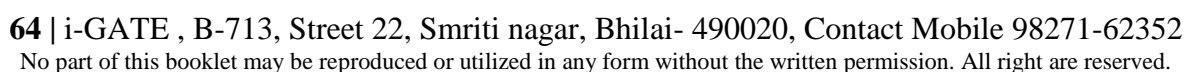
- Positions of redundancy bits in Hamming code



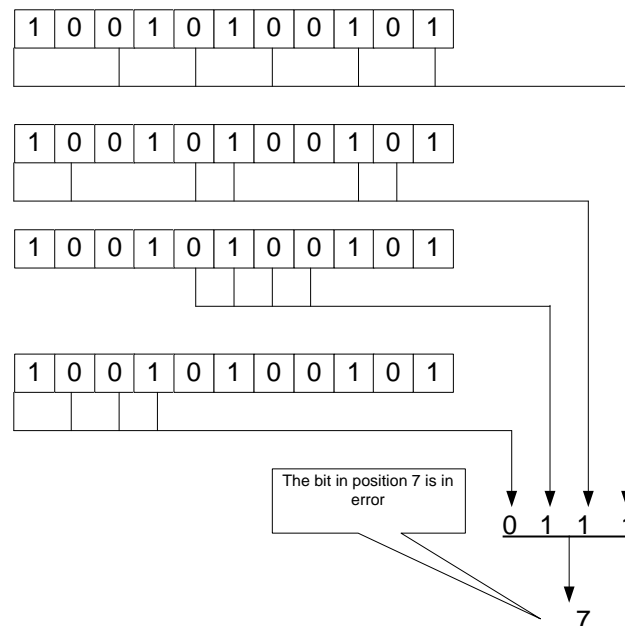
- r_1 = bits 1, 3, 5, 8, 7, 9, 11
 r_2 = bits 2, 3, 6, 7, 10, 11
 r_4 = bits 4, 5, 6, 7
 r_8 = bits 8, 9, 10, 11



Data	1	0	0		1	1	0		1		
------	---	---	---	--	---	---	---	--	---	--	--



•Error detection using Hamming Code:



FLOW CONTROL

The second aspect of data link control is flow control.

In most protocols, flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.

Flow control refers to a set of procedures used to restrict the amount of data, the sender can send before waiting for acknowledgement.

Two methods have been developed to control the flow of data across communications links: stop-and –wait and sliding window.

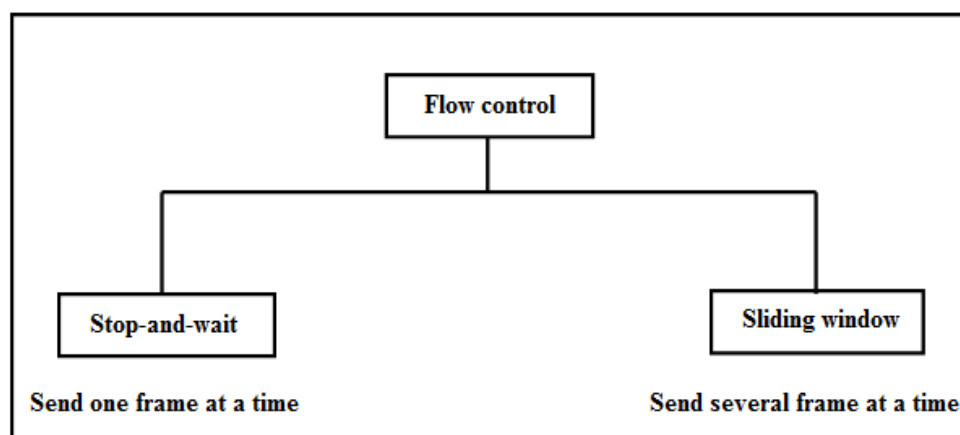


Figure: Categories of flow control

Stop-and-wait

In a stop-and-wait method of flow control, the sender waits for an acknowledgement after every frame it sends as shown in figure below. Only when an acknowledgement has been received is the next frame sent.

In the stop-and-wait method of flow control, the sender sends one frame and waits for an acknowledgement before sending the next frame.

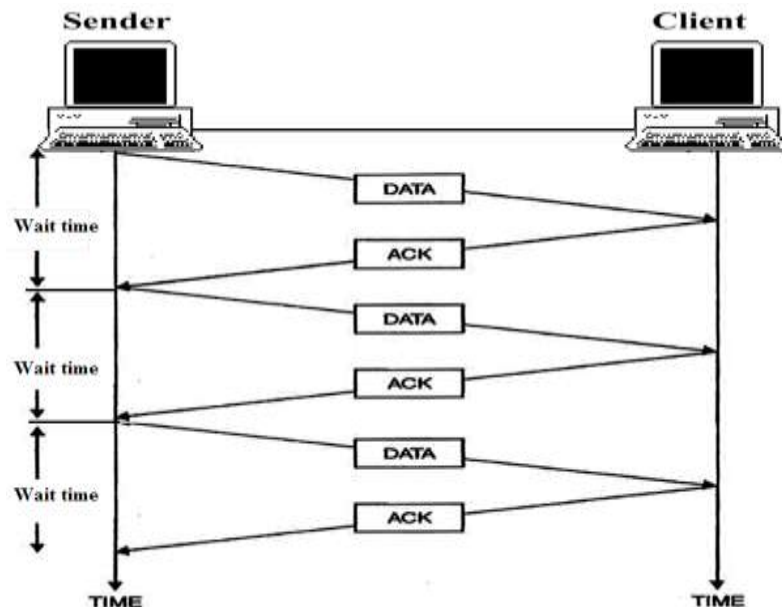


Figure: Stop-and-wait

The advantage of stop-and-wait is simplicity each frame is checked and acknowledged before the next frame is sent. The disadvantage is inefficiency: stop-and-wait is slow.

Stop-and-Wait Flow Control Protocol

1. Assume a half-duplex, point-to-point link
2. Throughput of stop & wait= One packet / RTT
3. $S_w = R_w = 1$
4. In stop & wait Ack's are numbered, but NACK's are not numbered.
5. In Stop & wait, the line utilization= $L/L+BR$
 Where B= bandwidth, L=Frame Size, R= RTT
6. It can be shown that the efficiency of the link is

$$U = 1/(1 + 2a)$$

Where a = Bit Propagation Time/Frame Transmission Time
 $T_p = D/V$, $T_t = L/B$.

Sliding Window

In the **sliding window** method of flow control, the sender can transmit several frames before needing an acknowledgement.

Frames can be sent one right after another, meaning the link can carry several frames at once and its capacity can be used efficiently.

The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames.

In the sliding window method of flow control, several frames can be in transmitting at a time.

The sliding window refers to imaginary boxes at both the sender and receiver.

This window can hold frames at either end and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement.

Frames may be acknowledged at any point without waiting for the window to fill up and may be transmitted as long as the window is not yet full.

To keep track of which frames have been transmitted and which received, sliding window introduces an identification scheme based, on the size of the window.

The frames are numbered modulo- n which means they are numbered from 0 to $n - 1$.

For example if $n = 8$, the frames are numbered 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1 The size of the window is $n - 1$ (in the case 7).

In other words the window cannot cover the whole module (8 frames); it covers one frame less.

When receiver sends an ACK, it includes the number of next frame it expects to receive. In other words to acknowledge the receipt of a string of the frame ending frame 4, the receiver sends an ACK containing the number 5. When the sender sees an ACK with the number 5, it knows that all frames up through number 4 have been received.

The window can hold $n - 1$ frame at either end; therefore a maximum of $n - 1$ frames may be sent before an acknowledgement is required. Figure below shows the relationship of a window to the main buffer.

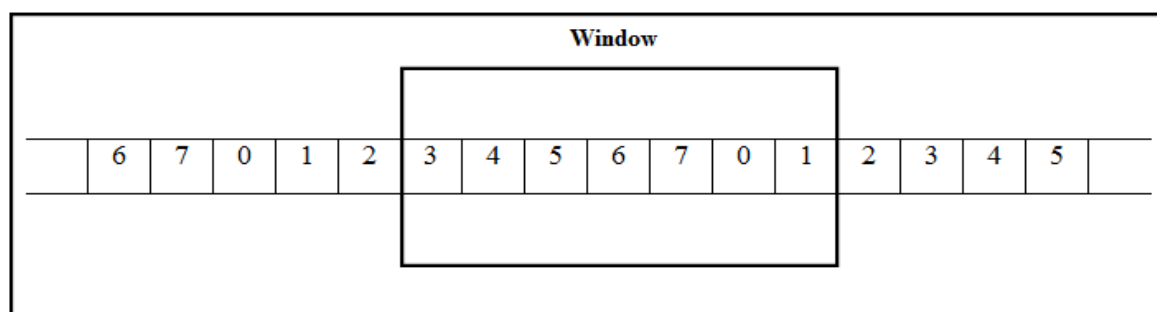


Figure: Sliding window

ERROR CONTROL

In the data link layer, the term *error control* refers primarily to methods of detection and retransmission.

Automatic Repeat Request (ARQ)

Error correction in the data link layer is implemented simply: anytime an error is detected in an exchange, a negative acknowledgement (NAK) is returned and the specified frame s are retransmitted. This process is called **automatic repeat request** (ARQ).

Error control in the data link layer is based on automatic repeat request (ARQ), which means retransmission of data in three cases: damaged frame, lost frame and lost acknowledgement.

ARQ error control is implemented in the data link layer as an adjacent to flow control; in fact, stop-and-wait flow control is usually implemented as stop-and-wait ARQ and sliding window is usually implemented as on of two variants of sliding window ARQ, called go-back-n or selective-reject.

Stop-and-wait ARQ

Stop-and-wait ARQ is a form of stop-and-wait flow control extended to include retransmission of data in case of lost or damaged frames.

Enables a sender to send multiple data frames before waiting for an ACK.

Sliding window protocol assumes two way communications (Full duplex).

SWP is used by most connection oriented protocol like PPP(Point to Point), HDLC, TCP etc.

SWP is used to take care of

- Error correction(By retransmissions) i.e. at packet level
- Flow control
- Message ordering by sender

Automatic Repeat request ARQ includes

- Error detection
- Positive ACK
- Retransmissions after time out
- Negative ACK and retransmissions

Popular ARQ mechanism are

- Stop & Wait

- GBN
- SR

Stop & wait, GBN and SR protocols are evaluated based on

- Buffer space utilization
- Channel Utilization
- Effective data rate

The technique of the temporarily delaying outgoing ACK at the receiver with an instruction to send it along with outgoing data frame is known as **piggybacking**.

For retransmission to work, four features are added to the basic flow control mechanism:

- The sending device keeps a copy of the last frame transmitted until it receives an acknowledgement for that frame. Keeping a copy allows the sender retransmit lost or damaged frames until they are received correctly.

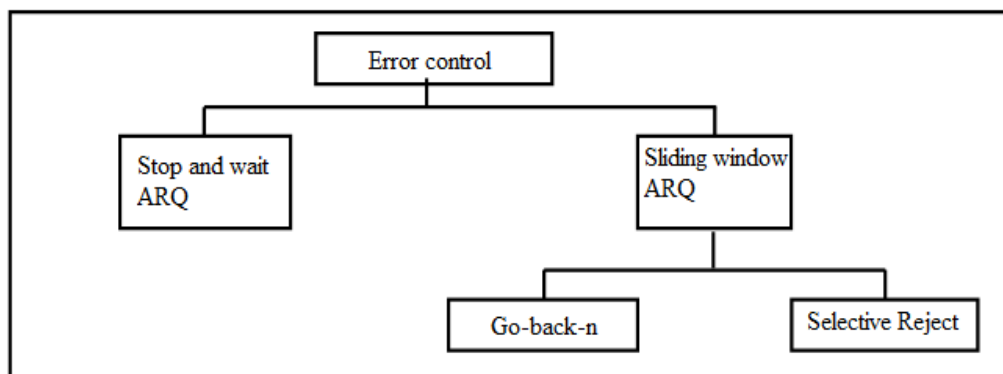


Fig. 3.17 Categories of error control

- For identification purpose, both data frames and ACK frame are numbered after 0 and 1. A data 0 frame is acknowledged by an ACK 1 frame, indicating that the receiver has gotten data 0 and is now expecting data 1. This numbering allows for identification of data frames in case of duplicating transmission (important in the case of lost acknowledgements, as we will see below).
- If an error is discovered in a data frame, indicating that it has been corrupted in transit, a NAK frame is returned. NAK frames, which are not numbered, tell the sender to transmit the last frame sent. Stop-and-wait ARQ requires that the sender wait until it receives an acknowledgement for the last frame transmitted before it transmits the next one. When the sending device receives a NAK, it resends the frame transmitted after the last acknowledgement, regardless of number.
- The sending device is equipped with a timer. If an expected acknowledgement is not received within an allotted time period the sender assumes that the last data frame was lost in transit and sends it again.

Advantage: Better use of channel band width.

Complication: As the outgoing packet is not readily available at the receiver, ACK waits for a long time than sender's time out period.

Sender: Manages a Send Window (SW)

A set of consecutive sequence numbers for packets the sender is permitted to send.

These packets have been (or, can be) sent, but are as yet not acknowledged.

- All data packets are numbered using a sequence field. n-bit sequence number = \Rightarrow sequence numbers range $[0 \dots 2^n - 1]$

SW size \leq sequence space size

Receiver: Manages a Receive Window (RW)

Receiver accepts packets falling within the receive window

Sender's normal behaviour:

The sender processes a data packet coming from the upper layer SW is NOT full

- Prepare a new packet with the "next" sequence number.
- Save a copy of the new packet
- Sends the new packet to MAC
- Starts a timer

Receiver's normal behaviour:

Packet corresponding to the first position in RW is received

- The "data" part of the packet is passed on to the upper layer.

An ACK is sent to the sender.

- The RW slides forward by 1 position (wrap around occurs)

- Handling error at the receiver

-

- An out-of-sequence packet is received

Note:

- $LFS - LAR \leq SWS$
- $LAF - LFR \leq RWS$

Where LFS= Last frame sent

LAR= Last Acknowledge received

LFR=Last Frame received

LAF= Last acceptable frame

Errors are handled in two different ways

Go-back-N
Selective Repeat

Go-back-n ARQ

It uses cumulative ACK or piggyback approach whenever possible to acknowledge the frame and **never accepts out of order packets** i.e. it refuses to accept any frame except the next frame it must give it to the network layer, so it corresponds to a receive **widow of size one**.

Receives algorithm is very simple, it accepts a packets if it is in sequence and rejects otherwise.

If the sender receives a NAK, it resends all outstanding frames.
It is conservative, because a single loss trigger a retransmissions of every possible last packet.

If the original packet lost was due to buffer overload, the bursts of packets triggered by go-back-n are likely to contribute to the overload and making it worse. So this can lead to a state where the network carries only retransmissions and this makes no net progress. We will call this as **Congestion Collapse**.

In GBN, if p is the error probability then the link efficiency = $w(1-p) / (1+2a)(1-p+wp)$
Where p is the packet loss probability and w is the senders window size.

Both ACK & NAK are numbered.
ACK-indicates the next number expected.
NAK-indicate only carry the number of the damaged frame.

When the packet error rate is high for link between sender and receiver, GBN is not useful and wastes lot of bandwidth.

Maximum sends window size in GBN is N where N is max sequence number or $N-1$ where N is the max number of sequence numbers available.

If k represent the number of bit of the available sequence number then $W_s=2^k-1$, $W_r=1$.

Error Control:

Assume that A is sending frames to B.

1. Damaged or Lost Frames:

A transmits frame i . B detects an error in frame i and has previously successfully received frame $i-1$. B sends a NAK i , indicating that frame i is rejected. When A receives this NAK, it must go back and retransmit frame i and all subsequent frames that it has transmitted.

Frame i is lost in transit. A subsequently sends frame $i+1$. B receives frame $i+1$ out of order, and sends a NAK i . Upon receipt of the NAK, A proceeds as retransmission.

Frame i is lost in transit and A does not soon send additional frames. B receives nothing and returns neither an ACK nor NAK. A will time out and retransmit frame i .

2. Damaged or Lost ACK:

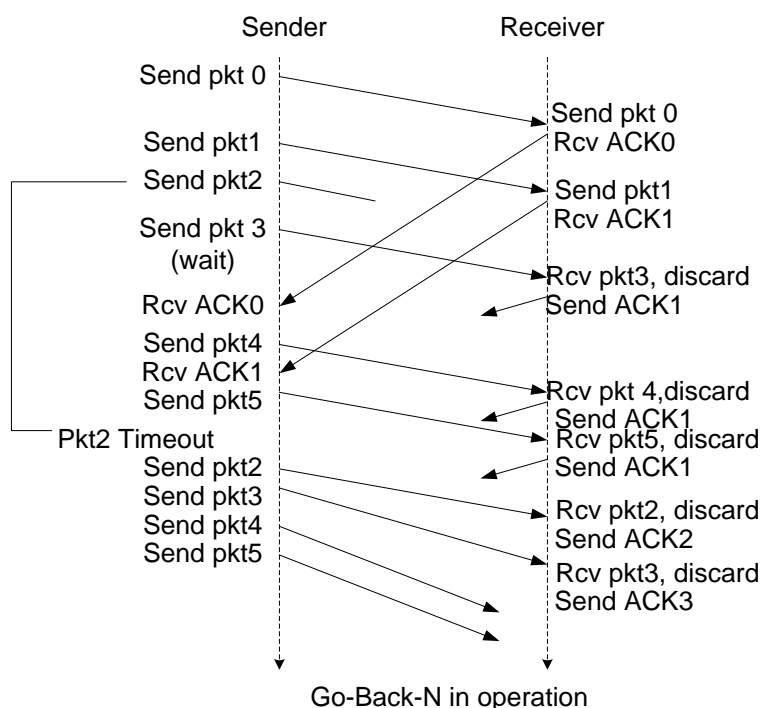
B receives frame i and sends ACK ($i+1$), which is lost in transit. Since ACKs are cumulative (e.g., ACK 6 means that all frames through 5 are acknowledged,) it may be that A will receive a subsequent ACK to a subsequent frame that will do the job of the lost ACK before the associated timer expires.

If A's timer expires, A retransmits frame i and all subsequent frames (or alternately, A can create a checkpoint by requesting an ACK).

3. Damaged or Lost NAK:

If a NAK is lost, A will eventually time out on the associated frame and retransmit that frame and all subsequent frames.

The following figure shows the operation of the GBN protocol for the case of a window size of four packets. Because of this window size limitation, the sender sends packets 0 through 3 but then must wait for one or more of these packets to be acknowledged before proceeding.



Selective-Reject ARQ

Receiver receives out of order packets, so the receiver's window size is more than one.

It uses independent or cumulative or piggyback ACK whenever possible.

ACK and NAK are numbered, but both refer to the frame received & frame lost respectively.

If the protocol receives a NAK, it resends just the frame specified by NAK.

Number of buffers and number of times needed in GBN, SR is equal to the **window size** but not the range of sequence numbers.

If frame is corrupted in transmit, a NAK is returned and the frame is reset out of sequence. The receiving device must be able to sort the frames it has and insert the retransmitted frame into its proper place in the sequence. To make such selectivity possible, a selective reject ARQ system differs from a go-back-n ARQ system in the following ways:

- The receiving device must contain sorting logic to enable it to recorder frame received out of sequence. It must also be able to store frame received after a NAK has been sent the damaged frame has been repaired.
- The sending device must contain a searching mechanism that allows it to find and select only the requested frame for retransmitted.
- A buffer in the receiver must keep all previously receives frame on hold until all retransmission have been sorted and any duplicate frames have been identified and discarded.
- To aid selectivity, ACK numbers, like NAK numbers, must refer to the frame receive for lost instead of the next frame expected.
- This complexity requires a smaller window size than is needed by the go-back-n method if it is to work efficiently. It is recommended that the window size be less than or equal to $(n + 1)/2$, where $n - 1$ is the go-back-n window size.
- If k represent the number of bit of the available sequence number then $W_s = 2^{k-1}$, $W_r = 2^{k-1}$.
- In SR if p is error probability then efficiency = $w(1-p) / (1+2a)(1+wp)$

Error Control:

Assume that A is sending frames to B.

1. Damaged or Lost frames:

A transmits frame i . B detects an error in frame i and has previously successfully received frame $i-1$. B sends a NAK i , indicating that frame i is rejected. B buffers any subsequent frames received that are within its receiving window. When A receives this NAK, it retransmits frame i only.

Frame i is lost in transit. A subsequently sends frame $i+1$. B receives frame $i+1$ out of order, and sends a NAK i . B buffers frame $i+1$ and all subsequent frames within its receiving window. When A receives the NAK, it retransmits frame i only.

Frame i is lost in transit and A does not soon send additional frames. B receives nothing and returns neither an ACK nor a NAK. A will time out and retransmit

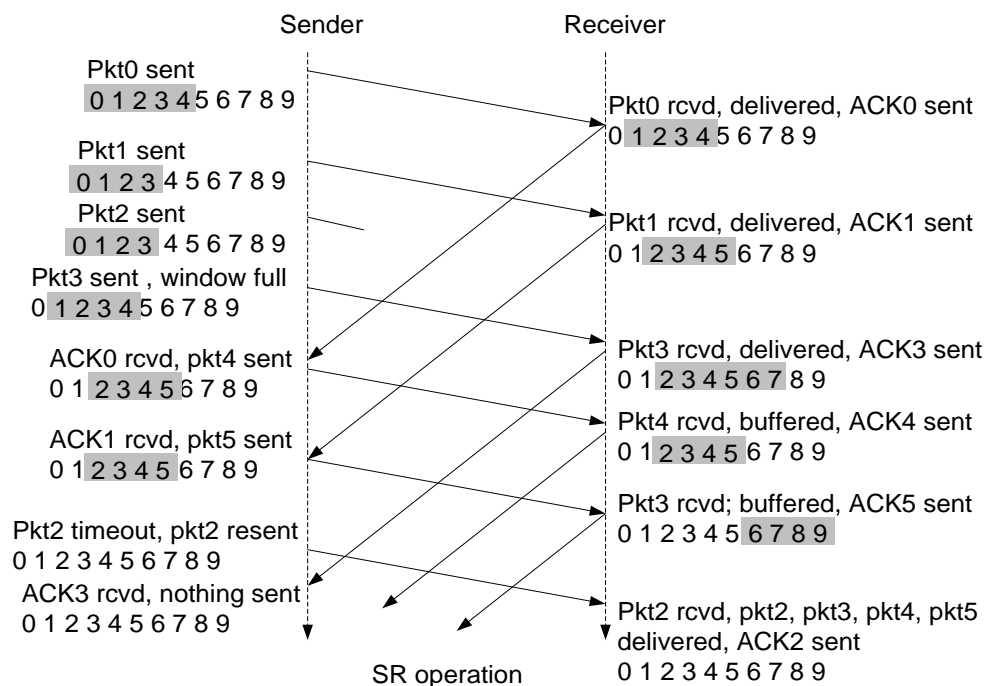
2. Damaged or Lost ACK:

B receives frame i and sends ACK ($i+1$), which is lost in transit. Since ACKs are cumulative, it may be that A will receive a subsequent ACK to a subsequent frame that will do the job of the lost ACK before the associated, timer expires.

If A's timer expires, A retransmits frame i only (or alternately, A can create a checkpoint by requesting an ACK).

3. Damaged or Lost NAK:

If a NAK is lost, A will eventually time out on the associated frame and retransmit that frame only.



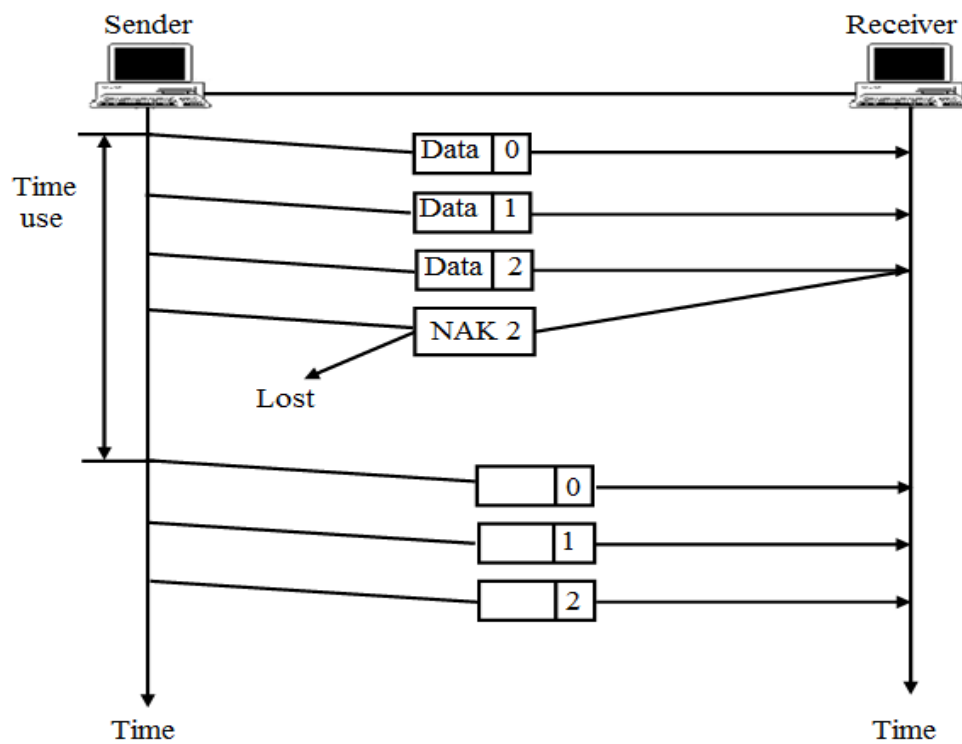


Figure: Go-back-n ACK

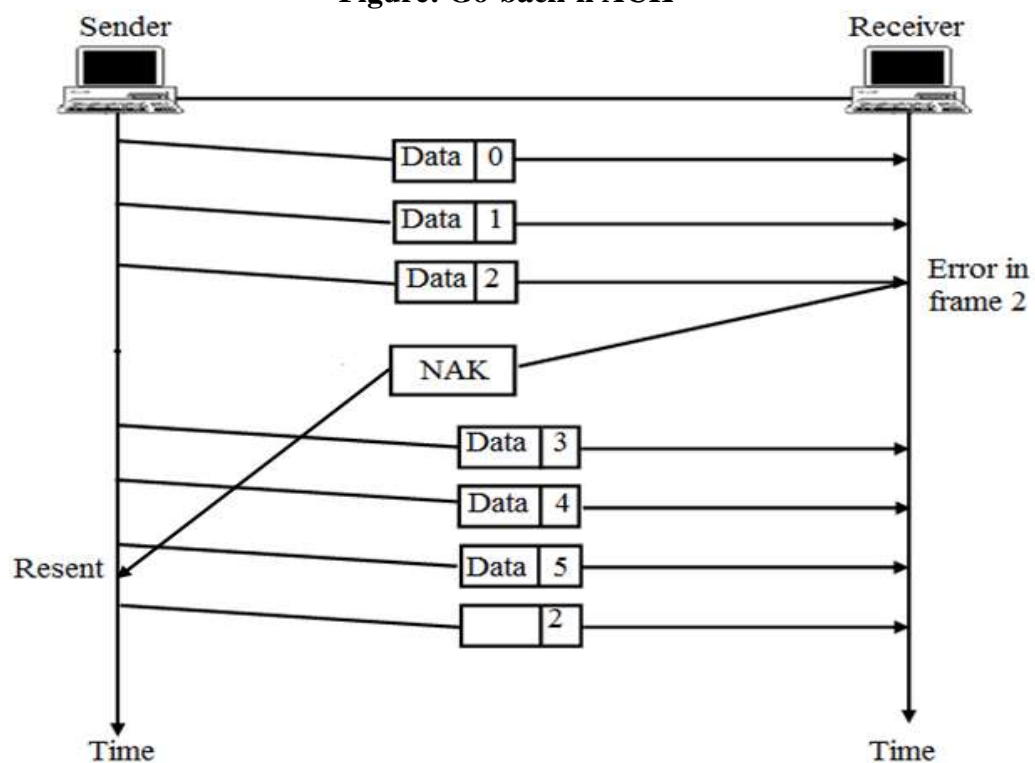
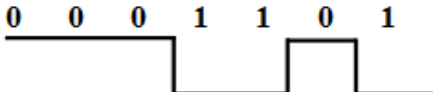
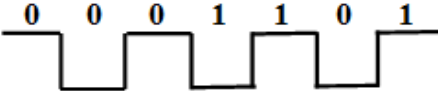
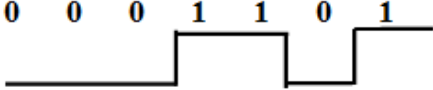


Figure: Selective reject damaged frame

Assignment:

- CRC – 8 polynomial is?
 (A) $x^8 + x^6 + x^4 + x^2 + 1$ (C) $x^8 + x^2 + x^1 + 1$
 (B) $x^6 + x^5 + x^4 + 1$ (D) $x^2 + x + 1$
- Calculate the latency for data transmission with the following parameter
 Fibre optic link of length 20 kms
 Packet size: 2KB
 Transfer rate: 100 Mbps
 Queuing time $40\mu s$
 (A) 303.84 s (C) 340 s
 (B) 330 s (D) 300.45 s
- CRC – 10 polynomial is?
 (A) $x^8 + x^4 + x^2 + 1$ (C) $x^{10} + x^9 + x^5 + x^4 + x^1 + 1$
 (B) $x^3 + x^2 + x + 1$ (D) $x^2 + x + 1$
- CRC – 8 comes into picture, when?
 (A) When the character length is 8 bits
 (B) When the character length > 4 bits
 (C) When the character length is 6 bits
 (D) None
- CRC – 12 polynomial is?
 (A) $x^{12} + x^{11} + x^3 + x^2 + x^1 + 1$ (C) $x^8 + x^6 + x^4 + x^2 + 1$
 (B) $x^{12} + x^{10} + x^8 + x^6 + x^4 + x^2 + 1$ (D) None
- Sketch the NRZL encoding for the bit stream 0001101
 (A) 
 (B) 
 (C) 
 (D) None
- CRC – CCITT polynomial is?
 (A) $x^{14} + x^5 + x^3 + 1$ (C) $x^{16} + x^{15} + x^5 + 1$
 (B) $x^{10} + x^5 + x^0 + 1$ (D) $x^{16} + x^8 + x^4 + x^2 + 1$
- FDM is commonly used on what type of broadcast?
 (A) Satellite transmissions (C) AM radio
 (B) FM radio (D) Bursty

9. What is the CCITT standard for a T3?
(A) 2 multiplexed T1S (C) 2 multiplexed T2S
(B) 4 multiplexed T1S (D) 4 multiplexed T2S
10. What is the 16 – bit checksum for the following phrase?
giGG1e
(A) 1B16 (C) 1B29
(B) 1C19 (D) 1BB2
11. In an old parity checksum scheme, what is the value of the parity bit for the following sequence 0101101?
(A) 2 (C) 3
(B) 1 (D) 0
12. Throughput is?
(A) $\frac{\text{Transfer time}}{\text{Data size}}$ (C) Data size \times transfer size
(B) $\frac{\text{Data size}}{\text{Transfer time}}$ (D) None
13. CRC – CCITT comes into picture, when?
(A) Character length is 10 (C) Character length is 6
(B) Character length is 8 (D) Character length is 4
14. How many hamming bits are required when using the Hamming code for the message “Help!”?
(A) 40 (C) 5
(B) 8 (D) 200
15. Sketch the NRZL encoding for the bit stream 10011001.
16. Station A is transferring data to Station B in packets of 50000 bit each, over a satellite link at 2 megabits/*sec. The satellite is at a distance of 36000 kms from both A and B; the satellite is just a repeater – it rebroadcasts the data without any delay. B sends a acknowledgement for each packet as soon as it is completely received. The acknowledgement is 560 bits long and it is sent over a twisted – pair land line, 460 kms long, at 56 kilobits per second. There is a switch with a constant delay of 1 millisecond on this line. Calculate the total latency measured from the first bit transmitted by A to the last bit of the acknowledgement received by A.
(A) 265 ms (C) 290 ms
(B) 278 ms (D) None
17. How many character per second (7 bits p 1 parity) can be transmitted over a 2400 line in case of synchronous transfer (1 stop and 1 start bit)
(A) 300 (C) 250
(B) 350 (D) 240
18. How many character per second can be transmitted in question 17 in case of asynchronous transfer.

- (A) 300 (C) 350
(B) 240 (D) 400
19. In a stop and wait ARQ bandwidth 1Mbps and 1 bit takes 20 ms to make round trip if system data frame are 1000 bits in length. What is the % of utilization of the link.
(A) 2% (C) 10%
(B) 3% (D) 5%
20. In the above question if Go Back N ARQ with 15 frames are used then what would be % of utilization
(A) 30% (C) 75%
(B) 50% (D) 80%

GATE Questions CS:

1. Let $G(x)$ be the generator polynomial used for CRC checking. What is the condition that should be satisfied by $G(x)$ to detect odd number of bits in error?
(A) $G(x)$ contains more than two terms
(B) $G(x)$ does not divide $1 + X^k$, for any K not exceeding the frame length
(C) $1 + X$ is a factor of $G(x)$
(D) $G(x)$ has an odd number of terms
[GATE-CS-2008]
2. The distance between two stations M & N is L km. All frames are K -bits long. The propagation delay per kilometre is t seconds. Let R bits/sec be the channel capacity. Assuming that processing delay is negligible, the max no of bits for the sequence no field in the frame for maximum utilization, when the sliding window protocol is used is:
(A) $\left\lceil \log_2 \frac{2LtR+2K}{K} \right\rceil$ (C) $\left\lceil \log_2 \frac{2LtR+K}{K} \right\rceil$
(B) $\left\lceil \log_2 \frac{2LtR}{K} \right\rceil$ (D) $\left\lceil \log_2 \frac{2LtR+2K}{2K} \right\rceil$
[GATE-CS-2007]
3. The message 11001001 is to be transmitted using the CRC. Polynomial $X^3 + 1$ to protect it from errors. The message that should be transmitted is:
(A) 11001001000 (C) 11001010
(B) 11001001011 (D) 110010010011
[GATE-CS-2007]
4. Station A needs to send a message consisting of 9 packets to Station B using a sliding window (window size 3) and go-back-n error control strategy. All packets are ready and immediately available for transmission. If every 5th packet that A transmits gets lost (but no acks from B ever get lost), then what is the number of packets that A will transmit for sending the message to B?
(A) 12 (C) 16
(B) 14 (D) 18
[GATE-CS-2006]
5. Station A uses 32 byte packets to transmit message to station B using a sliding window protocol. The round trip delay between A and B is 80 ms and the bottleneck bandwidth on the path between A and B is 128 kbps. What is the optimal window size that A should use?
(A) 20 (C) 160
(B) 40 (D) 320
[GATE-CS-2006]

6. The maximum window size for data transmission using the selective reject protocol with n bit frame sequence numbers is:
 (A) 2^n (C) $2^n - 1$
 (B) 2^{n-1} (D) 2^{n-2} [GATE-CS-2005]
7. How many 8-bit characters can be transmitted per second over a 9600 baud serial communication link using asynchronous mode of transmission with one start bit, two stop bits and one parity bit?
 (A) 600 (C) 876
 (B) 800 (D) 1200 [GATE-CS-2004]
8. In serial data transmission, every byte of data is padded with a '0' in the beginning and one or two '1's at the end of byte because
 (A) Receiver is to be synchronized for byte reception
 (B) Receiver recovers lost '0's and '1's from these padded bits
 (C) Padded bits are useful in parity computation
 (D) None of the above [GATE-CS-2002]

GATE Questions IT:

1. Data transmitted on a link uses the following 2D parity scheme for error:
 Each sequence of 28 bits is arranged in a 4×7 matrix (rows r_0 through r_3 and through d_i) and is padded with a column d_0 an row r_4 of parity bits computed using the even parity scheme. Each bit of column d_0 (respectively, row r_4) gives the parity of the corresponding row, (respectively column). These 40 bits are transmitted over the data link.

	d_7	d_6	d_5	d_4	d_3	d_2	d_1	d_0
r_0	0	1	0	1	0	0	1	1
r_1	1	1	0	0	1	1	1	0
r_2	0	0	0	1	0	1	0	0
r_3	0	1	1	0	1	0	1	0
r_4	1	1	0	0	0	1	1	0

The table shows data received by a receiver and has n corrupted bits. What is the minimum possible value of n?

- (A) 1 (C) 3
 (B) 2 (D) 4 [GATE-IT-2008]
2. Suppose that it takes 1 unit of time to transmit a packet (of fixed size) on a communication link. The link layer uses a window flow control protocol with a window size of N packets. Each packet causes an ACK or NAK to be generated by the receiver and ACK/NAK transmission times are negligible. Further, the round trip time on the link is equal to N units. Consider time $I > N$. If only acks have been received till time i(in packets per unit time) is

- (A) $1 - N/I$ (C) 1
 (B) $1/(N + i)$ (D) $1 - e^{(i/N)}$

[GATE-IT-2006]

3. Which of the following statements is TRUE?

- (A) Both Ethernet frame and IP packet include checksum fields
 (B) Ethernet frame includes a checksum field and IP packet includes a CRC field
 (C) Ethernet frame includes a CRC field and IP packet includes a checksum field
 (D) Both Ethernet frame and IP packet include CRC fields

[GATE-IT-2006]

4. Consider the following message $M = 1010001101$. The cyclic redundancy check (CRC) for this message using the divisor polynomial $x^5 + x^4 + x^2 + 1$ is:

- (A) 01110 (C) 10101
 (B) 01011 (D) 10110

[GATE-IT-2005]

5. Consider a parity check code with three data bit and four parity check bit. Three of the code words are 0101011, 10001101 and 1110001. Which of the following are also code words?

- I. 0010111
 II. 0110110
 III. 1011010
 IV. 0111010

- (A) I and III (C) II and IV
 (B) I, II and III (D) I, II, III and IV

[GATE-IT-2004]

6. A 20Kbps satellite link has a propagation delay of 400 ms. The transmitter employs the "go back n ARQ" scheme with n set to 10. Assuming that each frame is 100byte long, what is the maximum data rate possible?

- (A) 5 Kbps (C) 15 Kbps
 (B) 10 Kbps (D) 20 Kbps

[GATE-IT-2004]

7. In a sliding window ARQ scheme the transmitter's windows size is N and the receiver's windows size is M, the minimum number of distinct sequences numbered required to ensure correct operation of the ARQ scheme is

- (A) $\min(M, N)$ (C) $M + N$
 (B) $\max(M, N)$ (D) MN

[GATE-IT-2004]

8. A serial transmission T_1 uses 8 information bits, 2 start bits, 1 stop bit and 1 parity bit for each character. A synchronous transmission T_2 uses 3 eight bit sync character followed by 30 eight bit information character. If the bit rate is 1200 bits/second in the cases, what are the transfer rates of T_1 and T_2 ?

- (A) 100 character/sec, 153 character/sec
 (B) 80 character/sec, 136 character/sec
 (C) 100 character/sec, 136 character/sec
 (D) 80 character/sec, 153 character/sec

[GATE-IT-2004]

9. What is the rate of a video terminal unit with 80 character/line, 8bit/character and horizontal sweep time of $100\mu s$ (including $20\mu s$ of retrace)?

- (A) 8 Mbps (C) 0.8 Mbps
 (B) 6.4 Mbps (D) 0.64 Mbps

Answer keys

Assignment:

1	C	2	A	3	C	4	B	5	A	6	A	7	C	8	C	9	D	10	A
11	B	12	B	13	B	14	A	15	S	16	B	17	A	18	B	19	D	20	C

Note: "S" Implies subjective Questions

GATE Questions CS:

1	C	2	C	3	B	4	C	5	B	6	B	7	A	8	A
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

GATE Questions IT:

1	C	2	C	3	C	4	C	5	A	6	D	7	B	8	B	9	D
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Explanations:

Assignment:

1. [Ans. C]

$$x^8 + x^2 + x^1 + 1$$

2. [Ans. A]

$$\text{Latency} = 303.84 \text{ sec}$$

3. [Ans. C]

$$\text{CRC-10 polynomial is } x^{10} + x^9 + x^5 + x^4 + x^1 + 1$$

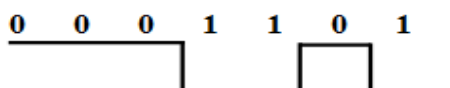
4. [Ans. B]

If character length > 4 bits.

5. [Ans. A]

$$\text{CRC-12: } x^{12} + x^{11} + x^3 + x^2 + x^1 + 1$$

6. [Ans. A]



0 → high

1 → low

7. [Ans. C]

CRC-CCITT: $x^{16} + x^{15} + x^5 + 1$

8. [Ans. C]

For FM radio

9. [Ans. D]

CCITT standard for a T3 is multiplexed T2S.

10. [Ans. A]

1B16

11. [Ans. B]

Parity bit = 1

12. [Ans. B]

Throughput = $\frac{\text{Data rate}}{\text{Transfer time}}$

13. [Ans. B]

If character length > 8

14. [Ans. A]

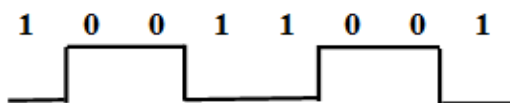
The total number of bits in the message is

$M = 8 \text{ bits / character} * 5 \text{ characters} = 40 \text{ bits}$

The number of bits in the message should be counted and the value applied in the equation $2H > M + H - 1$.

This when applied yields a value of 6 for H. This satisfies the equation.

15.



16. [Ans. B]

A – sat – B link:

Prop time = $72,000 \text{ kms} / 300,000 \text{ kms/sec} = 240 \text{ ms}$

Transmission time = $50,000 \text{ bits} / 2 \times 10^6$

bits/sec = 25 ms

Latency = 265 ms

B – switch – A link

Prop time = $460 \text{ kms} / 2.3 \times 10^5 \text{ kms/sec} = 2 \text{ ms}$

Queuing time = 1 ms

Transfer time = $560 \text{ bits} / 56,000 \text{ bits/sec} = 10 \text{ ms}$

Latency = 13 ms

Overall latency for message + ack = 278 ms

17. [Ans. A]

For synchronous transfer, start bit and stop bit are ignored.

$$\text{So for synchronous transfer} = \frac{2400}{8} = 300$$

18. [Ans. B]

$$\text{For synchronous transfer} = \frac{2400}{8+2} = 240 \text{ character/sec}$$

19. [Ans. D]

Band width delay product

$$1 \times 10^6 \times 20 \times 10^{-3} = 20000 \text{ bits}$$

System sends 1000 bits

$$\text{Link utilization} = \frac{1000 \times 100}{20000} = 5\%$$

20. [Ans. C]

$$\text{Total No. of bits} = 15 \times 1000$$

$$\text{Utilization} = \frac{15 \times 1000 \times 100}{20000} = 75\%$$

GATE Question CS:

1. [Ans. C]

$(1 + x)$ is a factor of $G(x)$

2. [Ans. C]

Frame Size = K bit

Propagation delay = t sec/km

Channel capacity = R bits/sec

Distance = L km

Round trip delay = $2Lt$ sec.

$$\text{Window size } \omega = \frac{2Lt}{R/R} + 1$$

$$= \frac{2L t R}{K} + 1$$

$$= \frac{2L t R + K}{K}$$

$$\# \text{ of bits} = \left\lceil \log_2 \frac{2L t R + K}{K} \right\rceil$$

3. [Ans. B]

$$P(x) = 11001001$$

divisor $D(x) = 1001$ and CRC remainder is 011, so the transmitted message is 11001001011

4. [Ans. C]

Number of packet = 16

5. [Ans. B]

Given round trip delay $t = 80$ ms

$$R = 128 \text{ Kbps} = 128 \times 10^3 \text{ bps}$$

$$L = R t = 128 \times 10^3 \times 80 \times 10^{-3}$$

So, optional window size = n

$$= \frac{128 \times 80}{32 \times 8}$$

6. [Ans. B]

In the case of selective Reject protocol; the maximum window size = $2^n/2 = 2^{n-1}$

7. [Ans. A]

No. of bit transmitted = $\frac{9600}{12 \text{ bits}} = 800$

8. [Ans. A]

Receiver is to be synchronized for byte reception

GATE Questions IT:

1. [Ans. C]

Here two dimensional checking is done, i.e. both horizontal and vertically,
 If the total number of 1's is odd, parity bit is 1 and for even number of 1's parity bit is 0.

2. [Ans. C]

Goodput = Packet/unit time

$$= \frac{I-N}{I} = 1 - N/I$$

$$= 1 - N/I$$

3. [Ans. C]

Ethernet frame include a CRC field and IP packet include a checksum field.

4. [Ans. C]

$M = 1010001101$
 Polynomial = $x^5 + x^4 + x^2 + 1$
 CRC for given message = 10101

5. [Ans. A]

0010111 and 1011010 are also code words.

6. [Ans. D]

Maximum data rate possible = speed of satellite transmission rate

$$= 20 \text{ Kbps}$$

7. [Ans. B]

Minimum number of distinct sequence number = $\max(M, N)$

8. [Ans. B]

Character transmitted = $T_1 = \frac{1200}{12} = 100$

$$= \frac{1200}{8.8} = 136$$

9. [Ans. D]

Bit rate = $\frac{64}{100 \mu} = 0.64 \text{ Mbps}$

Local Area Network

(Lan Technologies: Ethernet, Token Ring)

Introduction

Networks can be divided into two categories: those using **point to point connections** and those using **broadcast** channels.

Here we want to know how to handle broadcast networks. As compared to point to point networks, a major issue is handling arbitration when there is competition for the network. This is the bottom sub-layer of the Data Link Layer.

This Chapter is especially relevant for LANs.

1. The Channel Allocation Problem

How to allocate a single channel among multiple users.

2. Multiple Access Protocols

How to handle contention for the use of a channel.

3. IEEE Standards for LANs

How do the protocols of the last sections apply to real systems? Here we talk about the actual standards in use.

4. Bridges

Ways of connecting networks together.

5. High Speed LANs

Directions in high speed networks.

MAC sub-layer deals with broadcast networks and their protocols.

In broadcast networks, the key issue is: in a multiuser environment where many user using the single channels for their communication, Who will go next i.e. if a person stop using the channel and many are waiting for communication (either to send or receive the data) then out of them who can use the channel next.

The protocol used to determine who goes next on a multi access channel belong to sub-layer of the data link layer called the MAC (Media Access Control) sub-layer

CHANNEL ALLOCATION PROBLEM:

The traditional (phone company) way of allocating a single channel is Frequency Division Multiplexing. (See Figure) FDM works fine for limited and fixed number of users.

Inefficient to divide into fixed number of chunks. May not all be used, or may need more. Doesn't handle burstiness.

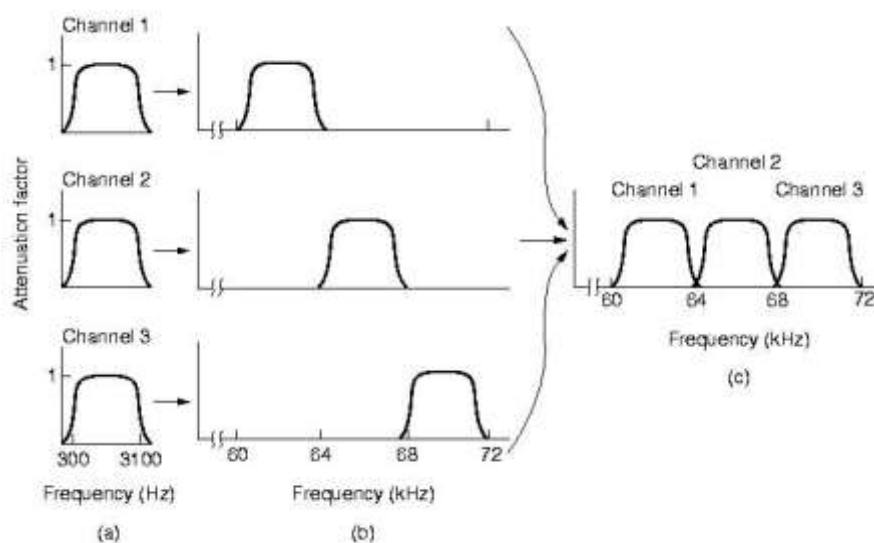
T = mean time delay

C = capacity (bps)

λ = arrival rate

$1/m$ = mean length

$$T = 1 / (mC - \lambda)$$



STATIC CHANNEL ALLOCATION IN LANs AND MANs

Now divide this channel into N subchannels, each with capacity C/N . Input rate on each of the N channels is λ/N . Now

$$T(\text{fdm}) = \frac{1}{m(C/N) - \lambda/N} = \frac{N}{mC - \lambda} = NT$$

DYNAMIC CHANNEL ALLOCATION

Possible underlying assumptions include:

Station Model

Assumes that each of N "stations" (packet generators) independently produce frames. The probability of producing a packet in the interval dt is λdt where λ is the constant arrival rate. That station generates no new frame until that previous one is transmitted.

Single Channel Assumption

There's only one channel; all stations are equivalent and can send and receive on that channel.

Collision Assumption

If two frames overlap in any way time-wise, then that's a collision. Any collision is an error, and both frames must be retransmitted. Collisions are the only possible error.

Continuous Time

There's no "big clock in the sky" governing transmission. Time is not in discrete chunks.

Slotted Time

Alternatively, frame transmissions always begin at the start of a time slot. Any station can transmit in any slot (with a possible collision.)

Carrier Sense

Stations can tell a channel is busy before they try it. NOTE - this doesn't stop collisions. LANs have this, satellite networks don't.

Multiple Access Protocol

Collisions work well for low utilization (they're not likely to happen.) Arbitration, which we'll talk about later, works better at high utilization.

Many algorithm for allocation for multiple access channel are known, we will discuss them in brief:

ALOHA Protocol

Developed in Hawaii in the 1970s

We will discuss the two version of ALOHA here: pure and slotted

PURE ALOHA

The basic idea of ALOHA system is simple let user transmit whenever they have data to be sent. There will be collision, of course, and colliding frames will be destroyed.

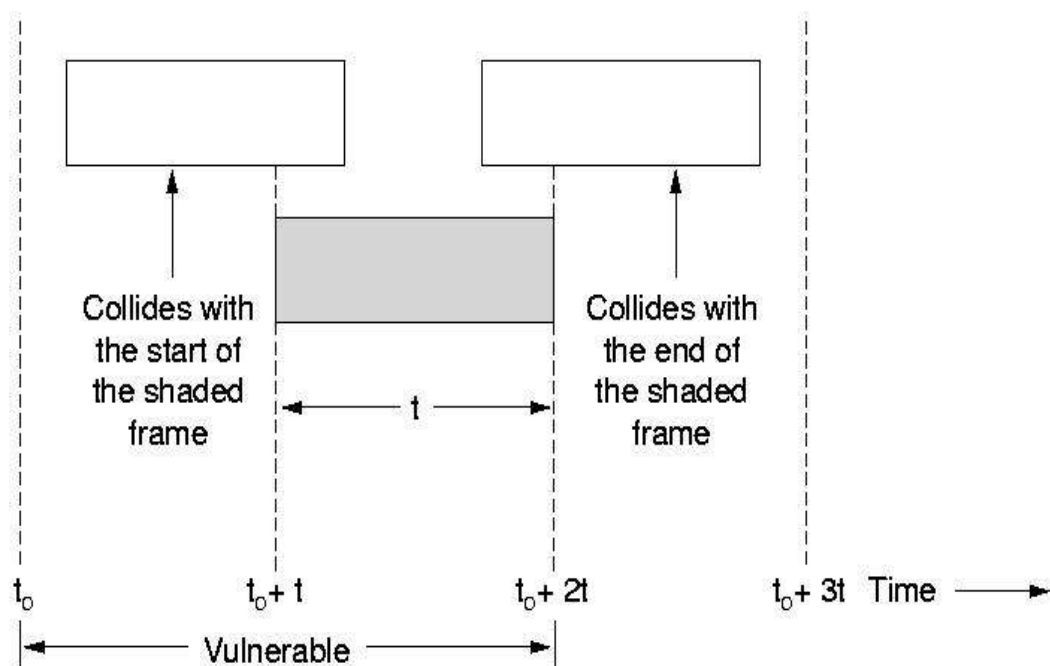
However due to feedback property of broadcasting, a sender can always find out whether or not its frame was destroyed by listening to the channels.

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

If the frame was destroyed, the sender just waits the random interval of time and sends again.

- S = frames to be transmitted. In units of frames per frame time so that $0 < S < 1$. (What is the meaning of frame time as used here??)
- $G = S +$ frames retransmitted due to previous collisions.
- P_0 = probability that a frame does NOT suffer collision.

- $S = P_0 \times G$



Use the Figure to determine collision vulnerability.

A sketch of frame generation in an ALOHA system is given in below figure we have made the frames all the same lengths the throughput of ALOHA system is maximized **by having the uniform** size rather than allowing variable length frames.

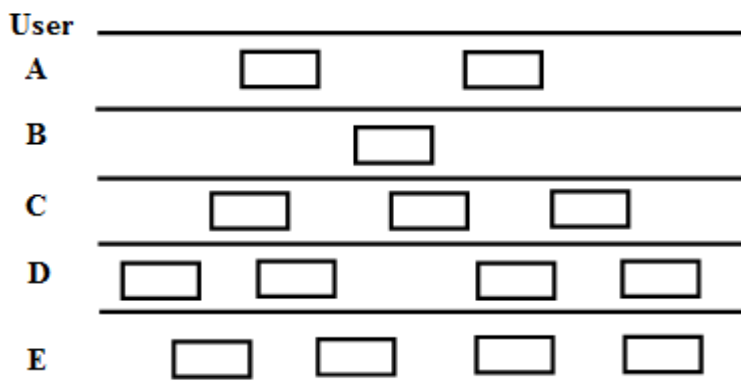


Figure: Pure ALOHA, frames are transmitted at completely arbitrary times.

Derivation of efficiency of ALOHA channel: Efficiency means, the number of successful transmission without collision.

Let the "frame time" denote the amount of time needed to transmit the standard fixed length frame. And assume that the infinite population of users generates the new frames according to a poisson distribution with mean N frames per frame – time.

If $N > 1$, the user community is generating frames at the higher rate than the channel can handle, and nearly every frame can suffer in collision. For the reasonable throughput we would expect $0 < N < 1$.

Let us further assume that the probability of k transmission attempts per frame – time, old and new frames combined, is also Poisson, with mean G per frame – time. Clearly, $G > N$. At low load (i.e, $N \gg 0$), there will be few collision, so $G \gg N$. At high load there will be many collisions, so $G > N$.

Under all loads, the throughput is just the offered load, G time the probability of transmission the being successful.

The is $S = G \times P_0$, where p_0 is the probability that a frame does not suffer a collision.

The frame will not suffer collision if no other frames are sent within one frame time of its start, as shown in above figure.

Probability that k frames are generated during a given frame time (Poisson distribution):

$$\Pr[k] = \frac{G^k e^{-G}}{k!}$$

So the probability of zero frames is just e^{-G} (i.e. $k=0$).

The average amount of transmission-attempts for 2 consecutive frame-times is $2G$. Hence, for any pair of consecutive frame-times, the probability of there being k transmission-attempts during those two frame-times is:

$$\frac{(2G)^k e^{-2G}}{k!}$$

Therefore, the probability ($Prob_{pure}$) of there being zero transmission-attempts between $t-T$ and $t+T$ (and thus of a successful transmission for us) is:

$$Prob_{pure} = e^{-2G}$$

The throughput can be calculated as the rate of transmission-attempts multiplied by the probability of success, and so we can conclude that the throughput (S_{pure}) is:

$$S_{pure} = G e^{-2G}$$

Vulnerable time = $2 \times T$.

The maximum throughput is $0.5/e$ frames per frame-time (reached when $G = 0.5$), which is approximately 0.184 frames per frame-time. This means that, in Pure ALOHA, only about 18.4% of the time is used for successful transmissions.

Let G be the average number of nodes that begin transmission within period T (the frame time). If a large number of nodes are trying to transmit, then by using Poisson distribution, the probability that exactly x nodes begin transmission during period T is

$$P[X = x] = \frac{G^x e^{-G}}{x!}$$

Therefore the probability that during any particular period from $t=2nT$ to $t=(2n+1)T$, (that is for any particular non-zero integral value of n) exactly one node will begin transmission is

$$P[X = 1] = \frac{G^1 e^{-G}}{1!} = Ge^{-G}$$

And the probability that during any particular period $t=(2n+1)T$ to $t=(2n+2)T$, no node will begin transmission is

$$P[X = 0] = \frac{G^0 e^{-G}}{0!} = e^{-G}$$

But for successful transmission of a frame, both the events should occur simultaneously. That is during period $t=2nT$ to $t=(2n+1)T$, exactly one node begins transmission and during $t=(2n+1)T$ to $t=(2n+2)T$ no node begins transmission. Hence the probability that both the independent events will occur simultaneously is

$$P = P(0) \times P(1) = Ge^{-G} \times e^{-G} = Ge^{-2G}$$

This is the throughput. By throughput we mean the probability of successful transmission during minimum possible period. Therefore the throughput in pure ALOHA,

$$S_{pure} = Ge^{-2G}$$

Similarly for slotted ALOHA, a frame will be successfully transmitted, if exactly one node will begin transmission at the beginning of any particular time slot (equal to frame time T). But the probability that one node will begin during any particular time slot is

$$P[X = 1] = \frac{G^1 e^{-G}}{1!} = Ge^{-G}$$

This is the throughput in slotted ALOHA. Thus,

$$S_{slotted} = Ge^{-G}$$

Slotted ALOHA

An improvement to the original ALOHA protocol was "Slotted ALOHA", which introduced discrete timeslots and increased the maximum throughput.^[11] A station can send only at the beginning of a timeslot, and thus collisions are reduced. In this case, we only need to worry about the transmission-attempts within 1 frame-time and not 2 consecutive frame-times, since collisions can only occur during each timeslot. Thus, the probability of there being zero transmission-attempts in a single timeslot is:

$$Prob_{slotted} = e^{-G}$$

the probability of k packets is:

$$Prob_{slotted} k = e^{-G} (1 - e^{-G})^{k-1}$$

The throughput is:

$$S_{slotted} = Ge^{-G}$$

The maximum throughput is $1/e$ frames per frame-time (reached when $G = 1$), which is approximately 0.368 frames per frame-time, or 36.8%.

Slotted ALOHA is used in low-data-rate tactical satellite communications networks by military forces, in subscriber-based satellite communications networks, mobile telephony call setup, set-top box communications and in the contactless RFID technologies.

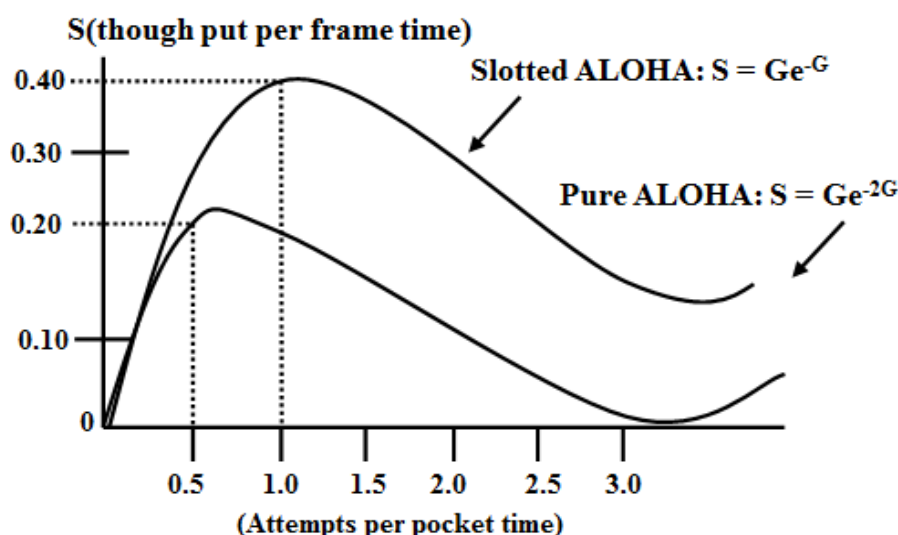


Figure: Throughput versus offered traffic for ALOHA systems

Carrier Sense Multiple Access Protocols

This is where the sender listens before ejecting something on the wire. Collision occurs when a station hears something other than what it sent.

PERSISTENT AND NONPERSISTENT CSMA:

1-persistent CSMA

1-persistent CSMA is an aggressive transmission algorithm. When the sender (station) is ready to transmit data, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it senses the transmission medium continuously until it becomes idle, then transmits the message (a frame) unconditionally (i.e. with probability=1). In case of a collision, the sender waits for a random period of time and attempts to transmit again unconditionally (i.e. with probability=1). 1-persistent CSMA is used in CSMA/CD systems including Ethernet.

Station listens. If channel idle, it transmits. If collision, wait a random time and try again. If channel busy, wait until idle.

If station wants to send AND channel == idle then do send.

Success here depends on transmission time - how long after the channel is sensed as idle will it stay idle (there might in fact be someone else's request on the way.)

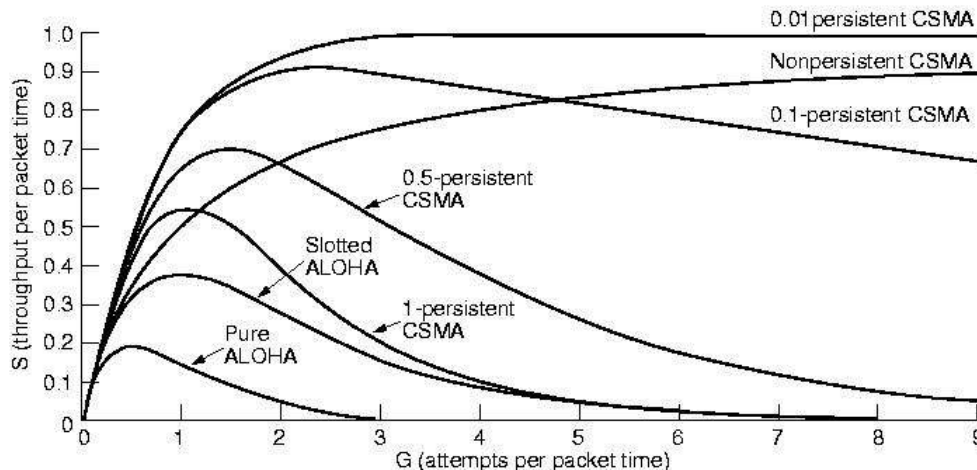
Nonpersistent CSMA (equivalent to 0-persistent CSMA)

Non persistent CSMA is a non aggressive transmission algorithm. When the sender (station) is ready to transmit data, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it waits for a random period of time (during which it does not sense the transmission medium) before repeating the whole logic cycle (which started with sensing the transmission medium for idle or busy) again. This approach reduces collision, results in overall higher medium throughput but with a penalty of longer initial delay compared to 1-persistent.

Same as above EXCEPT, when channel is found to be busy, don't keep monitoring to find the instant when it becomes free. Instead, wait a random time and then sense again.

Leads to

- 1) better utilization and
- 2) longer delays than 1 - persistent. (why?)



p-persistent CSMA [For slotted channels.]

This is an approach between 1-persistent and non-persistent CSMA access modes. When the sender (station) is ready to transmit data, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it senses the transmission medium continuously until it becomes idle, then transmits a frame with probability p . If the sender chooses not to transmit (the probability of this event is $1-p$), the sender waits until the next available time slot. If the transmission medium is still not busy, it transmits again with the same probability p . This probabilistic hold-off repeats until the frame is finally transmitted or when the medium is found to become busy again (i.e. some other sender has already started transmitting their data). In the latter case the sender repeats the whole logic cycle (which

started with sensing the transmission medium for idle or busy) again. p-persistent CSMA is used in CSMA/CA systems including Wi-Fi and other packet radio systems.

If ready to send AND channel == idle
then send with probability p,
and
with probability q = 1 - p defers to the next slot.

IEEE 802.3 and Ethernet

- Very popular LAN standard.
- Ethernet and IEEE 802.3 are distinct standards but as they are very similar to one another these words are used interchangeably.
- A standard for a 1-persistent CSMA/CD LAN.
- It covers the physical layer and MAC sublayer protocol.

Ethernet Cabling

Since the name “Ethernet” refers to the cable (the ether), five types of cabling are commonly used as shown in table in fig 2.6 The original wiring used for Ethernet is called ‘thicknet’ or 10 Base 5. The 5 stands for its maximum length: 500 meters (1650 feet) and 10 stands for 10Mbps (the speed at which it operates) The coaxial cable is marked every 205 meters called Vampire tap to connect the new connections to the thickened.

Name	Cable	Max, segment	Nodes/segments	Advantage
10 Base 5	Thick coax	500m	100	Good for backbone
10 Base 2	Thin coax	200m	30	Cheapest system
10 Base- T	Twisted pair	100m	1024	Easy maintenance
10 Base- FL	Fiber optic	2000m	1024	Best between buildings

The 10 Base T with hub arrangement is shown in figure.

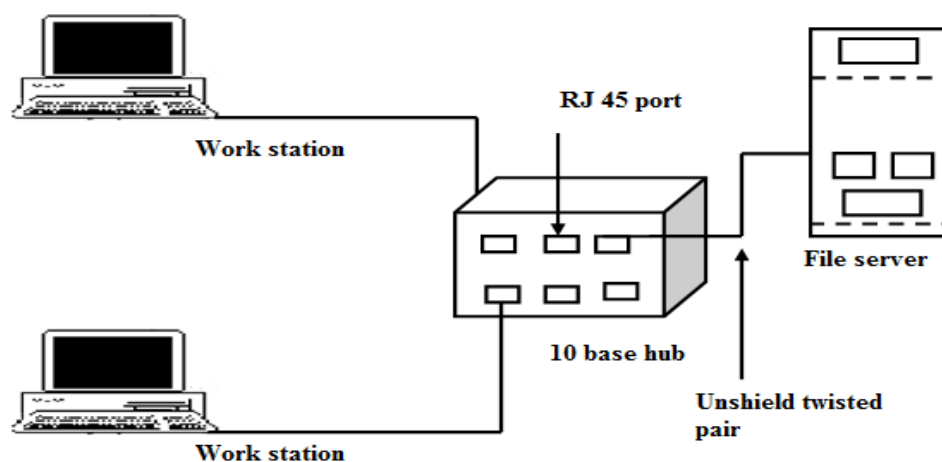
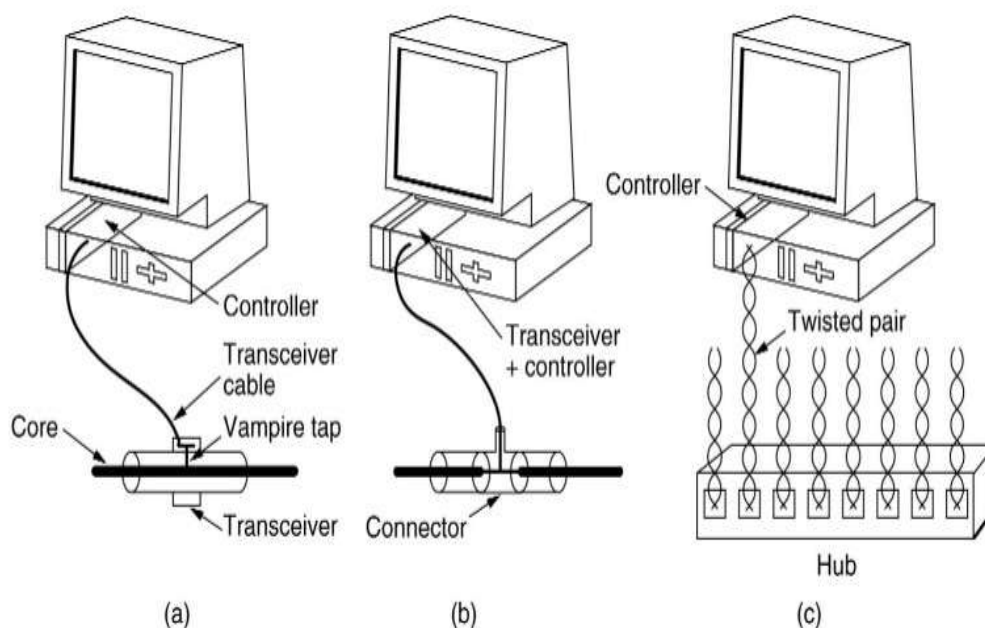


Figure: Hub arrangement

Ethernet Physical Layer

A Comparison of Various Ethernet and IEEE 802.3 Physical-Layer Specifications

Characteristic	Ethernet Value	IEEE 802.3 Values					
		10Base5	10Base2	10BaseT	10BaseF	10 Base -TX	100BaseT4
Data rate (Mbps)	10	10	10	10	10	100	100
Signaling method	Baseband	Baseband	Baseband	Baseband	Baseband	Baseband	Baseband
Maximum segment length (m)	500	500	185	100	2,000	100	100
Media	50-ohm coax (thick)	50-ohm coax (thick)	50-ohm coax (thin)	Unshielded twisted-pair cable	Fiber-optic	Cat 5 UTP	Unshielded twisted-pair cable
Nodes/segment	100	100	30	1024	1024		
Topology	Bus	Bus	Bus	Star	Point-to-point	Bus	Star



(a) 10Base5 (b) 10Base2 (c) 10Base-T

Note: To connect multiple segments, amplifier is not used because amplifier also amplifies the noise in the signal, whereas repeater regenerates signal after removing the noise.

IEEE 802.3 Frame Structure

Preamble (7 bytes)	Start of Frame Delimiter (1 byte)	Dest. Address (2/6 bytes)	Source Address (2/6 bytes)	Length (2 bytes)	802.2 Header+Data (46-1500 bytes)	Frame Checksum (4 bytes)
------------------------------	---	-------------------------------------	--------------------------------------	----------------------------	---	------------------------------------

A brief description of each of the fields

Preamble: Each frame starts with a preamble of 7 bytes, each byte containing the bit pattern 10101010. Manchester encoding is employed here and this enables the receiver's clock to synchronize with the sender's and initialize itself.

Start of Frame Delimiter: This field containing a byte sequence 10101011 denotes the start of the frame itself.

Dest. Address: The standard allows 2-byte and 6-byte addresses. Note that the 2-byte addresses are always local addresses while the 6-byte ones can be local or global.

2-Byte Address - Manually assigned address

Individual(0)/Group(1) (1 bit)	Address of the machine (15 bits)
--	--

6-Byte Address - Every Ethernet card with globally unique address

Individual(0)/Group(1) (1 bit)	Universal(0)/Local(1) (1 bit)	Address of the machine (46 bits)
--	---	--

Multicast: Sending to group of stations. This is ensured by setting the first bit in either 2-byte/6-byte addresses to 1.

Broadcast: Sending to all stations. This can be done by setting all bits in the address field to 1. All Ethernet cards (Nodes) are a member of this group.

Source Address: Refer to Dest. Address. Same holds true over here.

Length : The Length field tells how many bytes are present in the data field, from a minimum of 0 to a maximum of 1500.

The Data and padding together can be from 46 bytes to 1500 bytes as the valid frames must be at least 64 bytes long, thus if data is less than 46 bytes the amount of padding can be found out by length field.

Data : Actually this field can be split up into two parts - Data(0-1500 bytes) and Padding(0-46 bytes).

Reasons for having a minimum length frame:

To prevent a station from completing the transmission of a short frame before the first bit has even reached the far end of the cable, where it may collide with another frame. Note that the transmission time ought to be greater than twice the propagation time between two farthest nodes.

transmission time for frame > 2*propagation time between two farthest nodes

When a transceiver detects a collision, it truncates the current frame, which implies that stray bits and pieces of frames appear on the cable all the time. Hence to distinguish between valid frames from garbage, 802.3 states that the minimum length of valid frames ought to be 64 bytes (from Dest. Address to Frame Checksum).

Frame Checksum : It is a 32-bit hash code of the data. If some bits are erroneously received by the destination (due to noise on the cable), the checksum computed by the destination wouldn't match with the checksum sent and therefore the error will be detected. The checksum algorithm is a cyclic redundancy checksum (CRC) kind. The checksum includes the packet from Dest. Address to Data field.

Ethernet Frame Structure

Preamble (8 bytes)	Dest. Address (2/6 bytes)	Source Address (2/6 bytes)	Type (2 bytes)	Data (46-1500 bytes)	Frame Checksum (4 bytes)
------------------------------	-------------------------------------	--------------------------------------	--------------------------	--------------------------------	------------------------------------

A brief description of the fields which differ from IEEE 802.3

Preamble : The *Preamble* and *Start of Frame Delimiter* are merged into one in Ethernet standard. However, the contents of the first 8 bytes remains the same in both.

Type : The length field of IEEE 802.3 is replaced by Type field, which denotes the type of packet being sent viz. IP, ARP, RARP, etc. If the field indicates a value less than 1500 bytes then it is length field of 802.3 else it is the type field of Ethernet packet.

Truncated Binary Exponential Back off

In case of collision the node transmitting backs off by a random number of slots, each slot time being equal to transmission time of 512 bits (64 Byte- minimum size of a packet) in the following fashion:

<u>No of Collision</u>	<u>Random No of slots</u>
1st	0-1
2nd	0-3
3rd	0-7
10th	0-1023

11th	0-1023
12th	0-1023
16th	0-1023

In general after i collisions a random number between $0-2^i-1$ is chosen , and that number of slots is skipped.

However, after 10 collisions have been reached the randomization interval is frozen at maximum of 1023 slots.

After 16 collisions the controller reports failure back to the computer.

5-4-3 Rule

Each version of 802.3 has a maximum cable length per segment because long propagation time leads to difficulty in collision detection. To compensate for this the transmission time has to be increased which can be achieved by slowing down the transmission rate or increasing the packet size, neither of which is desirable. Hence to allow for large networks, multiple cables are connected via **repeaters**. Between any two nodes on an Ethernet network, there can be at most five segments, four repeaters and three populated segments (non-populated segments are those which do not have any machine connected between the two repeaters). This is known as the **5-4-3 Rule**.

Manchester Encoding

With Manchester encoding, each bit period is divided into equal intervals a binary 1 is sent by having voltage set high during the first interval and low during the second one. A binary 0 is just the reverse: first low and then high, this scheme ensures that every bit period has a transition in the middle, making it easy for the receiver to synchronise with the sender.

A disadvantage of the Manchester encoding is that it requires twice as much bandwidth as straight binary encoding, because the pulses are half the bandwidth. Manchester coding is shown in fig. 2.8

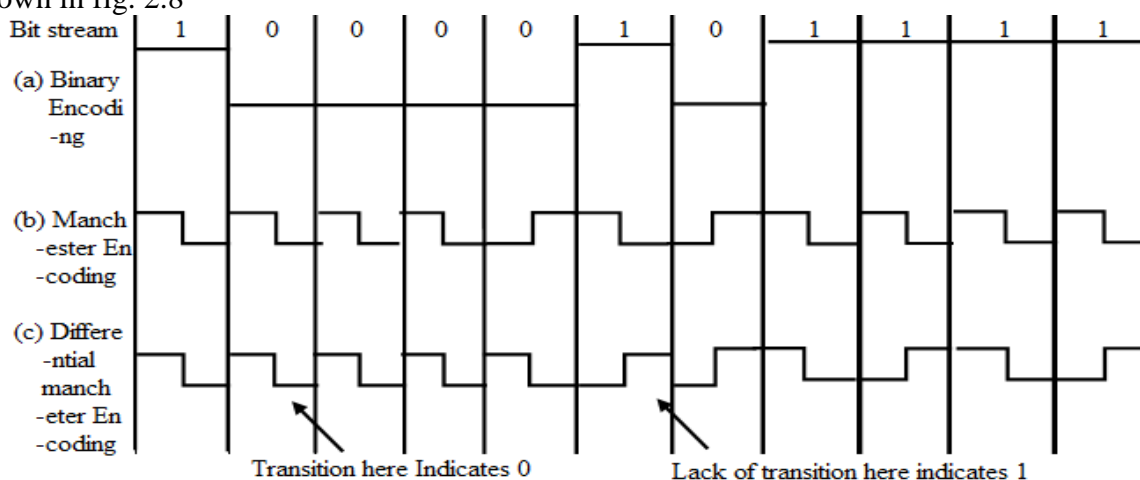


Fig. 2.8 (a) binary encoding. (b) Manchester encoding. (c) Differential Manchester encoding

Differential Manchester encoding, shown in fig is a variant of the basic Manchester encoding. In it a 1 bit is indicated by absence of transmission at the start of interval. A 0 bit is indicated by presence of transition at the start of interval. In both cases there is transition in middle as well.

The differential scheme requires more complex equipment but offers better noise immunity. All 802.3 base band system use Manchester encoding due to its simplicity.

The high signal is +0.85 volts and low signal is -8.85 volts, giving a DC value of 0 volts.

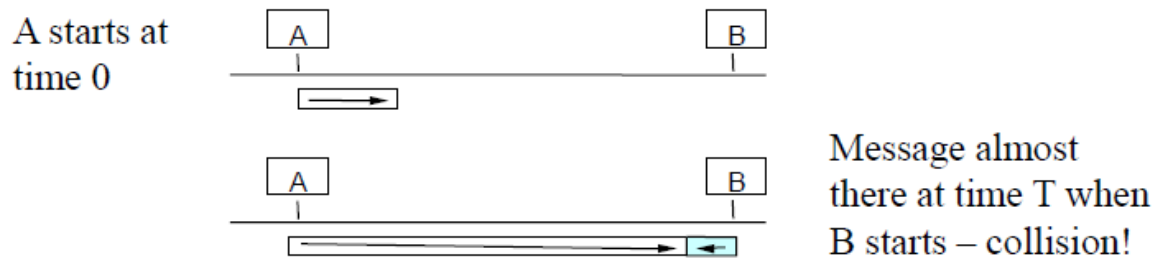
Carrier Sense Multiple Access Protocols with Collision Detection

In Aloha, decisions to transmit are made without paying attention to what other nodes might be doing

- Ethernet uses CSMA/CD –listens to line before/during sending
- If line is idle (no carrier sensed)
 - send packet immediately
 - upper bound message size of 1500 bytes
 - must wait 9.6μs between back-to-back frames
- If line is busy (carrier sensed)
 - wait until idle and transmit packet immediately
- called *1-persistent* sending
- If collision detected
 - Stop sending and jam signal
 - Try again later

Collisions are caused when two adaptors transmit at the same time (adaptors sense collision based on voltage differences)

- Both found line to be idle
- Both had been waiting to for a busy line to become idle



How can we be sure A knows about the collision?

How can A know that a collision has taken place?

- There must be a mechanism to insure retransmission on collision
- A's message reaches B at time T
- B's message reaches A at time $2T$
- So, A must still be transmitting at $2T$

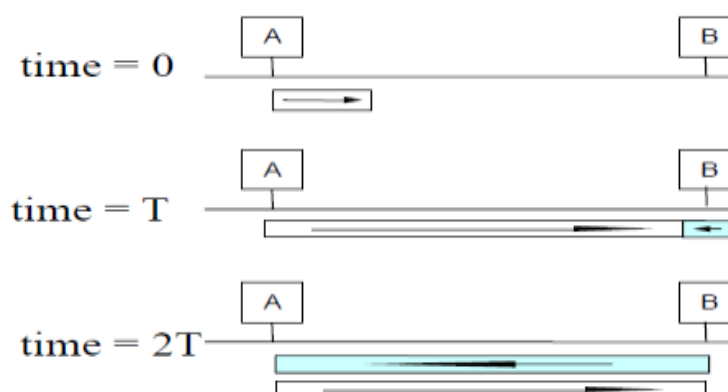
- IEEE 802.3 specifies max value of $2T$ to be 51.2us

- This relates to maximum distance of 2500m between hosts
- At 10Mbps it takes 0.1us to transmit one bit so 512 bits (64B) take 51.2us to send
- So, Ethernet frames must be at least 64B long

- 14B header, 46B data, 4B CRC

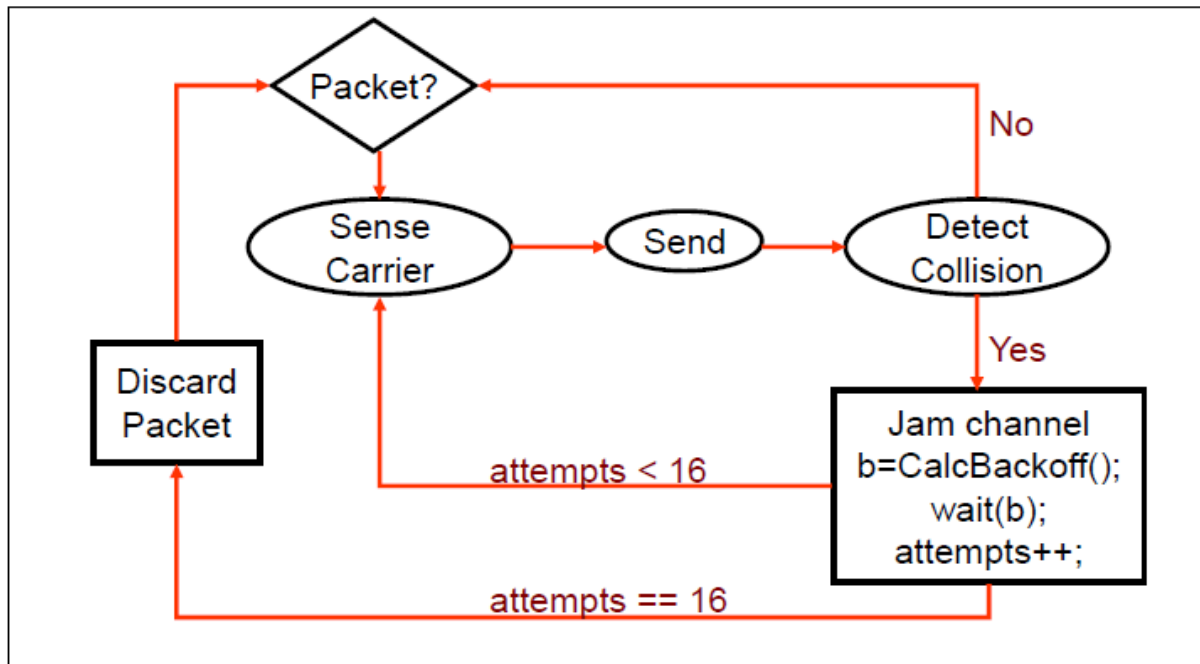
- Padding is used if data is less than 46B

- Send jamming signal after collision is detected to insure all hosts see collision–48 bit signal



Jam Signal: make sure all other transmitters are aware of collision; 48 bits;

Exponential Backoff:



If a collision is detected, delay and try again

Delay time is selected using binary exponential backoff

- 1st time: choose K from $\{0, 1\}$ then delay = $K * 51.2 \text{ us}$
- 2nd time: choose K from $\{0, 1, 2, 3\}$ then delay = $K * 51.2 \text{ us}$
- n th time: delay = $K * 51.2 \text{ us}$, for $K=0..2^{n-1}$

- Note max value for $k = 1023$
 - give up after several tries (usually 16)

- Report transmit error to host

If delay were not random, then there is a chance that sources would retransmit in lock step

- Why not just choose from small set for K
 - This works fine for a small number of hosts
 - Large number of nodes would result in more collisions

Slotted Aloha Efficiency

Question: What are max fraction slots successful?

Answer: Suppose N stations have packets to send

- Each transmits in slot with probability p
- Prob. successful transmission S is:

by single node:

$$S = p (1-p)^{(N-1)}$$

by any of N nodes

$$\begin{aligned} S &= \text{Prob (only one transmits)} \\ &= N p (1-p)^{(N-1)} \end{aligned}$$

$$\text{Probability of success } p = N p (1-p)^{N-1}$$

$$\text{Max}(p) \text{ ie } d/dp=0$$

$$\begin{aligned} d/dp(N p (1-p)^{N-1}) &= N[p d/dp (1-p)^{N-1} + (1-p)^{N-1} dp/dp] \\ &= N [p (N-1) (1-p)^{N-2}(-1) + (1-p)^{N-1}] \\ &= N (1-p)^{N-1} - N p (N-1) (1-p)^{N-2} \end{aligned}$$

Then

$$P = 1 / N$$

Which means at $p = 1/N$, We get maximum p .

$$p_{\max} = N \times 1/N \times (1-1/N)^{N-1}$$

$$\begin{aligned} \lim_{N \rightarrow \infty} p_{\max} &= \lim_{N \rightarrow \infty} (1-1/N)^{N-1} \\ &= 1/e \end{aligned}$$

Then min of tries before the first success = $1 / (1/e) = e$

Therefore number of contention slot = e

... choosing optimum p as $N \rightarrow \infty$...

$$\dots p = 1/N$$

$$= 1/e = .37 \text{ as } N \rightarrow \infty$$

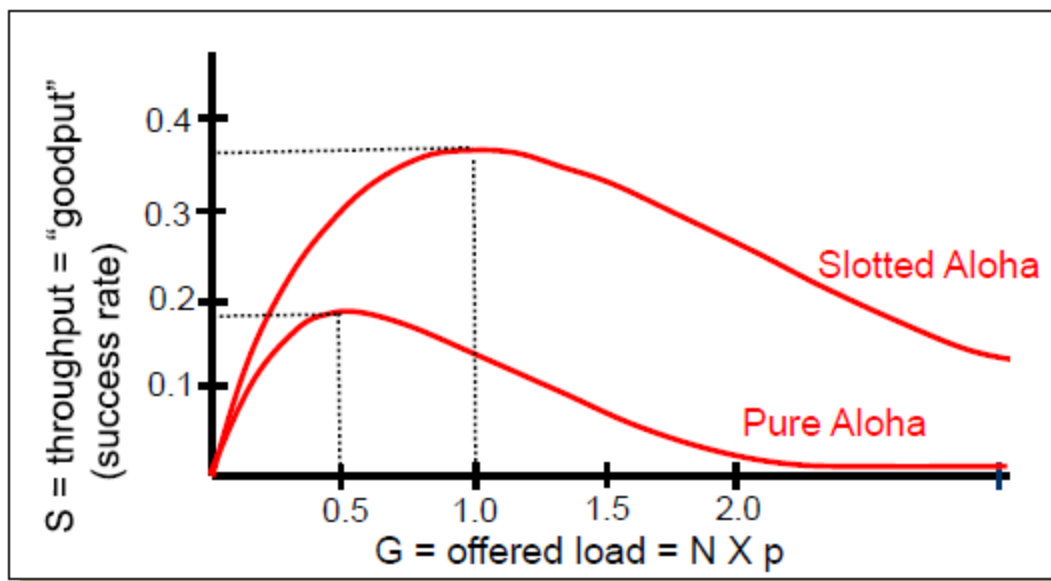
NOTE: At best: channel use for useful transmissions 37% of time!

Pure Aloha

$$P(\text{success by given node}) = P(\text{node transmits}) \times P(\text{no other node transmits in } [p_0-1, p_0]) \times P(\text{no other node transmits in } [p_0+1, p_0+1]) = p \times (1-p)^{(N-1)} \times (1-p)^{(N-1)}$$

$$P(\text{success by any of N nodes}) = N p \times (1-p)^{(N-1)} \times (1-p)^{(N-1)} = 1/(2e) = .18$$

... choosing optimum p as $N \rightarrow \infty \rightarrow p = 1/2N$...



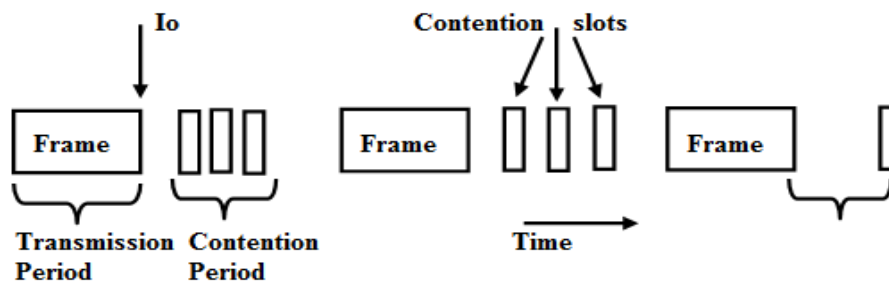
Ethernet Problems

- Ethernet's peak utilization is pretty low (like Aloha)
- Peak throughput worst with
 - More hosts
- More collisions needed to identify single sender
 - Smaller packet sizes
- More frequent arbitration
 - Longer links
- Collisions take longer to observe, more wasted bandwidth
 - Efficiency is improved by avoiding these conditions

Why did Ethernet Win?

- There are LOTS of LAN protocols
- Price
- Performance
- Availability
- Ease of use
- Scalability

Ethernet Efficiency:



The actual formula for efficiency of ethernet is $1 / (1 + 6.44 a)$

Where $a = T_p / T_t$

Efficiency = $T_t / \text{Total cycle time}$

$$\begin{aligned}
 \text{Total Cycle time} &= \text{Transmission Time} + \text{Contention Time or Collision Period} + \text{Propagation delay} \\
 &= T_t + 2 e T_p + T_p \\
 &= T_t + (1 + 2 e) T_p \\
 &= T_t + (1 + 6.44) T_p
 \end{aligned}$$

If we are considering T_p in total cycle time then we get $1 / (1 + 5.44 a)$

Collision free protocols

Still with CSMA/CD the collisions are possible. For reliable and better performance we need absolutely collision free protocols. Some of them are discussed below:

(A) A Bit Map Protocol: In basic bit map method, each contention period consists of exactly N slots, of station 0 has the frame to send, it transmits the 1 bit during the zeros slot. No other station is allowed to transmit during this slot. After the station 0 the station 1 gets the opportunity to transmit during slot 1. In general the station j may, tells priory that it has the frame to send, by inserting the slots 1 bit into slot j . after all N slots have passed by, each station has complete knowledge of which station wish to transmit. At that point they begins transmitting in numerical order.

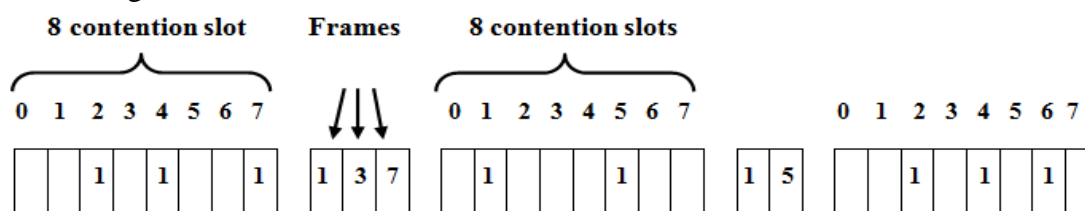


Figure: The basic bit map protocol

Since everyone agrees on who goes next, there will be no collision. Because of its nature of working it is sometime called as reservation protocols,

(B) Binary countdown: A problem with the basic bitmap protocol is that the overhead is one bit per station. We can achieve collision free environment by binary station, starting with the high order bit. All addresses are assumed to of same length. The bits in each address position

from different station are BOOLEAN Oared. Together, we will call this protocol as binary countdown.

To avoid conflicts, an arbitration rule must be applied: as soon as station sees that a high order bit position that is zero in its address has been overwrite with a 1. it gives up. For e.g. if station 0010, 0100, 1001, and 1010 are all trying to get the channel, in the first bit time the station transmits 1, 0, 1 and 1010 continue.

The next bit is o, and both stations continue, the next bit is 1, so station 1001 gives up. The winner is 1010, because it has highest address. After winning it may now transmit a frame, after which another bidding cycle starts. The protocol is illustrated in below figure.

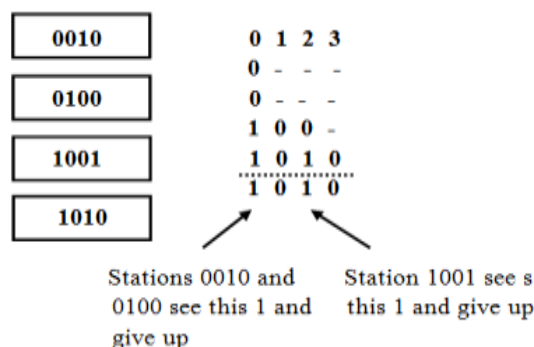


Figure: The binary countdown a dash indicates silence.

Few points to be noted:

1. Ethernet uses CSMA / CD as access methods (No Ack) and uses Manchester encoding due to its simplicity. The minimum length of the frame is 72 bytes or 64 bytes from D.A. Minimum data will be 46 byte always. This is because of two reasons
 - a) When the sender detects a collision, it truncates the current frame, so strays bits and pieces of frame appear on the cable, so to distinguish valid frames from garbage's, we will maintain minimum number of bytes.
 - b) To find out collision.
2. 10 Mbps Ethernet operates up to 2500 mtrs, 100 Mbps Ethernet operates up to 250 mtrs, 1 Gbps Ethernet operates up to 25 mtrs only. But 25 mtrs is not acceptable, so two features are added to 1Gbps line, they are
 - a) Carrier extension – Hardware will add its own padding
 - b) Frame bursting- Allows the sender to transmit a concatenated sequence of multiple frames in a single transmissions.
3. Preamble of 7 bytes containing the bit pattern 10101010to allow the receiver's clock to synchronize with sender's clock.
4. The lower and upper limits of the data in 802.3 are 46 B to 1500 B. The lower limit is to make sure the collision techniques work properly. The upper limit is used to prevent one transmission from monopolizing the medium for too long.

5. Ethernet adaptor normally retry up to 16 times, though N is limited to 10, then gives up and reports a transmit error to the host.

IEEE 802.4 Standard Token Bus

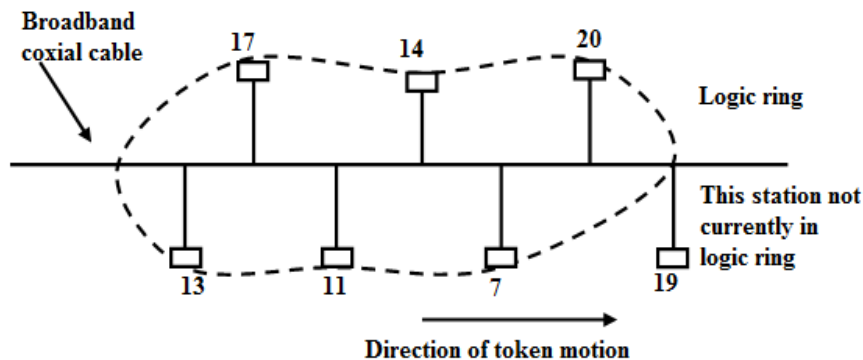


Figure: A Token ring

This standard, 802.4 describes a LAN called a Token bus. A linear or tree-shaped cable into which a station are attached.

Logically, the stations are organized into a ring (see fig 2.9), with each station knowing the address of the station to its “left” or “right”

When the logical ring is initialized, the highest numbered station may send the first frame, after it is done, it passes permission to its immediate neighbour by sending the neighbour a special control frame called ‘token’. The token propagates around the logical ring, with only the token holder being permitted to transmit frames.

Since only one station at a time holds a token, collision do not occur.

An important point to realize is that the physical order in which the stations are connected to the cable is not important. Since the cable is inherently a broadcast medium, each station receives each frame, discarding those not addressed to it.

2.5.1 The Token bus MAC sublayer protocol

The Token Bus format is shown in fig 2.10. The preamble is used to synchronize the receiver clock, as in 802.3, except that here it may be as short as 1 byte. The starting and ending delimiter fields are used to make the frame boundaries. Both of these fields contain analog encoding of symbols other than 0’s and 1’s, so that they cannot occur accidentally in the user data. As result, no length field is needed.

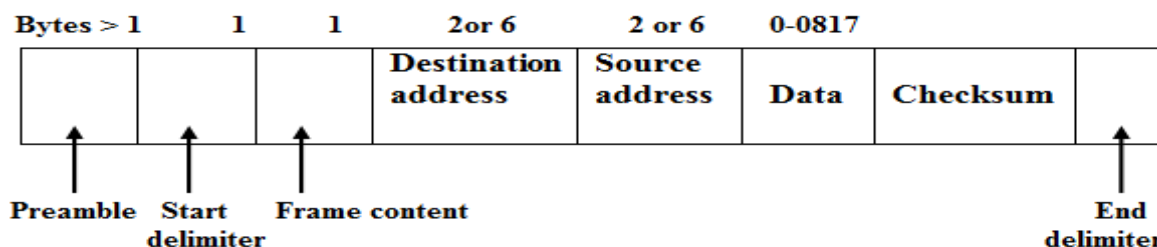


Fig. 2.10 The 802.4 frame format

The ‘frame control’ field is used to distinguish data from control frames. The destination address and source address field are same as 802.3. The data field may be upto 8192 bytes long, when 8-byte addresses are used. The checksum is used to detect transmission errors.

2.6 IEEE Standard 802.5 token ring

Token ring was developed by IBM as a robust, highly reliable network. It is more complex than Ethernet since it has self healing properties.

A ring really consists of collection of ring interfaces. Connected by point to point lines. Each bit arriving at interfaces is copied into a 1 bit buffer and then copied out onto the ring again. When in the buffer, the bit can be inspected and possibly modified before being writing out. This coping step introduces a 1 bit delay. At each interface. A ring and its interfaces are shown in fig 2.11.

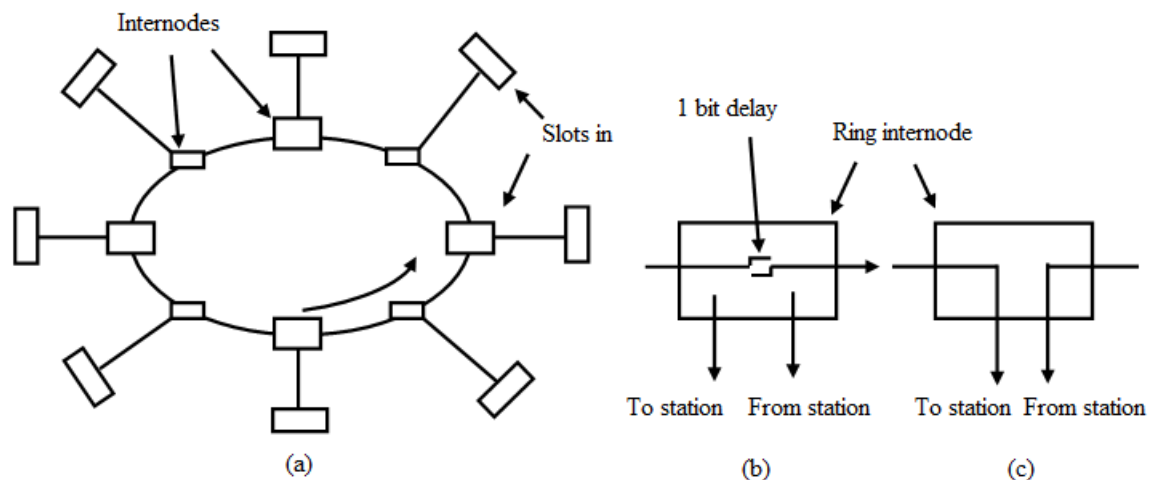


Fig 2.11 (a) Ring network (b) Listen mode (c) Transmit mode

In a token ring a special bit pattern, called a token, circulated around the ring whenever all station are idle. When station wants to transmit the frame, it is required to seize the token and remove it from the ring before transmitting. This action is done by inverting a single bit (i.e. of taken), in the 3 byte token, only one station can transmit at the given instant, thus solving the channel access problem the same way the token bus solves it. Ring interfaces have two operating modes, listen and transmit, in listen mode the input bits are simply copied into output, with a delay of 1 bit time, as shown in fig2.11 (b). In a transmit mode; Which is entered only after token has been seized, the interface breaks the connection between input and output, entering its own data the ring. To be able to switch from listen to transmit mode in 1 bit time, the interfaces usually needs to buffer one or more frames itself rather than having to fetch them from station on such short notice.

As bits that propagated amount the ring comes back, they are removed from the ring by the sender. The sending station can either save them, to compare with the original data to monitor ring reliability, or discard them. Because entire frame never appears on the ring at one instant, this ring architecture puts no limits on the size of frames, After a station has finished transmitting the last bit of its last frame, it must regenerate the token.

When traffic is light, the token ring will spend most of its time ideally circulating around the ring. Occasionally a station will size it, transmit the frame and then out put a new token. However, when the traffic is heavy, so that there is queue at the station, downstream will see and remove the token, the next station smoothly around the ring, in round fashion. The network sufficiency can begin to approach 100 percent under condition of heavy loads.

One problem with the ring network is that if the cable break somewhere, the ring dies. This problem can be solved elegantly by the use of 'wire center' as shown in figure 2.12 while logically still a ring. Physically each station is connected to a wire centred by a cable containing (at least) two twisted pairs, one of the station and one for data from station.

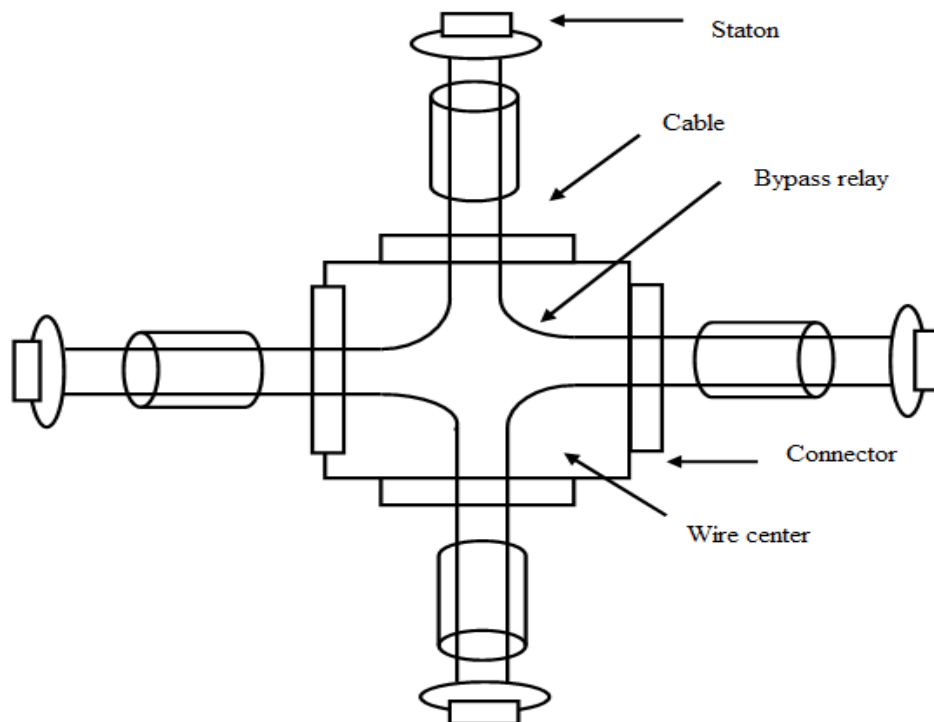


Fig 2.12 four stations connected via a wire centre

Inside the wire centre are bypass relays that are energized by current from the station. If the ring breaks or station goes down, loss of the device current will release the relay and bypass the station. The relay can also be operated by software to permit diagnostic programs to remove station one at a time to find faulty station and ring segments. The ring can then continue operating with the bad segment bypassed. Although the 802.5 standards does not formally require this kind of ring, often called a star shaped ring most 802.5 LANs, in fact, do use wire centre to improve their reliability and maintainability.

2.6.1 The Token ring MAC sublayer Protocol

The basic operation of MAC protocol is no traffic on the ring; a 3-byte token circulates endlessly, waiting for a station to seize it by setting a specific 0 bit to a 1 bit, thus converting the token into start of the frame sequence. The station then output the rest of normal data frames, as shown in fig 2.13.

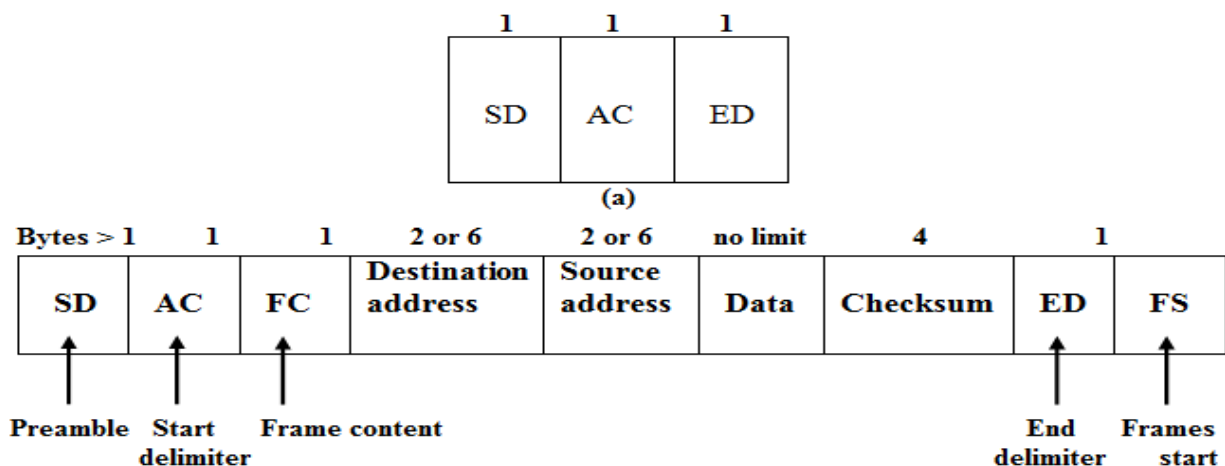


Fig. 2.13 (a) Token format (b) Data frame format

The starting and ending delimiter fields mark the starting and ending of the frames. The access control byte contains the token bit, and also the monitor bit, priority bit, and Reservation bits and frame control byte distinguishes data frame from various possible control frames.

Next comes the Destination and source address fields, which are the same as in 802.3 and 802.4. The checksum field is also same as 802.3 and 802.4.

An interesting bytes not present in the other two protocols is the **frame status byte**. It contains the A and C bits.

When frames arrives at the interface of the destination address, the interface turns on a A bit as it passes through. If the interface copies the frame to the station it also turns on the C bit. A station might fail to copy frame due to lack of buffer space or other reasons.

When the sending station drains the frame the ring it examines the A and C bits. Three combinations are possible:

1. A=0 and C=0 : destination not present or not powered up.
2. A=1 and C=0 : destination presents no frame not accepted.
3. A=1 and C=1 : destination present and no frame copied.

This arrangement provides an automatic acknowledgement for each frame. The ending delimiter contains an E bit which is set if any interface detects the error. It also contains the bit that can be used to make the last frame in a logical sequence, sort of like an end of file bit.

Assignment:

1. On a CSMA/CD network, computer A has an inter frame spacing of two slots, computer B's inter frame spacing is six slots and the inter spacing for computer C is four slots. Which device has the highest priority?
(A) Computer A (C) Computer C
(B) Computer B (D) Priority cannot assigned in CSMA/CD
2. Throughput of pure ALOHA is?
(A) 15% (C) 20%
(B) 15% (D) 36%
3. Throughput of slotted ALOHA is?
(A) 15% (C) 20%
(B) 18% (D) 36%
4. Calculate the time required to transfer a 1000 KB file, assuming an RTT of 100ms, a packet size of 1 kb data with an initial $2 \times \text{RTT}$ of handshaking when the bandwidth is 1.5 Mbps and the data is sent continuously.
(A) 5.46 sec (C) 20 sec
(B) 50 sec (D) 4.29 sec
5. Calculated the time required to transfer a 1000 KB file, assuming an RTT of 100 ms, a packet size of 1 kb data with an initial $2 \times \text{RTT}$ of handshaking, when the bandwidth is 1.5 Kbps and the data is sent continuously. However, after sending each data packet, one has to wait for 1 RTT before sending the next.
(A) 105 sec (C) 100 sec
(B) 105.66 sec (D) 108.29 sec
6. We want to send a 1000 KB file ($K = 1000$, and B is Byte) in 1 KB packets. The distance is 10 Km and the signal propagation speed is 2×10^5 km/sec. The bandwidth is 1.5 Mb/sec. (note $M = 1,000,000$.) How long will it take to send the file?
(A) 5 sec (C) 2 sec

- (B) 4 sec (D) 5.333 sec
7. An ATM network uses a token bucket scheme for traffic shaping. A new token reaches the bucket every 5 μ second. Calculate the maximum data rate which is sustainable.
(A) 76.8 Mbps (C) 20 Mbps
(B) 48 Mbps (D) 75 Mbps
8. A 100 Mbps delayed release token ring has 10 stations. A ring latency of 30 seconds. The TTRT is set to 350 μ seconds. Calculate the total number of synchronous frame bytes each station can send assuming that all are allotted the same amount.
(A) 200 bytes (C) 400 bytes
(B) 256 bytes (D) None
9. In Ethernet, MAC sub-layer uses access method
(A) ALOHA (C) Slotted CSMA
(B) CSMA/CD (D) None
10. 10 base-FL Ethernet uses
(A) Twisted pair cable (C) Wired cable
(B) Fiber cable (D) None
11. If stations are there and if each slot contains 25 μ s then what would be the max waiting time for a station for safe transmission
(A) 200 (C) 250
(B) 500 (D) 400
12. For Manchester coding scheme to send data at 10 Mbps the signal has to change
(A) 10 million time/sec (C) 30 million time/sec
(B) 20 million time/sec (D) 5 million time/sec
13. Which of the following Ethernet standard run over coaxial cabling
(A) 10 Base T (C) 1000 Base SX
(B) 10 Base 2 (D) 10 Base 5T
14. 10 Base-T refer to
(A) Ethernet using thin coaxial cable
(B) Ethernet using thick coaxial cable
(C) Ethernet using unshielded twisted pair cabling
(D) None of the above
15. 10-Base-5 refer to
(A) Ethernet using thin coaxial cable
(B) Ethernet using thick coaxial cable
(C) Ethernet using unshielded twisted pair cabling
(D) None of the above
-

16. 10-Base T network typically uses
- (A) CSMA/CA and coaxial cable
 - (B) CSMA/CD and UTP cable
 - (C) CSMA/CD and infrared transmission
 - (D) CSMA/CA and radio signals
17. In a Token ring MAC frame the RIF route control field contains the following information
- (A) MAC Address
 - (B) Ring number
 - (C) Bridge number
 - (D) Length of RIF

GATE Questions CS:

1. A computer on a 10Mbps network is regulated by a token but the bucket is filled at a rate of 2Mbps. If it is initially filled capacity. With 16 megabits. What is the maximum for the computer can transmit at the full 10Mbps?
- (A) 1.6 seconds
 - (B) 2 seconds
 - (C) 5 seconds
 - (D) 8 seconds
- [GATE-CS-2008]**
2. In a token network the transmission speed is 10 bps & the propagation speed is 200 meters/ms. The 1-bit delay in this network is equivalent to:
- (A) 500 meters of cable
 - (B) 200 meters of cable
 - (C) 20 meters of cable
 - (D) 50 meters of cable
- [GATE-CS-2007]**
3. There are n stations in a slotted LAN. Each station attempts to transmit with a probability p in each time slot. What is the probability that ONLY one station transmits in a given time slot?
- (A) $np(1-p)^{n-1}$
 - (B) $(1-p)^{n-1}$
 - (C) $p(1-p)^{n-1}$
 - (D) $1 - (1-p)^{n-1}$
- [GATE-CS-2007]**
4. In Ethernet when Manchester encoding is used the bit rate is
- (A) Half the baud rate
 - (B) Twice the baud rate
 - (C) Same as the baud rate
 - (D) None of these
- [GATE-CS-2007]**
5. A and B are the only two stations on an Ethernet. Each has a steady queue of frames to send. Both A and B attempt to transmit a frame, collide, and A wins the first back off race. At the end of this successful transmission by A, both A and B attempt to transmit and collide. The probability that A wins the second back off race is
- (A) 0.5
 - (B) 0.625
 - (C) 0.75
 - (D) 1.0
- [GATE-CS-2004]**
6. Host A is sending data to host B over a full duplex link. A and B are using the sliding window protocol for flow control. The send and receive window size are 5 packets each.

Data packets (sent only from A to B) are all 1000 bytes long and the transmission time for such a packet is 50 μ s. Acknowledgement packets the link is 200 μ s. What is the maximum achievable throughput in this communication?

- (A) 7.60×10^6 bps (C) 12.33×10^6 bps
(B) 11.11×10^6 bps (D) 12.00×10^6 bps

[GATE-CS-2003]

7. A 2 km long broadcast LAN has 10^7 bps bandwidth and uses CSMA/CD. The signal travels along the wire at 2×10^8 m/s. What is the minimum packet size that can be used on this network?

- (A) 50 bytes (C) 200 bytes
(B) 100 bytes (D) None of the above

[GATE-CS-2003]

GATE Questions IT:

1. The minimum frame size required for CSMA/CD based computer network running at 1.Gbps on a 200m cable with a link speed of 2×10^8 m/s is

- (A) 125 bytes (C) 240 bytes
(B) 250 bytes (D) None of the above

[GATE-IT-2008]

Common Data Questions 2 & 3:

Consider a token ring topology with N stations (numbered 1 to N) running token ring protocol where the stations are equally spaced. When a station gets the token it is to send one frame of fixed size. Ring latency is t_p . All other latencies can be neglected.

2. The maximum utilization of the token ring when $t_t = 3$, $t_p = 5$ ms, $N = 10$ is

- (A) 0.545 (C) 0.857
(B) 0.6 (D) 0.961

[GATE-IT-2007]

3. The maximum utilization of the token ring when $t_t = 5$ ms, $t_p = 3$ ms, $N = 15$ is

- (A) 0.545 (C) 0.9375
(B) 0.655 (D) 0.961

[GATE-IT-2007]

4. A broadcast channel has 10 nodes and total capacity of 10 Mbps. It uses polling for medium access. Once a node finishes transmission, there is a polling delay of 80 μ s to poll the next node. Whenever a node is polled, it is allowed to transmit a maximum of 1000 bytes. The maximum throughput of the broadcast channel is

- (A) 1 Mbps (C) 10 Mbps
(B) 100/11 Mbps (D) 100 Mbps

[GATE-IT-2007]

5. In a TDM medium access control bus LAN, each station is assigned one time slot per cycle for transmission. Assume that the length of each time slot is time to transmit 100 bits plus the end-to-end propagation delay. Assume a propagation speed of 2×10^8 m/sec. The length of the LAN is 1 km with a throughput of each station can be 2/3 Mbps is:

- (A) 3 (C) 10
(B) 5 (D) 20

[GATE-IT-2005]

6. A channel has a bit rate of 4 kbps and one-way propagation delay of 20 ms. The channel uses stop and wait protocol. The transmission time of the acknowledgement frame is negligible. To get a channel efficiency is at least 50%, the minimum frame size should be
- (A) 80 bytes (C) 160 bytes
(B) 80 bits (D) 160 bits

[GATE-IT-2005]

7. A network with CSMA/CD protocol in the MAC layer is running at 1 Gbps over a 1 km cable with no repeaters. The signal speed in the cable is 2×10^8 m/sec. The minimum frame size for this network should be
- (A) 10000 bits (C) 5000 bits
(B) 10000 bytes (D) 5000 Bytes

[GATE-IT-2005]

8. Which of the following statements is TRUE about CSMA/CD
- (A) IEEE 802.11 wireless LAN runs CSMA/CD protocol
(B) Ethernet is not based on CSMA/CD protocol
(C) CSMA/CD is not suitable for a high propagation delay network like satellite network
(D) There is no contention in a CSMA/CD network

[GATE-IT-2005]

9. Consider a simplified time slotted MAC protocol where each host always has data to send and transmit with probability $p = 0.2$ in every slot. There is no back off and frame can be transmitted in one slot. If more than one host transmit in the same slot, then the transmission are unsuccessful due to collision, what is the maximum number of hosts which this protocol can support, if each hosts has to be provided a minimum throughput of 0.16 frames per time slots?
- (A) 1 (C) 3
(B) 2 (D) 4

[GATE-IT-2004]

10. Consider a 10 Mbps token ring LAN with a ring latency of 400 μ s. A host that needs to transmit seizes the token. Then it sends a frame of 1000 bytes, removes the frame after it has circulated all around the ring, and finally releases the token. This process is repeated for every frame. Assuming that only a single host wishes to transmit, the effective data rate is
- (A) 1 Mbps (C) 5 Mbps
(B) 2 Mbps (D) 6 Mbps

[GATE-IT-2004]

11. A host is connected to a department network which is a part of university network. The university network, in turn, is part of the internet. The largest network in which the Ethernet address of the host is unique is
- (A) The subnet to which the host belongs
(B) The department network
(C) The university network
(D) The internet

[GATE-IT-2004]

Answer keys

Assignment:

1	A	2	B	3	D	4	A	5	B	6	D	7	A	8	C	9	B	10	B
11	B	12	B	13	B	14	C	15	B	16	B	17	D						

GATE Questions CS:

1	B	2	C	3	A	4	B	5	B	6	B	7	D
---	---	---	---	---	---	---	---	---	---	---	---	---	---

GATE Questions IT:

1	B	2	C	3	A	4	B	5	C	6	B	7	A	8	C	9	B	10	D
11	A																		

Explanations:

Assignment:

1. [Ans. A]

Computer A, smaller the interface, higher the priority.

2. [Ans. B]

Throughput of pure ALOHA = $18\% = G e^{-2G}$. $G = .5 \frac{1}{2e} = .184 = 18\%$

3. [Ans. D]

Throughput of slotted ALOHA = $36\% = G e^{-G}$, $G = 1, \frac{1}{e} = .368 = 36\%$

4. [Ans. A]

Given Data

Initial delay = 2 RTT = 200 ms

Propagation Time = 0.5 RTT = 50 ms

Transmit Time = $\frac{(1000 \times 1024 \times 8 \text{ bits})}{(1.5 \times 10^6)}$ bits/sec
 = 5.46 secs

5. [Ans. B]

For each data packet,

Transmit Time = $\frac{(1000 \times 1024 \times 8 \text{ bits})}{(1.5 \times 10^6)}$ bits/sec
 5.46 secs

Waiting Time = 1 RTT = 100 ms

Total time = 105.46 ms

Time for 1000 packets = 105.46 secs

Adding initial handshake time, total time = 105.66 secs

6. [Ans. D]

We are sending packets continuously. In real life an ACK (acknowledgement) is usually involved but we aren't using ACK, so the total time will be 1 propagation delay + transmission time for 1000 KB. Propagation delay is

$$\frac{10 \text{ km}}{2 \times 10^5 \text{ km/sec}} = 5 \times 10^{-5} \text{ sec.}$$

Transmission time is (KB = 8000b)

$$\frac{8 \times 10^6 \text{ kb}}{1.5 \times 10^6 \text{ b}} = 5.33333 \text{ sec}$$

Total time is $5.33333 + .00005 = 5.33338 \text{ sec}$. In effect, propagation delay is negligible here.

7. [Ans. A]

A token is generated every 5 μ seconds. Then a total of 200,000 cells can be forwarded. The ATM frame has a cell which holds 48 data bytes. Hence, the net data rate is 76.8 Mbps.

8. [Ans. C]

$TTRT = n \times THT + \text{Ring Latency}$

$$350 = 10 \times THT + 30 \text{ which gives } THT = 32$$

This means a station can transmit $3200 \text{ bps} = 400 \text{ bytes of synchronous data}$

9. [Ans. B]

MAC sub-layer uses CSMA/CD access method.

10. [Ans. B]

Fiber cable

11. [Ans. B]

As station waits max of 25 slot time so $25 \times 25 \mu\text{s} = \text{waiting time}$.

12. [Ans. B]

$$\begin{aligned} \text{No. of times signal has to change} &= 2 \times \text{data rate} \\ &= 2 \times 10 \text{ Mbps} = 20 \text{ million times/sec} \end{aligned}$$

13. [Ans. B]

10 Base 2 run over coaxial cable

14. [Ans. C]

10-Base-T refers to Ethernet using unshielded twisted pair cabling.

15. [Ans. B]

10-Base-5 refers to Ethernet using thick coaxial cable.

16. [Ans. B]

It uses CSMA/CD and UTP cable.

17. [Ans. D]

It contains RIF length information.

GATE Question CS:

1. [Ans. B]

Data transfer rate of token = 10Mbps initially filled to capacity 16 Megabits

$$\begin{aligned} & \frac{16}{10} + \frac{16}{10} \times \frac{2}{10} + \frac{16}{10} \times \frac{2}{10} \times \frac{2}{10} + \frac{16}{10} \times \frac{2}{10} \times \frac{2}{10} \times \frac{2}{10} \\ & \frac{16}{10} \left(1 + \frac{2}{10} + \frac{2^2}{10^2} + \frac{2^3}{10^3} + \dots \right) \\ & \frac{16}{10} \left(\frac{1}{1 - \frac{2}{10}} \right) = \frac{16}{10} \times \frac{10}{8} = \frac{16}{8} = 2 \end{aligned}$$

2. [Ans. A]

$$\begin{aligned} \text{Length of a bit on cable} &= \frac{\text{speed}}{\text{bw}} \\ &= \frac{200}{10} = 20 \end{aligned}$$

3. [Ans. A]

$$\begin{aligned} P(1) &= {}^n C_1 P^1 (1-P)^{n-1} \\ &= \frac{n!}{1!(n-1)!} P (1-P)^{n-1} \\ &= n p (1-P)^{n-1} \end{aligned}$$

4. [Ans. B]

At increase the bit rate twice the baud rate

5. [Ans. B]

The sample space is : {(0, 0), (0, 1), (1, 2), (0, 3), (1, 0), (1, 1), (1, 2), (1, 3)}

and the Req Event $A = \{(i, j) | (i, j) \in \text{sample space and } i < j\}$

$A = \{(0, 1), (0, 2), (0, 3), (1, 2), (1, 2)\}$

$$\begin{aligned} P_r(A) &= \frac{\# \text{ elements in } A}{\# \text{ elements in sample space}} \\ &= 5/8 = .625 \end{aligned}$$

6. [Ans. D]

Total time = Transmission time + propagation time

$$= 5 \times 50 + 200 \mu s = 450 \times 10^{-6} s$$

$$\text{Maximum achievable through put} = \frac{\text{total size}}{\text{total time}}$$

7. [Ans. D]

Min Frame size = $2 \times Z \times \text{data rate}$

$$Z = \frac{d}{v} = \frac{2 \times 10^3}{2 \times 10^8} = 10^{-5}$$

$$\begin{aligned} \therefore \text{Packet size} &= 2 \times 10^{-5} \times 10^7 \\ &= 200 \text{ bit} \end{aligned}$$

GATE Questions IT:

1. [Ans. B]

$$\begin{aligned} \text{Min Frame size} &= 2 * \frac{d}{v} * \text{data rate} \\ &= 2 \times \frac{200}{2 \times 10^8} \times 10^9 \end{aligned}$$

$$= 2 \times 10^2 \times 10^1 = 2 \times 10^3$$

$$= 2000 \text{ bits} = 250 \text{ bytes}$$

2. [Ans. C]

Given, $t_t = 3\text{ms}$

$t_p = 5\text{ms}$

$N = 10$

So, maximum utilization = 0.857

3. [Ans. A]

Given, $t_t = 3\text{ms}$

$t_p = 5\text{ms}$

$N = 15$

So, maximum utilization = 0.545

4. [Ans. B]

Polling delay = $80 \mu\text{s}$

Max $t_x = 8000 \text{ bits}$, $800 \mu\text{s}$ at 10 Mbps

$$\text{Max throughput} = \frac{\text{effective } t_x \text{ time}}{\text{total time}} \times \text{DR}$$

$$= \frac{800 \mu\text{s}}{800 + 80} \times 10^6 = \frac{10}{11} \times 10 \text{ Mbps}$$

6. [Ans. B]

$$\text{Throughput} = \frac{\text{Format size / data rate}}{\frac{\text{Frame size}}{\text{Data rate}} + \text{delay}} = 1/2$$

$$= \frac{FS/4 \times 10^3}{FS/4 \times 10^3 + 2 \times 10^{-3}} = 1/2$$

$$= \frac{FS}{4 \times 10^3} = 20 \times 10^{-3}$$

$$FS = 4 \times 10^3 \times 20 \times 10^{-3}$$

$$= 80 \text{ bits}$$

7. [Ans. A]

$$\text{Round trip propagation} = \frac{2 \times 1000}{2 \times 10^8}$$

$$= 10 \mu\text{s}$$

Bits transmit over 1 Gbps link with in $10 \mu\text{s}$ is 1 bit take $1 \text{ n sec} = 1 \times 10^{-9}$

So, $10,000 \text{ bits}$ takes $10 \mu\text{s}$.

9. [Ans. B]

Minimum throughput = 0.16

Maximum number of host = 2

In order to have minimum throughput 16 per slot per device, total throughput Req.

$$16 \times K \leq \frac{1}{K \times .2 \times (.8)^{K-1}} \text{ for } K = 2, .32 \leq \frac{1}{2 \times 2.8} \leq \frac{1}{.32} = .32$$

10. [Ans. D]

Effective data transmission rate = $10 \text{ Mbps} - 4000 \times 1000 = 10 \text{ Mbps} - 4 \text{ Mbps} = 6 \text{ Mbps}$

$$= \frac{T_x \text{ time}}{\text{Total time}} \times B\omega = \frac{T_x \text{ time}}{T_x \text{ time delay}} \times B\omega = \frac{800 \mu\text{s}}{800 \mu\text{s} + 400 \mu\text{s}} \times 10^6 = \frac{2}{3} \times 10^6 = 6 \text{ Mbps}$$

11. [Ans. A]

The largest network in which the Ethernet address of the host is unique is the subnet to which the host belongs

(TCP/UDP and sockets)

Introduction

TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages. TCP connection is a duplex connection. That means there is no difference between two sides once the connection is established.

Salient Features of TCP

- **Piggybacking of acknowledgments:** The ACK for the last received packet need not be sent as a new packet, but gets a free ride on the next outgoing data frame (using the ACK field in the frame header). The technique is temporarily delaying outgoing ACKs so that they can be hooked on the next outgoing data frame is known as piggybacking. But ACK can't be delayed for a long time if receiver (of the packet to be acknowledged) does not have any data to send.
- **Flow and congestion control:** TCP takes care of flow control by ensuring that both ends have enough resources and both can handle the speed of data transfer of each other so that none of them gets overloaded with data. The term congestion control is used in almost the same context except that resources and speed of each router is also taken care of. The main concern is network resources in the latter case.
- **Multiplexing / Demultiplexing:** Many application can be sending/receiving data at the same time. Data from all of them has to be multiplexed together. On receiving some data from lower layer, TCP has to decide which application is the recipient. This is called demultiplexing. TCP uses the concept of port number to do this.

Header format of TCP

TCP Header

Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
0	Source port																Destination port																	
32	Sequence number																																	
64	Acknowledgment number (if ACK set)																																	
96	Data offset				Reserved				C	E	U	A	P	R	S	F	Window Size																	
W									C	R	C	S	S	Y	I																			
R									E	G	K	H	T	N	N																			
128	Checksum																Urgent pointer (if URG set)																	
160	Options (if Data Offset > 5)																										padding							
...	...																																	

Explanation of header fields

- **Source and destination port :** These fields identify the local endpoint of the connection. Each host may decide for itself how to allocate its own ports starting at 1024. The source and destination socket numbers together identify the connection.
- **Sequence and ACK number :** This field is used to give a sequence number to each and every byte transferred. This has an advantage over giving the sequence numbers to every packet because data of many small packets can be combined into one at the time of retransmission, if needed. The ACK signifies the next byte expected from the source and not the last byte received. The ACKs are cumulative instead of selective. Sequence number space is as large as 32-bit although 17 bits would have been enough if the packets were delivered in order. If packets reach in order, then according to the following formula:

$$(\text{sender's window size}) + (\text{receiver's window size}) < (\text{sequence number space})$$

the sequence number space should be 17-bits. But packets may take different routes and reach out of order. So, we need a larger sequence number space. And for optimisation, this is 32-bits.

- **Header length :** This field tells how many 32-bit words are contained in the TCP header. This is needed because the options field is of variable length.
- **Flags :** There are six one-bit flags.
 1. **URG :** This bit indicates whether the urgent pointer field in this packet is being used.
 2. **ACK :** This bit is set to indicate the ACK number field in this packet is valid.
 3. **PSH :** This bit indicates PUSHed data. The receiver is requested to deliver the data to the application upon arrival and not buffer it until a full buffer has been received.

4. **RST** : This flag is used to reset a connection that has become confused due to a host crash or some other reason. It is also used to reject an invalid segment or refuse an attempt to open a connection. This causes an abrupt end to the connection, if it existed.
 5. **SYN** : This bit is used to establish connections. The connection request (1st packet in 3-way handshake) has SYN=1 and ACK=0. The connection reply (2nd packet in 3-way handshake) has SYN=1 and ACK=1.
 6. **FIN** : This bit is used to release a connection. It specifies that the sender has no more fresh data to transmit. However, it will retransmit any lost or delayed packet. Also, it will continue to receive data from other side. Since SYN and FIN packets have to be acknowledged, they must have a sequence number even if they do not contain any data.
- **Window Size** : Flow control in TCP is handled using a variable-size sliding window. The Window Size field tells how many bytes may be sent starting at the byte acknowledged. Sender can send the bytes with sequence number between (ACK#) to (ACK# + window size - 1). A window size of zero is legal and says that the bytes up to and including ACK# - 1 have been received, but the receiver would like no more data for the moment. Permission to send can be granted later by sending a segment with the same ACK number and a nonzero Window Size field.
 - **Checksum** : This is provided for extreme reliability. It checksums the header, the data, and the conceptual pseudoheader. The pseudoheader contains the 32-bit IP address of the source and destination machines, the protocol number for TCP(6), and the byte count for the TCP segment (including the header). Including the pseudoheader in TCP checksum computation helps detect misdelivered packets, but doing so violates the protocol hierarchy since the IP addresses in it belong to the IP layer, not the TCP layer.
 - **Urgent Pointer** : Indicates a byte offset from the current sequence number at which urgent data are to be found. Urgent data continues till the end of the segment. This is not used in practice. The same effect can be had by using two TCP connections, one for transferring urgent data.
 - **Options** : Provides a way to add extra facilities not covered by the regular header. eg,
 - Maximum TCP payload that sender is willing to handle. The maximum size of segment is called MSS (Maximum Segment Size). At the time of handshake, both parties inform each other about their capacity. Minimum of the two is honoured. This information is sent in the options of the SYN packets of the three way handshake.
 - Window scale option can be used to increase the window size. It can be specified by telling the receiver that the window size should be interpreted by shifting it left by specified number of bits. This header option allows window size up to 230.

Data : This can be of variable size. TCP knows its size by looking at the IP size header.

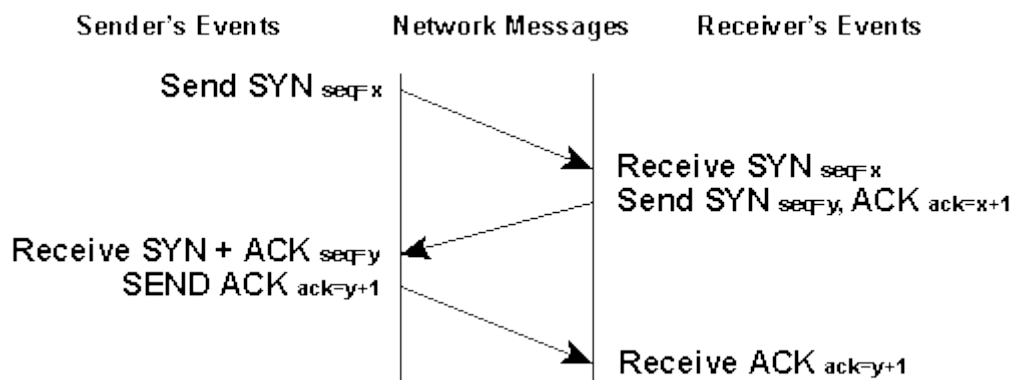
TCP Connection management

The "three-way handshake" is the procedure used to establish a connection. This procedure normally is initiated by one TCP and responded to by another TCP. The procedure also works if two TCP simultaneously initiate the procedure. When simultaneous attempt occurs, each TCP receives a "SYN" segment which carries no acknowledgment after it has sent a "SYN".

Of course, the arrival of an old duplicate "SYN" segment can potentially make it appear, to the recipient, that a simultaneous connection initiation is in progress. Proper use of "reset" segments can disambiguate these cases

The three-way handshake reduces the possibility of false connections. It is the implementation of a trade-off between memory and messages to provide information for this checking.

Connection Establish



- The sender sends a SYN packet with sequence number say 'x'.
- The receiver on receiving SYN packet responds with SYN packet with sequence number 'y' and ACK with seq number 'x+1'
- On receiving both SYN and ACK packet, the sender responds with ACK packet with seq number 'y+1'
- The receiver when receives ACK packet, initiates the connection.

TCP transmission policy

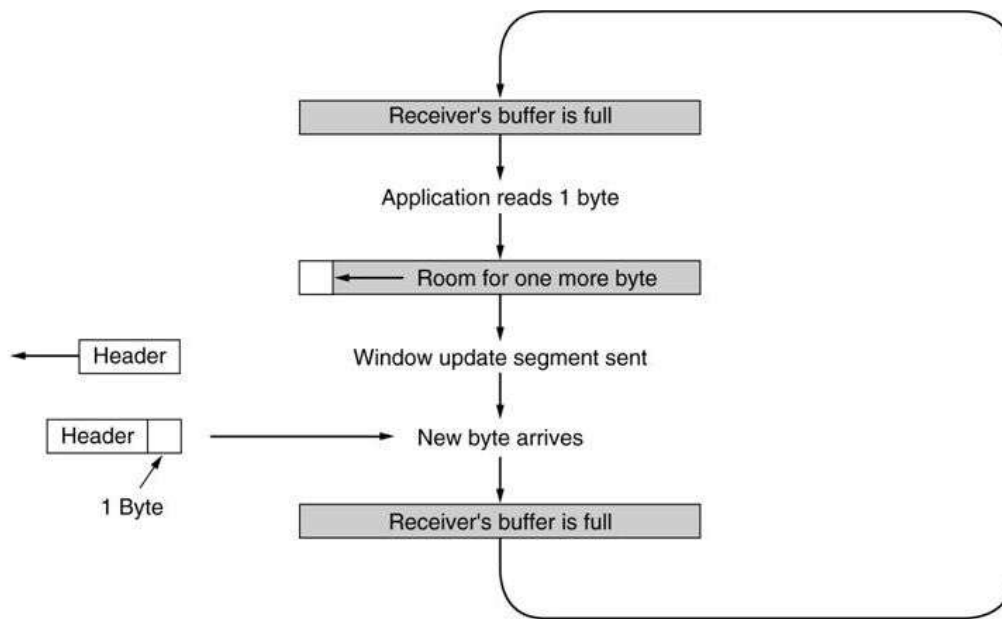
For every packet received, The recipient returns an ACK.

Recipient send duplicate ACK, If packet is lost.

Sender retransmit lost packet.

Silly Window Syndrome

This happens when the application supplying data to the sender does so in large chunks, but the application taking data from receiver (probably an interactive application) does it in very small chunks, say 1 byte at a time. The sender keeps advertising windows of size 1 byte each as the application consumes the bytes one at a time.



Silly Window Syndrome

TCP Optimization

Nagle's algorithm

when data comes to the sender one byte at a time , send the first byte and buffer all the remaining bytes till the outstanding byte is acknowledged. Then send all the buffered characters in one segment and start buffering again till they are acknowledged. It can help reduce the bandwidth usage for example when the user is typing quickly into a telnet connection and the network is slow .

Clark's Solution to this problem

We try to prevent the sender from advertising very small windows. The sender should try to wait until it has accumulated enough space in the window to send a full segment or half the receiver's buffer size, which it can estimate from the pattern of window updates that it received in the past.

TCP congestion control mechanism

If the receiver advertises a large window-size , larger than what the network en route can handle , then there will invariably be packet losses. So there will be re-transmissions as well . However , the sender cannot send all the packets for which ACK has not been received because this way it will be causing even more congestion in the network. Moreover , the sender at this point of time cannot be sure about how many packets have actually been lost . It might be that this is the only one that has been lost , and some following it have actually

been received and buffered by the receiver. In that case, the sender will have unnecessarily sent a number of packets.

So the re-transmission of the packets also follows slow-start mechanism. However, we do indeed need to keep an upper bound on the size of the packets as it increases in slow start, to prevent it from increasing unbounded and causing congestion. This cap is put at half the value of the segment size at which packet loss started.

Congestion Control : Congestion is a condition of severe delay caused by an overload of datagrams at any intermediate node on the Internet. If unchecked it may feed on itself and finally the node may start dropping arriving datagrams. This can further aggravate congestion in the network resulting in congestion collapse. TCP uses two techniques to check congestion.

1. **Slow Start :** At the time of start of a connection no information about network conditions is available. A Recv_Win size can be agreed upon however C_Win size is not known. Any arbitrary C_Win size can not be used because it may lead to congestion. TCP acts as if the window size is equal to the minimum of (Recv_Win & C_Win). So following algorithm is used.
 1. Recv_Win=X
 2. SET C_Win=1
 3. for every ACK received C_Win++
2. **Multiplicative decrease :** This scheme is used when congestion is encountered (ie. when a segment is lost). It works as follows. Reduce the congestion window by half if a segment is lost and exponentially backoff the timer (double it) for the segments within the reduced window. If the next segment also gets lost continue the above process. For successive losses this scheme reduces traffic into the connection exponentially thus allowing the intermediate nodes to clear their queues. Once congestion ends SLOW START is used to scale up the transmission.
2. **Congestion Avoidance :** This procedure is used at the onset of congestion to minimize its effect on the network. When transmission is to be scaled up it should be done in such a way that it doesn't lead to congestion again. Following algorithm is used.
 1. At loss of a segment SET C_Win=1.
 2. SET SLOW START THRESHOLD (SST) = Send_Win / 2.
 3. Send segment.
 4. If ACK Received, C_Win++ till C_Win <= SST.
 5. else for each ACK C_Win += 1 / C_Win.

TCP Timer Management

TCP uses multiple timers to do its work

The most important is the retransmission timer

- When a segment is sent, a retransmission timer is started.
- If the segment is acknowledged before this timer expires, the timer is stopped

- If the timer goes off before the segment is acknowledged ,then the segment gets retransmitted(and the timer restarted).
- The big question is how long this timer interval should be?

Keepalive timer is designed to check for connection integrity

- Another important timer in TCP is keep alive timer. It is basically used by a TCP peer to check whether the other end is up or down. It periodically checks this connection. If the other end did not respond, then that connection will be closed.
- When goes off (because a long time of inactivity),causing one side to check if the other side is still there.

Persistence timer is designed to prevent deadlock

- As we saw in TCP window management, when source sends one full window of packets, it will set its window size to 0 and expects an ACK from remote TCP to increase its window size. Suppose such an ACK has been sent and is lost. Hence source will have current window size = 0 and cannot send & destination is expecting next byte.
- To avoid such a deadlock, a Persist Timer will be used. When this timer goes off, the source will send the last one byte again. So we hope that situation has improved and an ACK to increase the current window size will be received.

State Transition Diagram Of TCP

The state diagram approach to view the TCP connection establishment and closing simplifies the design of TCP implementation. The idea is to represent the TCP connection state, which progresses from one state to other as various messages are exchanged. To simplify the matter, we considered two state diagrams, viz., for TCP connection establishment and TCP connection closing.

Fig 1 shows the state diagram for the TCP connection establishment and associated table briefly explains each state.

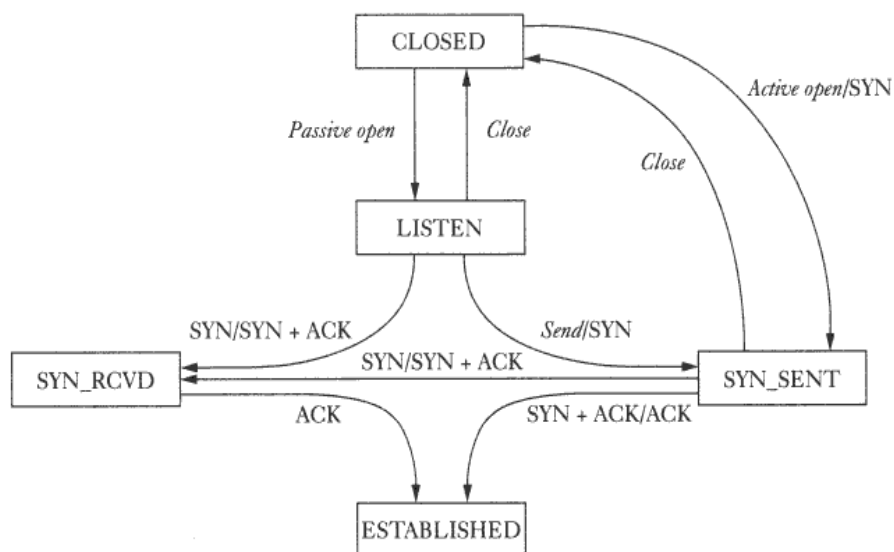


Fig 1. TCP Connection establishment

Brief description of each state of the above diagram.

	Represents the state when waiting for connection request from any remote host and port. This specifically applies to a Server.
Listen	From this state, the server can close the service or actively open a connection by sending SYN.
	Represents waiting for a matching for a connection request after having sent a connection request. This applies to both server and client side. Even though server is considered as the one with passive open, it can also send a SYN packet actively.
Syn-Sent	
	Represents waiting for a confirmation connection request acknowledgment after having both received and sent connection request.
Syn_Rcvd	
	Represents an open connection. Data transfer can take place from this point onwards.
Estab	

After the connection has been established, two end-points will exchange useful information and terminate the connection. Fig. 2 shows the state diagram for terminating an active connection.

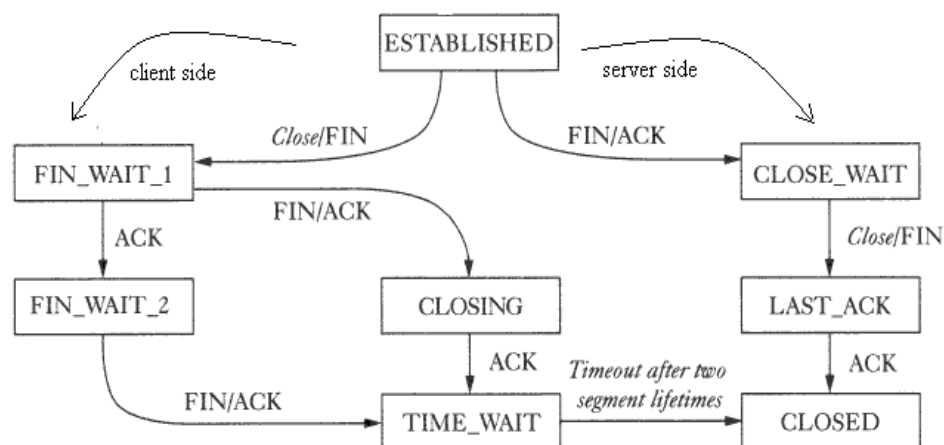


Fig 2. TCP Connection termination

State Description

FIN-WAIT-1	Represents connection termination request from the remote TCP peer, or an acknowledgment of the connection termination request previously sent.
FIN-WAIT-2	This state is entered when server issues close call. Represents waiting for a connection termination request from the remote TCP.
CLOSING	Represents connection termination request acknowledgment from the remote TCP.
TIME_WAIT	This represents waiting time enough for the packets to reach their destination. This waiting time is usually 4 min.
CLOSE_WAIT	Represents a state when the server receives a FIN from the remote TCP , sends ACK and issues close call sending FIN
LAST_ACK	Represents waiting for an ACK for the previously sent FIN-ACK to the remote TCP
CLOSE	Represents a closed TCP connection having received all the ACKs

UDP –User Datagram Protocol

UDP like its cousin the Transmission Control Protocol (TCP) sits directly on top of the base Internet Protocol (IP). In general, UDP implements a fairly "lightweight" layer above the Internet Protocol. It seems at first site that similar service is provided by both UDP and IP, namely transfer of data. But we need UDP for multiplexing /demultiplexing of addresses.

UDP's main purpose is to abstract network traffic in the form of datagrams. A datagram comprises one single "unit" of binary data; the first eight (8) bytes of a datagram contain the header information and the remaining bytes contain the data itself.

UDP Headers

The UDP header consists of four (4) fields of two bytes each:

Source Port	Destination Port
Length	Checksum

- source port number
 - destination port number
 - datagram size
 - checksum
-
- UDP port numbers allow different applications to maintain their own "channels" for data; both UDP and TCP use this mechanism to support multiple applications sending and receiving data concurrently.
 - The sending application (that could be a client or a server) sends UDP datagrams through the source port, and the recipient of the packet accepts this datagram through the destination port. Some applications use static port numbers that are reserved for or registered to the application.
 - Other applications use dynamic (unregistered) port numbers. Because the UDP port headers are two bytes long, valid port numbers range from 0 to 65535; by convention, values above 49151 represent dynamic ports.
 - The datagram size is a simple count of the number of bytes contained in the header and data sections . Because the header length is a fixed size, this field essentially refers to the length of the variable-sized data portion (sometimes called the payload).
 - The maximum size of a datagram varies depending on the operating environment. With a two-byte size field, the theoretical maximum size is 65535 bytes. However,

some implementations of UDP restrict the datagram to a smaller number sometimes as low as 8192 bytes.

- UDP checksums work as a safety feature. The checksum value represents an encoding of the datagram data that is calculated first by the sender and later by the receiver. Should an individual datagram be tampered with (due to a hacker) or get corrupted during transmission (due to line noise, for example), the calculations of the sender and receiver will not match, and the UDP protocol will detect this error. The algorithm is not fool-proof, but it is effective in many cases.
- In UDP, check summing is optional -- turning it off squeezes a little extra performance from the system -- as opposed to TCP where checksums are mandatory. It should be remembered that check summing is optional only for the sender, not the receiver. If the sender has used checksum then it is mandatory for the receiver to do so.
- Usage of the Checksum in UDP is optional. In case the sender does not use it, it sets the checksum field to all 0's. Now if the sender computes the checksum then the recipient must also compute the checksum and set the field accordingly.
- If the checksum is calculated and turns out to be all 1's then the sender sends all 1's instead of all 0's. This is since in the algorithm for checksum computation used by UDP, a checksum of all 1's is equivalent to a checksum of all 0's. Now the checksum field is unambiguous for the recipient, if it is all 0's then checksum has not been used, in any other case the checksum has to be computed.

Protocols Used For TCP and UDP

Protocols used for TCP

Port	Protocol	Use
21	FTP	File transfer
23	Telnet	Remote login
25	SMTP	E-mail
69	TFTP	Trivial file transfer protocol
79	Finger	Lookup information about a user
80	HTTP	World Wide Web
110	POP-3	Remote e-mail access
119	NNTP	USENET news

Protocols used for UDP

Port	Protocol
7	Echo
9	Discard
11	Users
13	Daytime
17	Quote
19	Chargen
53	Nameserver
67	Bootps
68	Bootpc
69	TFTP
111	RPC
123	NTP

Routing Algorithms

Routing is the process of forwarding of a packet in a network so that it reaches its intended destination. The main goals of routing are:

1. **Correctness:** The routing should be done properly and correctly so that the packets may reach their proper destination.
2. **Simplicity:** The routing should be done in a simple manner so that the overhead is as low as possible. With increasing complexity of the routing algorithms the overhead also increases.
3. **Robustness:** Once a major network becomes operative, it may be expected to run continuously for years without any failures. The algorithms designed for routing should be robust enough to handle hardware and software failures and should be able to cope with changes in the topology and traffic without requiring all jobs in all hosts to be aborted and the network rebooted every time some router goes down.
4. **Stability:** The routing algorithms should be stable under all possible circumstances.
5. **Fairness:** Every node connected to the network should get a fair chance of transmitting their packets. This is generally done on a first come first serve basis.
6. **Optimality:** The routing algorithms should be optimal in terms of throughput and minimizing mean packet delays. Here there is a trade-off and one has to choose depending on his suitability.

Classification of Routing Algorithms

The routing algorithms may be classified as follows:

1. **Adaptive Routing Algorithm:** These algorithms change their routing decisions to reflect changes in the topology and in traffic as well. These get their routing information from adjacent routers or from all routers. The optimization parameters are the distance, number of hops and estimated transit time. This can be further classified as follows:
 1. **Centralized:** In this type some central node in the network gets entire information about the network topology, about the traffic and about other nodes. This then transmits this information to the respective routers. The advantage of this is that only one node is required to keep the information. The disadvantage is that if the central node goes down the entire network is down, i.e. single point of failure.
 2. **Isolated:** In this method the node decides the routing without seeking information from other nodes. The sending node does not know about the status of a particular link. The disadvantage is that the packet may be sent through a congested route resulting in a delay. Some examples of this type of algorithm for routing are:
 - **Hot Potato:** When a packet comes to a node, it tries to get rid of it as fast as it can, by putting it on the shortest output queue without regard to where that link leads. A variation of this algorithm is to combine static routing with the hot potato algorithm. When a packet arrives, the routing algorithm takes into account both the static weights of the links and the queue lengths.
 - **Backward Learning:** In this method the routing tables at each node gets modified by information from the incoming packets. One way to implement backward learning is to include the identity of the source node in each packet, together with a hop counter that is incremented on each hop. When a node receives a packet in a particular line, it notes down the number of hops it has taken to reach it from the source node. If the previous value of hop count stored in the node is better than the current one then nothing is done but if the current value is better then the value is updated for future use. The problem with this is that when the best route goes down then it cannot recall the second best route to a particular node. Hence all the nodes have to forget the stored informations periodically and start all over again.
 3. **Distributed:** In this the node receives information from its neighbouring nodes and then takes the decision about which way to send the packet. The disadvantage is that if in between the the interval it receives information and sends the packet something changes then the packet may be delayed.
2. **Non-Adaptive Routing Algorithm:** These algorithms do not base their routing decisions on measurements and estimates of the current traffic and topology. Instead the route to be taken in going from one node to the other is computed in advance, off-line, and downloaded to the routers when the network is booted. This is also known as static routing. This can be further classified as:
 1. **Flooding:** Flooding adapts the technique in which every incoming packet is sent on every outgoing line except the one on which it arrived. One problem with this method is that packets may go in a loop. As a result of this a node

may receive several copies of a particular packet which is undesirable. Some techniques adapted to overcome these problems are as follows:

- **Sequence Numbers:** Every packet is given a sequence number. When a node receives the packet it sees its source address and sequence number. If the node finds that it has sent the same packet earlier then it will not transmit the packet and will just discard it.
- **Hop Count:** Every packet has a hop count associated with it. This is decremented(or incremented) by one by each node which sees it. When the hop count becomes zero(or a maximum possible value) the packet is dropped.
- **Spanning Tree:** The packet is sent only on those links that lead to the destination by constructing a spanning tree routed at the source. This avoids loops in transmission but is possible only when all the intermediate nodes have knowledge of the network topology.

Flooding is not practical for general kinds of applications. But in cases where high degree of robustness is desired such as in military applications, flooding is of great help.

2. **Random Walk:** In this method a packet is sent by the node to one of its neighbours randomly. This algorithm is highly robust. When the network is highly interconnected, this algorithm has the property of making excellent use of alternative routes. It is usually implemented by sending the packet onto the least queued link.

Link state routing protocol:

Dijkstra's algorithm

Notation:

D_i = Length of shortest path from node 'i' to node 1.

$d_{i,j}$ = Length of path between nodes i and j .

Algorithm

- Each node j is labeled with D_j , which is an estimate of cost of path from node j to node 1. Initially, let the estimates be infinity, indicating that nothing is known about the paths.
- We now iterate on the length of paths, each time revising our estimate to lower values, as we obtain them. Actually, we divide the nodes into two groups ; the first one, called set P contains the nodes whose shortest distances have been found, and the other Q containing all the remaining nodes.

- Initially P contains only the node 1. At each step, we select the node that has minimum cost path to node 1. This node is transferred to set P. At the first step, this corresponds to shifting the node closest to 1 in P.
- Its minimum cost to node 1 is now known. At the next step, select the next closest node from set Q and update the labels corresponding to each node using :

$$D_j = \min [D_j , D_i + d_{j,i}]$$

Finally, after N-1 iterations, the shortest paths for all nodes are known, and the algorithm terminates.

Principle

- Let the closest node to 1 at some step be i. Then i is shifted to P. Now, for each node j, the closest path to 1 either passes through i or it doesn't. In the first case D_j remains the same.
- In the second case, the revised estimate of D_j is the sum $D_i + d_{i,j}$. So we take the minimum of these two cases and update D_j accordingly. As each of the nodes get transferred to set P, the estimates get closer to the lowest possible value.
- When a node is transferred, its shortest path length is known. So finally all the nodes are in P and the D_j 's represent the minimum costs. The algorithm is guaranteed to terminate in N-1 iterations and its complexity is $O(N^2)$.

Examples of link-state routing protocols include open shortest path first(OSPF) and intermediate system to intermediate system (IS-IS).

Distance Vector Routing Algorithms:

Bellman-Ford Algorithm

This algorithm iterates on the number of edges in a path to obtain the shortest path. Since the number of hops possible is limited (cycles are implicitly not allowed), the algorithm terminates giving the shortest path.

Notation:

- $d_{i,j}$ = Length of path between nodes i and j, indicating the cost of the link.
- h = Number of hops.
- $D[i,h]$ = Shortest path length from node i to node 1, with upto 'h' hops.
- $D[1,h] = 0$ for all h.

Algorithm :

Initial condition : $D[i, 0] = \text{infinity}$, for all i ($i \neq 1$)

Iteration : $D[i, h+1] = \min \{ d_{i,j} + D[j, h] \}$ over all values of j .

Termination : The algorithm terminates when

$$D[i, h] = D[i, h+1] \quad \text{for all } i.$$

Principle:

- For zero hops, the minimum length path has length of infinity, for every node. For one hop the shortest-path length associated with a node is equal to the length of the edge between that node and node 1.
- Hereafter, we increment the number of hops allowed, (from h to $h+1$) and find out whether a shorter path exists through each of the other nodes. If it exists, say through node ' j ', then its length must be the sum of the lengths between these two nodes (i.e. $d_{i,j}$) and the shortest path between j and 1 obtainable in upto h paths. If such a path doesn't exist, then the path length remains the same.
- The algorithm is guaranteed to terminate, since there are utmost N nodes, and so $N-1$ paths. It has time complexity of $O(N^3)$.

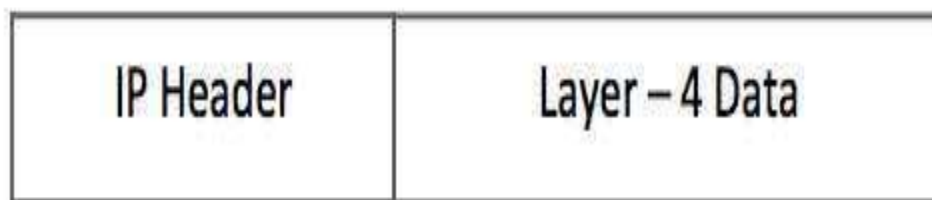
Examples of distance-vector routing protocols include RIPv1 and RIPv2, IGRP and Babel.

IP(V4)

- Internet Protocol is one of the major protocols in the TCP/IP protocols suite. This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model.
- Thus this protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.
- IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination.
- Internet Protocol version 4 uses 32-bit logical address.

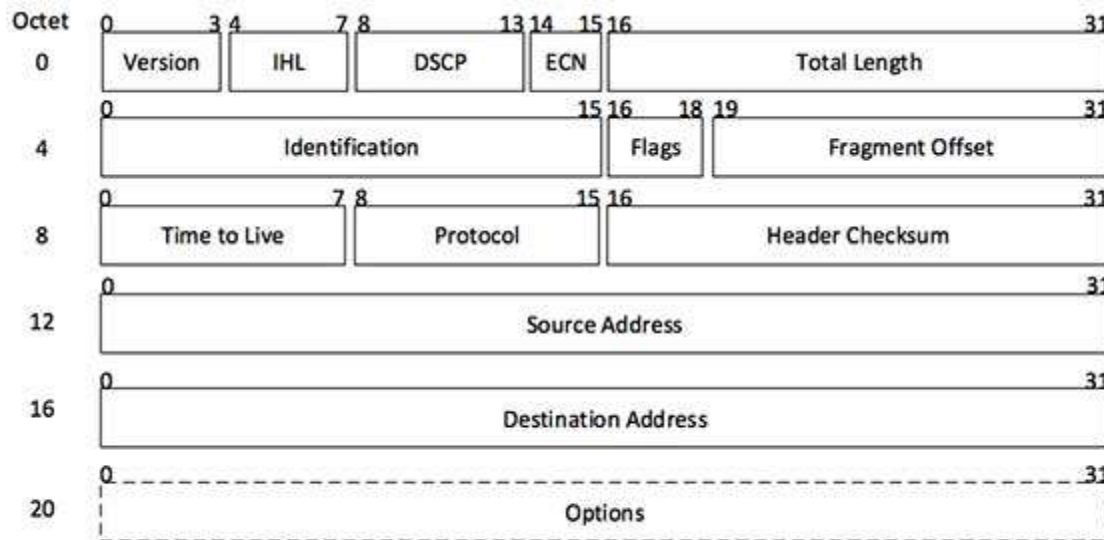
IP(v4)-Frame format

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.



(IP Encapsulation)

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.



[Image: IP Header]

IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows:

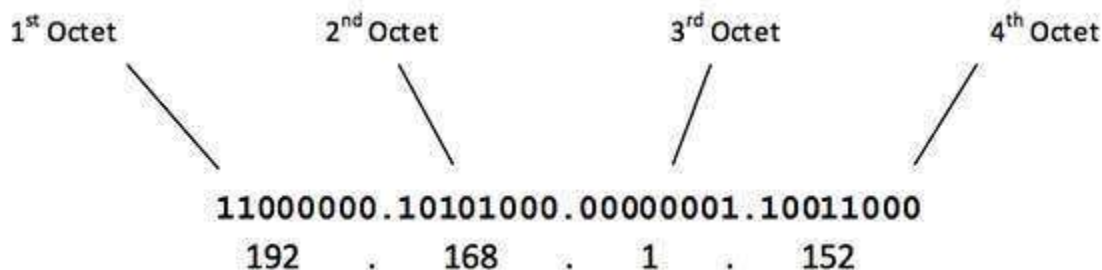
- **Version:** Version no. of Internet Protocol used (e.g. IPv4).
- **IHL:** Internet Header Length; Length of entire IP header.
- **DSCP:** Differentiated Services Code Point; this is Type of Service.
- **ECN:** Explicit Congestion Notification; It carries information about the congestion seen in the route.
- **Total Length:** Length of entire IP Packet (including IP header and IP Payload).
- **Identification:** If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
- **Flags:** As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- **Fragment Offset:** This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live:** To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross.

- At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol:** Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum:** This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- **Source Address:** 32-bit address of the Sender (or source) of the packet.
- **Destination Address:** 32-bit address of the Receiver (or destination) of the packet.
- **Options:** This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

Different class (A,B,C etc) Addressing

- Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network.
- Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.
- Internet Corporation for Assigned Names and Numbers(ICANN) is responsible for assigning IP addresses

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address:



The number of networks and the number of hosts per class can be derived by this formula:

$$\text{Number of networks} = 2^{\text{network_bits}}$$

$$\text{Number of Hosts/Network} = 2^{\text{host_bits}} - 2$$

- When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Class A Address :

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.

00000001 – 01111111
1 – 127

- Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.
- The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts ($2^{24}-2$).
- Class A IP address format is thus:

0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B Address :

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

10000000 – 10111111
128 – 191

- Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.
- Class B has 16384 (2^{14}) Network addresses and 65534 ($2^{16}-2$) Host addresses.
- Class B IP address format is:

10NNNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

Class C Address :

The first octet of Class C IP address has its first 3 bits set to 110, that is:

11000000 – 11011111
192 – 223

- Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

- Class C gives 2097152 (2^{21}) Network addresses and 254 (2^8-2) Host addresses.
- Class C IP address format is:

110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

Class D Address :

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of:

11100000 – **1110**1111
224 – 239

- Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting.
- In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address :

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class range from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

Subnetting

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

Class A Subnets

- In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network).
- To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.

- For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets ($2^1=2$) with ($2^{23}-2$) 8388606 Hosts per Subnet.
- The Subnet mask is changed accordingly to reflect subnetting. Given below is a list of possible combination of Class A subnets:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
⋮	⋮	⋮	⋮	⋮
28	255.255.255.240	20	1048576	14
29	255.255.255.248	21	2097152	6
30	255.255.255.252	22	4194304	2

- In case of subnetting too, the very first and last IP address of every subnet is used for Subnet Number and Subnet Broadcast IP address respectively.
- Because these two IP addresses cannot be assigned to hosts, sub-netting cannot be implemented by using more than 30 bits as Network Bits, which provides less than two hosts per subnet.

Class B Subnets

- By default, using Classful Networking, 14 bits are used as Network bits providing (2^{14}) 16384 Networks and ($2^{16}-2$) 65534 Hosts.
- Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
16	255.255.0.0	0	0	65534
17	255.255.128.0	1	2	32766
18	255.255.192.0	2	4	16382
19	255.255.224.0	3	8	8190
20	255.255.240.0	4	16	4094
21	255.255.248.0	5	32	2046
22	255.255.252.0	6	64	1022
23	255.255.254.0	7	128	510
24	255.255.255.0	8	256	254
25	255.255.255.128	9	512	126
26	255.255.255.192	10	1024	62
27	255.255.255.224	11	2048	30
28	255.255.255.240	12	4096	14
29	255.255.255.248	13	8192	6
30	255.255.255.252	14	16384	2

Class C Subnets

- Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address:

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
24	255.255.255.0	0	1	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	255.255.255.224	3	8	30
28	255.255.255.240	4	16	14
29	255.255.255.248	5	32	6
30	255.255.255.252	6	64	2

Supernetting

- Supernetting, also called Classless Inter-Domain Routing (CIDR), is a way to aggregate multiple Internet addresses of the same class.
- The original Internet Protocol (IP) defines IP addresses in four major classes of address structure, Classes A through E. Each class allocates one portion of the 32-bit

Internet address format to a network address and the remaining portion to the specific host machines within the network.

- Using supernetting, the network address 192.168.2.0/24 and an adjacent address 192.168.3.0/24 can be merged into 192.168.2.0/23. The "23" at the end of the address says that the first 23 bits are the network part of the address, leaving the remaining nine bits for specific host addresses.
- Supernetting is most often used to combine Class C network addresses and is the basis for most routing protocols currently used on the Internet.
- The Border Gateway Protocol (BGP) and the Open Shortest Path First (OSPF) router protocol both support supernetting, but the Exterior Gateway Protocol (EGP) and the Routing Information Protocol (RIP) do not support it.

IPV4 Reserved Addresses

There are a few reserved IPv4 address spaces which cannot be used on the internet. These addresses serve special purpose and cannot be routed outside the Local Area Network.

Private IP Addresses

- Every class of IP, (A, B & C) has some addresses reserved as Private IP addresses. These IPs can be used within a network, campus, company and are private to it.
- These addresses cannot be routed on the Internet, so packets containing these private addresses are dropped by the Routers.

Class A IP Range	Subnet Mask
10.0.0.0 – 10.255.255.255	255.0.0.0
172.16.0.0 – 172.31.255.255	255.240.0.0
192.168.0.0 – 192.168.255.255	255.255.0.0

Loopback IP Addresses

- The IP address range 127.0.0.0 – 127.255.255.255 is reserved for loopback, i.e. a Host's self-address, also known as localhost address. This loopback IP address is managed entirely by and within the operating system.
- Loopback addresses, enable the Server and Client processes on a single system to communicate with each other. When a process creates a packet with destination address as loopback address, the operating system loops it back to itself without having any interference of NIC.

- Data sent on loopback is forwarded by the operating system to a virtual network interface within operating system. This address is mostly used for testing purposes like client-server architecture on a single machine.

Link-local Addresses

- In case a host is not able to acquire an IP address from the DHCP server and it has not been assigned any IP address manually, the host can assign itself an IP address from a range of reserved Link-local addresses . Link local address ranges from 169.254.0.0 to 169.254.255.255.

IPv6

- Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.

The major points that played a key role in the birth of IPv6:

- Internet has grown exponentially and the address space allowed by IPv4 is saturating. There is a requirement to have a protocol that can satisfy the needs of future Internet addresses that is expected to grow in an unexpected manner.
- IPv4 on its own does not provide any security feature. Data has to be encrypted with some other security application before being sent on the Internet.
- Data prioritization in IPv4 is not up to date. Though IPv4 has a few bits reserved for Type of Service or Quality of Service, but they do not provide much functionality.
- IPv4 enabled clients can be configured manually or they need some address configuration mechanism. It does not have a mechanism to configure a device to have globally unique IP address.

It offers the following features:

- **Larger Address Space**

In contrast to IPv4(32 bit), IPv6 uses 4 times more bits to address a device on the Internet. An IPv6 address is made of 128 bits divided into eight 16-bits blocks.

- **Simplified Header**

IPv6's header has been simplified by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header.

- **End-to-end Connectivity**

Every system now has unique IP address and can traverse through the Internet without using NAT or other translating components

- **Faster Forwarding/Routing**

Simplified header puts all unnecessary information at the end of the header. The information contained in the first part of the header is adequate for a Router to take routing decisions, thus making routing decision as quickly as looking at the mandatory header.

- **IPSec**

Initially it was decided that IPv6 must have IPSec security, making it more secure than IPv4. This feature has now been made optional.

- **No Broadcast**

Though Ethernet/Token Ring are considered as broadcast network because they support Broadcasting, IPv6 does not have any broadcast support any more. It uses multicast to communicate with multiple hosts.

- **Anycast Support**

This is another characteristic of IPv6. IPv6 has introduced Anycast mode of packet routing. In this mode, multiple interfaces over the Internet are assigned same Anycast IP address. Routers, while routing, send the packet to the nearest destination.

- **Mobility**

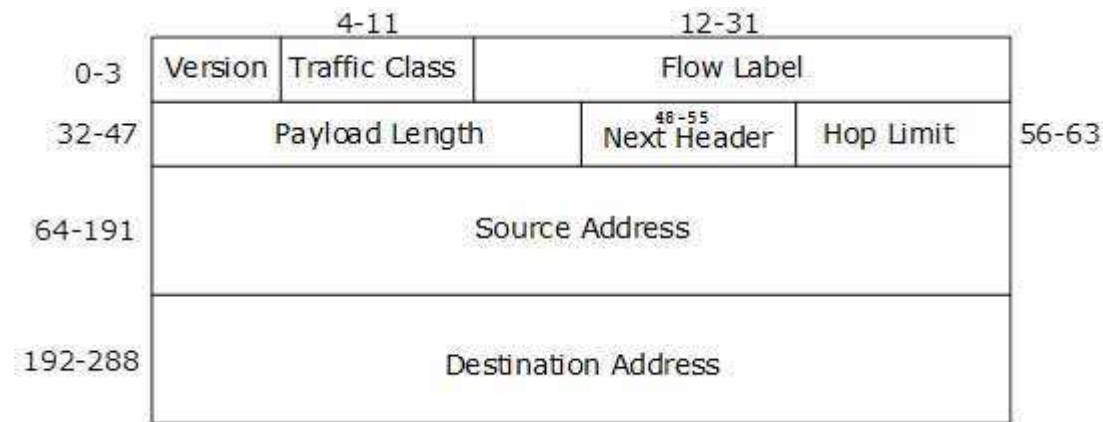
IPv6 was designed keeping mobility in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address.

- **Extensibility**

One of the major advantages of IPv6 header is that it is extensible to add more information in the option part. IPv4 provides only 40-bytes for options, whereas options in IPv6 can be as much as the size of IPv6 packet itself.

Fixed Header

IPv6 fixed header is 40 bytes long.

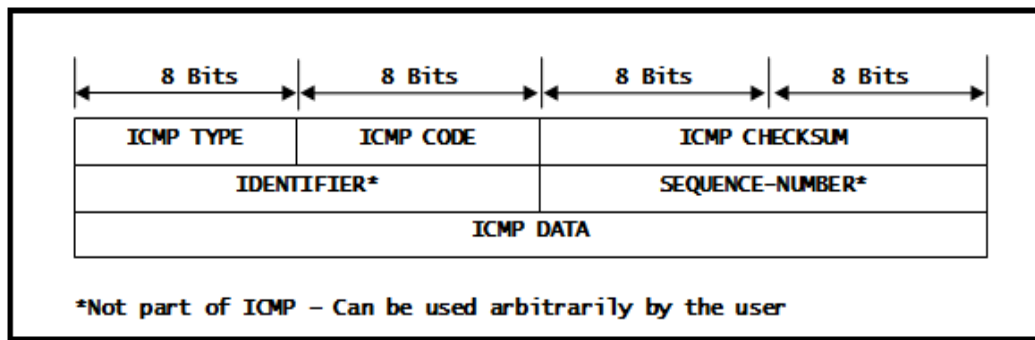


Application Layer Protocols

ICMP

- ICMP (Internet Control Message Protocol) is an error-reporting protocol network devices like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets.
- ICMP creates and sends messages to the source IP address indicating that a gateway to the Internet that a router, service or host cannot be reached for packet delivery. Any IP network device has the capability to send, receive or process ICMP messages.
- ICMP is *not* a transport protocol that sends data between systems.
- While ICMP is not used regularly in end-user applications, it is used by network administrators to troubleshoot Internet connections in diagnostic utilities including ping and trace route.
- One of the main protocols of the Internet Protocol suite, ICMP is used by routers, intermediary devices or hosts to communicate error information or updates to other routers, intermediary devices or hosts. The widely used IPv4 (Internet Protocol version 4) and the newer IPv6 use similar versions of the ICMP protocol (ICMPv4 and ICMPv6, respectively).

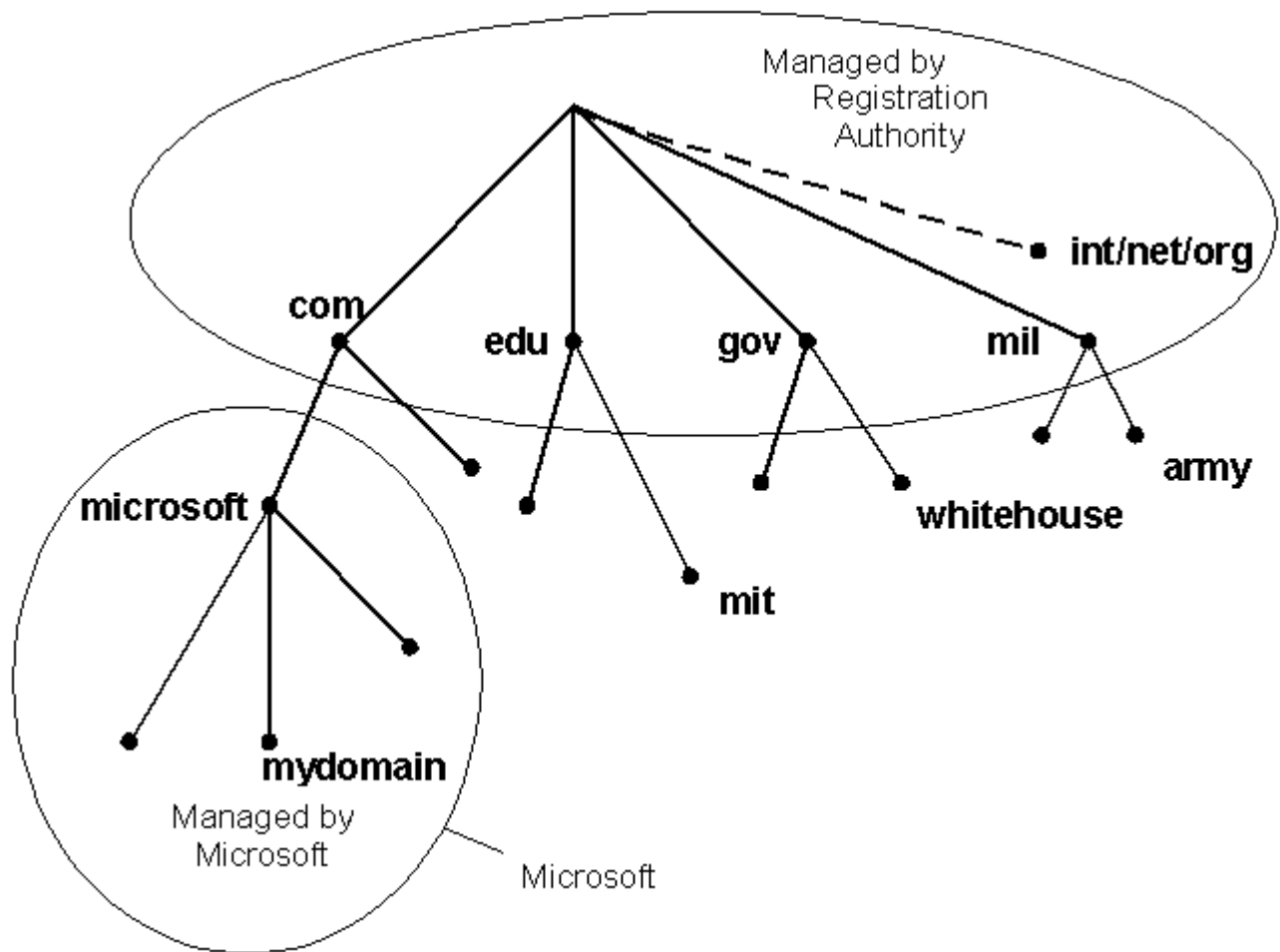
Frame format - ICMP



DNS(Domain Name Service)

- DNS is an abbreviation for Domain Name System, a system for naming computers and network services that is organized into a hierarchy of domains. DNS naming is used in TCP/IP networks, such as the Internet, to locate computers and services through user-friendly names.
- When a user enters a DNS name in an application, DNS services can resolve the name to other information associated with the name, such as an IP address.
- Conceptually, the internet is divide into several hundred top level domains where each domain covers many hosts. Each domain is partitioned in sub-domains which may be further partitioned into sub-domains and so on... So the domain space is partitioned in a tree like structure as shown below. It should be noted that this tree hierarchy has nothing in common with the IP address hierarchy or organization.

The internet uses a hierarchical tree structure of Domain Name Servers for IP address resolution of a host name :



- The top level domains are either generic or names of countries. eg of generic top level domains are .edu .mil .gov .org .net .com .int etc. For countries we have one entry for each country as defined in ISO3166. eg. .in (India) .uk (United Kingdom).
- The leaf nodes of this tree are target machines. Obviously we would have to ensure that the names in a row in a subdomain are unique. The max length of any name between two dots can be 63 characters.
- The absolute address should not be more than 255 characters. Domain names are case insensitive. Also in a name only letters, digits and hyphen are allowed. For eg. www.iitk.ac.in is a domain name corresponding to a machine named www under the subsubdomain iitk.ac.in.

SMTP

- SMTP stands for Simple Mail Transfer Protocol. SMTP is used when email is delivered from an email client, such as Outlook Express, to an email server or when email is delivered from one email server to another. SMTP uses port 25.
- SMTP is part of the application layer of the TCP/IP protocol. Using a process called "store and forward," SMTP moves your email on and across networks.

- SMTP is generally integrated within an email client application and is composed of four key components:
 1. Local user or client-end utility known as the mail user agent (MUA)
 2. Server known as mail submission agent (MSA)
 3. Mail transfer agent (MTA)
 4. Mail delivery agent (MDA)
- It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox.
- SMTP spells out and directs how your email moves from your computer's MTA to an MTA on another computer, and even several computers. Using that "store and forward" feature mentioned before, the message can move in steps from your computer to its destination.

POP3

- Post Office Protocol (POP) is a type of computer networking and Internet standard protocol that extracts and retrieves email from a remote mail server for access by the host machine.
- POP is an application layer protocol in the OSI model that provides end users the ability to fetch and receive email.
- Post Office Protocol is the primary protocol behind email communication. POP works through a supporting email software client that integrates POP for connecting to the remote email server and downloading email messages to the recipient's computer machine.
- POP uses the TCP/IP protocol stack for network connection and works with Simple Mail Transfer Protocol (SMTP) for end-to-end email communication, where POP pulls messages and SMTP pushes them to the server.

FTP

- File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.
- FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content.

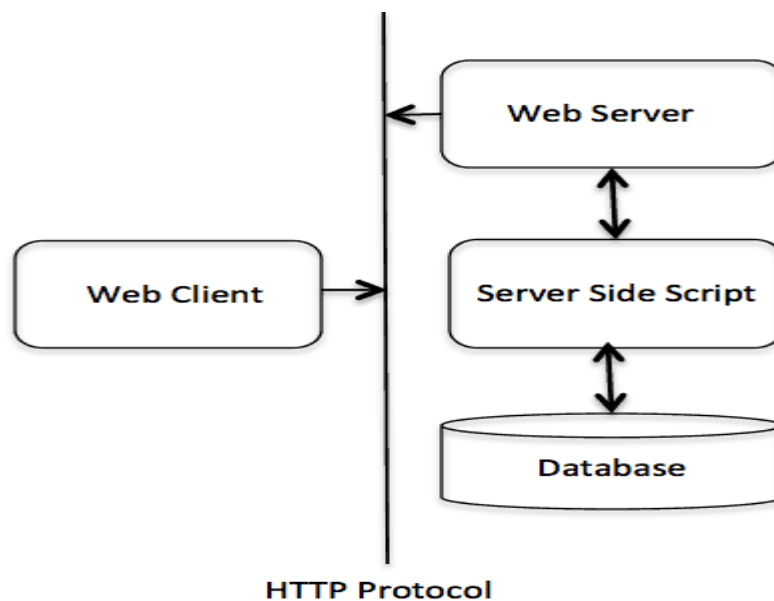
- Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, also known as anonymous FTP.

HTTP

- The Hypertext Transfer Protocol (HTTP) is an application-level protocol.
- HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers.
- HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web. The default port is TCP 80, but other ports can be used as well.

There are three basic features that make HTTP a simple but powerful protocol:

- **HTTP is connectionless:** The HTTP client, i.e., a browser initiates an HTTP request and after a request is made, the client disconnects from the server and waits for a response. The server processes the request and re-establishes the connection with the client to send a response back.
- **HTTP is media independent:** It means, any type of data can be sent by HTTP
- **HTTP is stateless:** As mentioned above, HTTP is connectionless and it is a direct result of HTTP being a stateless protocol



Network Security

- Data on the network is analogous to possessions of a person. It has to be kept secure from others with malicious intent. This intent ranges from bringing down servers on the network to using people's private information like credit card numbers to sabotage of major organizations with a presence on a network.
- To secure data, one has to ensure that it makes sense only to those for whom it is meant. This is the case for data transactions where we want to prevent eavesdroppers from listening to and stealing data.
- Other aspects of security involve protecting user data on a computer by providing password restricted access to the data and maybe some resources so that only authorized people get to use these, and identifying miscreants and thwarting their attempts to cause damage to the network among other things.

The various issues in Network security are as follows :

1. **Authentication:** We have to check that the person who has requested for something or has sent an e-mail is indeed allowed to do so. In this process we will also look at how the person authenticates his identity to a remote machine.
2. **Integrity:** We have to check that the message which we have received is indeed the message which was sent. Here CRC will not be enough because somebody may deliberately change the data. Nobody along the route should be able to change the data.
3. **Confidentiality:** Nobody should be able to read the data on the way so we need Encryption
4. **Non-repudiation:** Once we sent a message, there should be no way that we can deny sending it and we have to accept that we had sent it.
5. **Authorization:** This refers to the kind of service which is allowed for a particular client. Even though a user is authenticated we may decide not to authorize him to use a particular service.

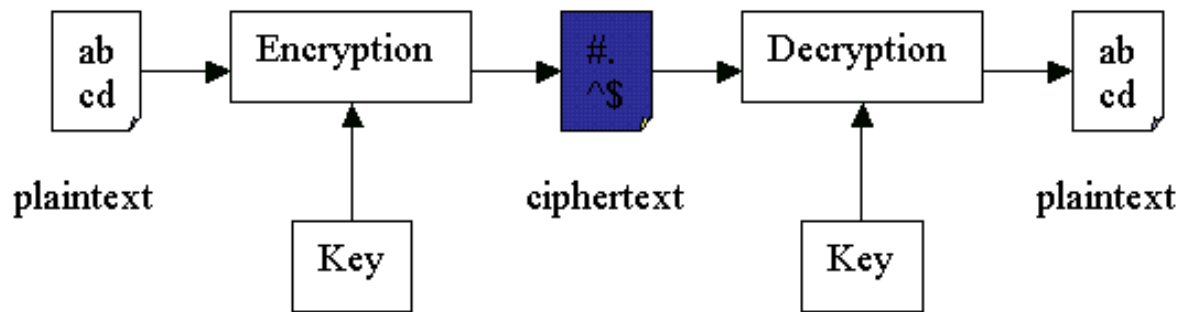
Basic concepts of public key and private key cryptography :**Common term usage:**

- **Private Key Crypto** - refers to symmetric cryptography where the one and only key must be kept private.
- **Public Key Crypto** - refers to as asymmetric cryptography because one of two keys is made public.

Symmetric Key Encryption:

- There is a single key which is shared between the two users and the same key is used for encrypting and decrypting the message. Symmetric key encryption is much faster and efficient in terms of performance. But it does not give us Non-repudiation.

- And there is a problem of how do the two sides agree on the key to be used assuming that the channel is insecure (others may snoop on our packet). In symmetric key exchange, we need some amount of public key encryption for authentication.

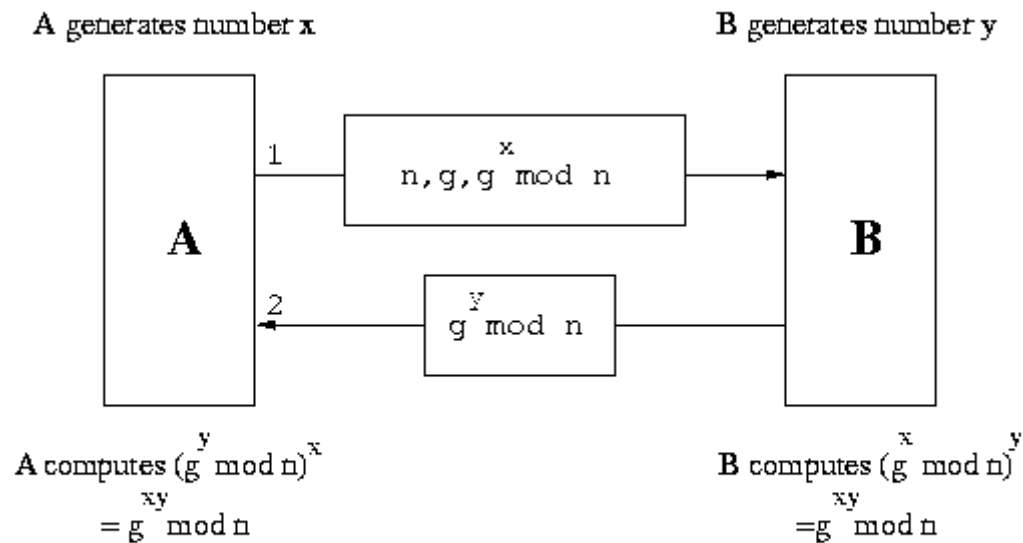


Key Exchange in Symmetric Key Schemes

Key exchange in symmetric key schemes is a tricky business because anyone snooping on the exchange can get hold of the key if we are not careful and since there is no public-private key arrangement here, he can obtain full control over the communication. There are various approaches to the foolproof exchange of keys in these schemes. We look at one approach which is as follows:-

Diffie - Hellman Key Exchange

- A and B are two persons wishing to communicate. Both of them generate a random number each, say x and y respectively. There is a function f which has no inverse. Now A sends $f(x)$ to B and B sends $f(y)$ to A. So now A knows x and $f(y)$ and B knows y and $f(x)$.
- There is another function g such that $g(x, f(y)) = g(y, f(x))$. The key used by A is $g(x, f(y))$ and that used by B is $g(y, f(x))$. Both are actually same. The implementation of this approach is described below :



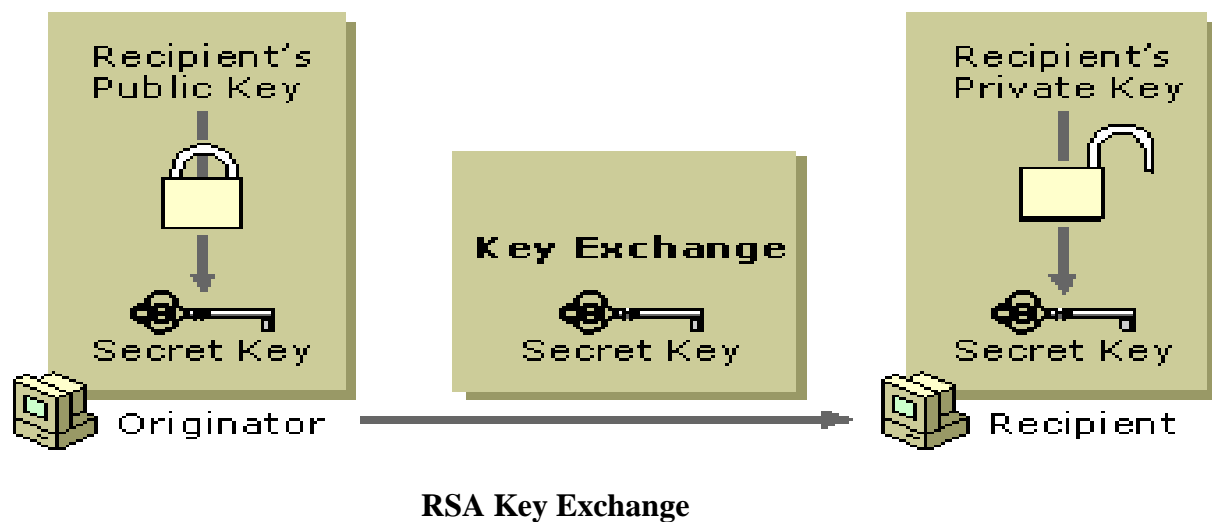
The Diffie-Hellman Key Exchange

1. A has two large prime numbers n and g . There are other conditions also that these numbers must satisfy.
2. A sends n, g and $g^x \bmod n$ to B in a message. B evaluates $(g^x \bmod n)^y$ to be used as the key.
3. B sends $g^y \bmod n$ to A. A evaluates $(g^y \bmod n)^x$ to be used as the key. So now both parties have the common number $g^{xy} \bmod n$. This is the symmetric (secret communication) key used by both A and B now.

This works because though the other people know $n, g, g^x \bmod n, g^y \bmod n$ but still they cannot evaluate the key because they do not know either x or y .

RSA Key Exchange

- The Rivest-Shamir-Adleman (RSA) algorithms available from RSA Data Security, Inc., are the most widely used public key cryptography algorithms. For RSA key exchange, secret keys are exchanged securely online by encrypting the secret key with the intended recipient's public key.
- Only the intended recipient can decrypt the secret key because it requires the use of the recipient's private key. Therefore, a third party who intercepts the encrypted, shared secret key cannot decrypt and use it.



- Digital signature
- firewalls



***i*-GATE** CS/IT (Systematic Gate Preparation)

