SKP Engineering College

Tiruvannamalai – 606611

A Course Material

on

Computer Networks

By

A.Owaise Ahmed

Assistant Professor

Computer Science and Engineering Department

Quality Certificate

This is to Certify that the Electronic Study Material

Subject Code: CS6551
Subject Name: Computer Networks
Year/Sem: III/VI

Being prepared by me and it meets the knowledge requirement of the University curriculum.

Signature of the Author

Name: A.Owaise Ahmed

Designation: Assistant Professor

This is to certify that the course material being prepared by Mr. A.Owaise Ahmed is of the adequate quality. He has referred more than five books and one among them is from abroad author.

Signature of HD	Signature of Principal
Name: K.Baskar	Name: Dr.V.Subramania Bharathi
Seal:	Seal:

CS6551 COMPUTER NETWORKS L T P C 3 0 0 3

OBJECTIVES: **The student should be made to:**

- Understand the division of network functionalities into layers.
- Be familiar with the components required to build different types of networks
- Be exposed to the required functionality at each layer
- Learn the flow control and congestion control algorithms

UNIT I FUNDAMENTALS & LINK LAYER 9

Building a network – Requirements - Layering and protocols - Internet Architecture – Network software – Performance ; Link layer Services - Framing - Error Detection - Flow control

UNIT II MEDIA ACCESS & INTERNETWORKING 9

Media access control - Ethernet (802.3) - Wireless LANs – 802.11 – Bluetooth - Switching and bridging – Basic Internetworking (IP, CIDR, ARP, DHCP,ICMP)

UNIT III ROUTING 9

Routing (RIP, OSPF, Metrics) - Switch basics - Global Internet (Areas, BGP, IPv6), Multicast -addresses - multicast routing (DVMRP, PIM)

UNIT IV TRANSPORT LAYER 9

Overview of Transport layer - UDP - Reliable byte stream (TCP) - Connection management - Flow control - Retransmission – TCP Congestion control - Congestion avoidance (DECbit,RED) – QoS – Application requirements

UNIT V APPLICATION LAYER 9

Traditional applications -Electronic Mail (SMTP, POP3, IMAP, MIME) – HTTP – Web Services – DNS - SNMP

TOTAL: 45 PERIODS

OUTCOMES: At the end of the course, the student should be able to:

- Identify the components required to build different types of networks
- Choose the required functionality at each layer for given application
- Identify solution for each functionality at each layer
- Trace the flow of information from one node to another node in the network

TEXT BOOK:

1. Larry L. Peterson, Bruce S. Davie, “Computer Networks: A systems approach”, Fifth Edition, Morgan Kaufmann Publishers, 2011.

REFERENCES:

1. James F. Kurose, Keith W. Ross, “Computer Networking - A Top-Down Approach Featuring the Internet”, Fifth Edition, Pearson Education, 2009.
2. Nader. F. Mir, “Computer and Communication Networks”, Pearson Prentice Hall

Publishers, 2010.

3. Ying-Dar Lin, Ren-Hung Hwang, Fred Baker, “Computer Networks: An Open Source Approach”, Mc Graw Hill Publisher, 2011.
4. Behrouz A. Forouzan, “Data communication and Networking”, Fourth Edition, Tata

McGraw – Hill, 2011.

CONTENTS

Prerequisite

Bachelor of Science (B.S.) programs in computer network engineering teach students the theories and methods behind designing secure connections between computers. Students learn about virtual private networks (VPNs), network routing and system development. Some programs offer specializations in internet technology or LAN networking.

Network engineering B.S. programs require incoming students to have strong math and science skills, especially in calculus and physics. Applicants should also take any available high school classes in computer science or computer programming. Most applicants also need to submit their high school transcript and scores on either the ACT or the SAT Reasoning Test.

The classes offered in computer network technology B.S. programs emphasize technical and theoretical knowledge about creating, maintaining and troubleshooting computer connections. Students learn to makes sure that only certain computers can access the networks, and that the information transferred can't be intercepted or accessed by outside computers. Classes on the following subjects are usually offered:

- Internetwork programming
- Network development
- VPN troubleshooting
- Firewall technology
- Multilayer switching

UNIT I
FUNDAMENTALS & LINK LAYER

PART-A

1. Define Computer Network. [CO1 – L1 – MAY/JUNE 2015]

Interconnected collection of autonomous computers is called computer network. This interconnection among computers facilitates information sharing among them. Computers may connect to each other by either wired or wireless media.

2. How Computer Networks are classified? [CO1 – H1]

Computer networks are classified based on various factors. They include:

- Geographical span
- Inter-connectivity
- Administration
- Architecture

3. Mention the Network Applications. [CO1 – L1]

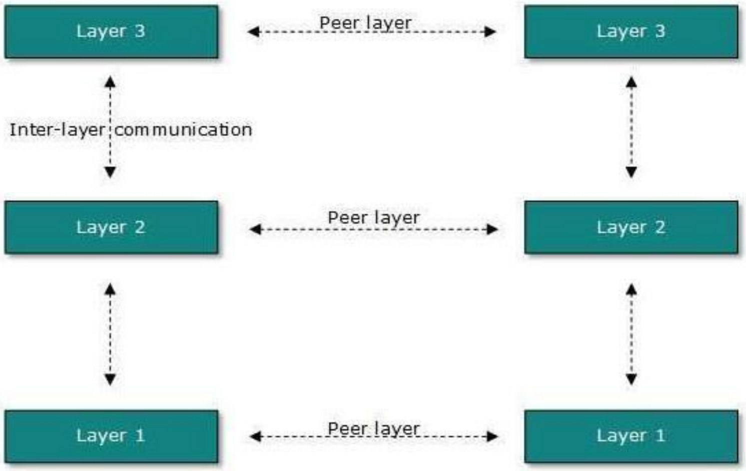
Computer systems and peripherals are connected to form a network. They provide numerous advantages:

- Resource sharing such as printers and storage devices
- Exchange of information by means of e-Mails and FTP
- Information sharing by using Web or Internet
- Interaction with other users using dynamic web pages
- IP phones
- Video conferences
- Parallel computing
- Instant messaging

4.Briefly explain Layering. [CO1 – L1]

In layered architecture of Network Model, one whole network process is divided into small tasks. Each small task is then assigned to a particular layer which works dedicatedly to process the task only. Every layer does only specific work.

In layered communication system, one layer of a host deals with the task done by or to be done by its peer layer at the same level on the remote host. The task is either initiated by layer at the lowest level or at the top most level. If the task is initiated by the-top most layer, it is passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task and passes on to lower layer. If the task is initiated by lower most layer, then the reverse path is taken.



5. What are the three criteria necessary for an effective and efficient network? [CO1 – L1]

The most important criteria are performance, reliability and security. Performance of the network depends on number of users, type of transmission medium, and the capabilities of the connected h/w and the efficiency of the s/w. Reliability is measured by frequency of failure, the time it takes a link to recover from the failure and the network's robustness in a catastrophe. Security issues include protecting data from unauthorized access and viruses.

6. Group the OSI layers by function. [CO1 – L2]

The seven layers of the OSI model belonging to three subgroups. Physical, data link and network layers are the network support layers; they deal with the physical aspects of moving data from one device to another. Session, presentation and application layers are the user support layers; they allow interoperability among unrelated software systems. The transport layer ensures end-to-end reliable data transmission.

7. What are header and trailers and how do they get added and removed? [CO1 – L1]

Each layer in the sending machine adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it. This information is added in the form of headers or trailers. Headers are added to the message at the layers 6,5,4,3, and 2. A trailer is added at layer2. At the receiving machine, the headers or trailers attached to the data unit at the corresponding sending layers are removed, and actions appropriate to that layer are taken.

8. What are the features provided by layering? [CO1 – L1]

Two nice features:

It decomposes the problem of building a network into more manageable components.
It provides a more modular design.

9. Why are protocols needed? [CO1 – L1 MAY/JUNE 2016]
In networks, communication occurs between the entities in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol. A protocol is a set of rules that govern data communication.

10. What are the two interfaces provided by protocols? [CO1 – L1]
Service interface
Peer interface

Service interface- defines the operations that local objects can perform on the protocol.
Peer interface- defines the form and meaning of messages exchanged between protocol peers to implement the communication service.

11. Mention the different physical media. [CO1 – L1]
Twisted pair(the wire that your phone connects to)
Coaxial cable(the wire that your TV connects to)
Optical fiber(the medium most commonly used for high-bandwidth, long-distance links)
Space(the stuff that radio waves, microwaves and infra red beams propagate through)

12. Define Signals. [CO1 – L1]
Signals are actually electromagnetic waves traveling at the speed of light. The speed of light is, however, medium dependent-electromagnetic waves traveling through copper and fiber do so at about two-thirds the speed of light in vacuum.

13. What is bit stuffing? [CO1 – L1]
Bit stuffing is the process of adding one extra zero whenever there are five consecutive ones so the receiver will not consider data as flag.

14. Define Modulation. [CO1 – L1]
Modulation -varying the frequency, amplitude or phase of the signal to effect the transmission of information. A simple example of modulation is to vary the power (amplitude) of a single wavelength.

15. Explain the two types of duplex. [CO1 – L2]
Full duplex-two bit streams can be simultaneously transmitted over the links at the same time, one going in each direction.
Half duplex-it supports data flowing in only one direction at a time.

16. What is CODEC? [CO1 – L1]
A device that encodes analog voice into a digital ISDN link is called a CODEC, for coder/decoder.

17. What is spread spectrum and explain the two types of spread spectrum? [CO1 – L1]

Spread spectrum is to spread the signal over a wider frequency band than normal in such a way as to minimize the impact of interference from other devices.

Frequency Hopping
Direct sequence

18. What are the different encoding techniques? [CO1 – L1]

NRZ
NRZI
Manchester
4B/5B

19. How does NRZ-L differ from NRZ-I? [CO1 – L1]

In the NRZ-L sequence, positive and negative voltages have specific meanings: positive for 0 and negative for 1. In the NRZ-I sequence, the voltages are meaningless. Instead, the receiver looks for changes from one level to another as its basis for recognition of 1s.

20. What are the responsibilities of data link layer? [CO1 – L1]

Specific responsibilities of data link layer include the following. a) Framing b) Physical addressing c) Flow control d) Error control e) Access control.

21. What are the ways to address the framing problem? [CO1 – L1]

Byte-Oriented Protocols(PPP)
Bit-Oriented Protocols(HDLC)
Clock-Based Framing(SONET)

22. Distinguish between peer-to-peer relationship and a primary-secondary relationship? [CO1 – H1]

Peer-to-peer relationship: All the devices share the link equally. Primary-secondary relationship: One device controls traffic and the others must transmit through it.

23. Mention the types of errors and define the terms. [CO1 – L1]

Single-bit error.
Burst-bit error.
Single bit error: The term single bit error means that only one bit of a given data unit (such as byte character/data unit or packet) is changed from 1 to 0 or from 0 to 1.
Burst error: Means that 2 or more bits in the data unit have changed from 1 to 0 from 0 to 1.

24. List out the available detection methods. [CO1 – L1 MAY/JUNE 2016]

There are 4 types of redundancy checks are used in data communication.
Vertical redundancy checks (VRC).
Longitudinal redundancy checks (LRC).
Cyclic redundancy checks (CRC).
Checksum.

25. Write short notes on VRC. [CO1 – H3]

The most common and least expensive mechanism for error detection is the vertical redundancy check (VRC) often called a parity check. In this technique a redundant bit called a parity bit, is appended to every data unit so, that the total number of 0‟s in the unit (including the parity bit) becomes even.

26. Write short notes on LRC. [CO1 – H3]

In longitudinal redundancy check (LRC), a block of bits is divided into rows and a redundant row of bits is added to the whole block.

27. Write short notes on CRC. [CO1 – H3]

The third and most powerful of the redundancy checking techniques is the cyclic redundancy checks (CRC) CRC is based on binary division. Here a sequence of redundant bits, called the CRC remainder is appended to the end of data unit.

28. Write short notes on CRC checker. [CO1 – H3]

A CRC checker functions exactly like a generator. After receiving the data appended with the CRC it does the same modulo-2 division. If the remainder is all 0s the CRC is dropped and the data accepted. Otherwise, the received stream of bits is discarded and the dates are resent.

29. Define checksum. [CO1 – L1]

The error detection method used by the higher layer protocol is called checksum. Checksum is based on the concept of redundancy.

30. What are the steps followed in checksum generator? [CO1 – L1]

The sender follows these steps a) the units are divided into k sections each of n bits. b) All sections are added together using 2‟s complement to get the sum. c) The sum is complemented and become the checksum. d) The checksum is sent with the data.

31. Mention the types of error correcting methods. [CO1 – L1]

There are 2 error-correcting methods.

Single bit error correction

Burst error correction.

32. Write short notes on error correction? [CO1 – H3]

It is the mechanism to correct the errors and it can be handled in 2 ways.

When an error is discovered, the receiver can have the sender retransmit the entire data unit.

A receiver can use an error correcting coder, which automatically corrects certain errors.

33. What is the purpose of hamming code? [CO1 – L1]

A hamming code can be designed to correct burst errors of certain lengths. So the simple strategy used by the hamming code to correct single bit errors must be redesigned to be applicable for multiple bit correction.

34. What is redundancy? [CO1 – L1]

It is the error detecting mechanism, which means a shorter group of bits or extra bits may be appended at the destination of each unit.

35. Define flow control. [CO1 – L1]

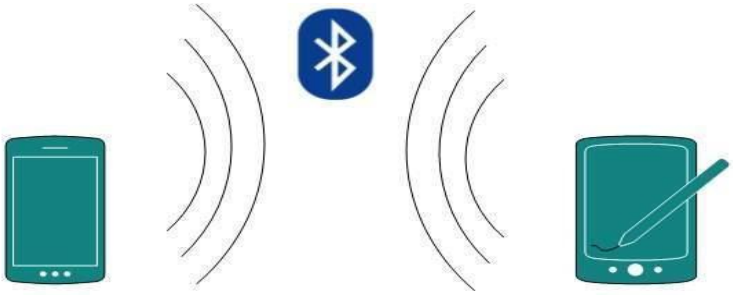
Flow control refers to a set of procedures used to restrict the amount of data.
It answers the question how much data sender can send before waiting for acknowledgment.

PART-B

1. EXPLAIN THE CATEGORIES OF COMPUTER NETWORK. [CO1 – L2 NOV/DEC 2015]

Personal Area Network

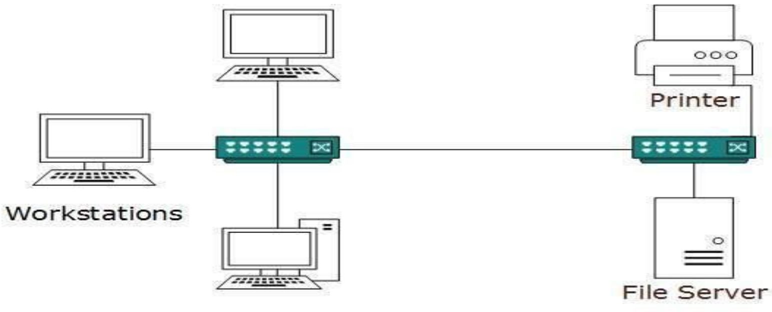
A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes.



For example, Piconet is Bluetooth-enabled Personal Area Network which may contain up to 8 devices connected together in a master-slave fashion.

Local Area Network

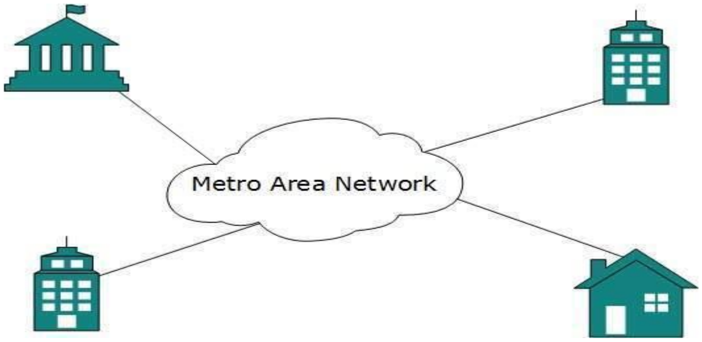
A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). Usually, LAN covers an organization' offices, schools, colleges or universities. LAN provides a useful way of sharing the resources between end users. The resources such as printers, file servers, scanners, and internet are easily sharable among computers.



LANs are composed of inexpensive networking and routing equipment. It may contain local servers serving file storage and other locally shared applications. It mostly operates on private IP addresses and does not involve heavy routing. LAN works under its own local domain and controlled centrally. LAN uses either Ethernet or Token-ring technology. Ethernet is most widely employed LAN technology and uses Star topology, while Token-ring is rarely seen.LAN can be wired, wireless, or in both forms at once.

Metropolitan Area Network

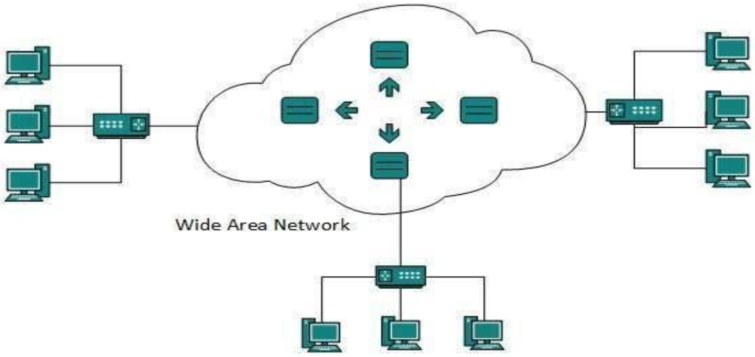
The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city.



Backbone of MAN is high-capacity and high-speed fiber optics. MAN works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or internet.

Wide Area Network

As the name suggests, the Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provide connectivity to MANs and LANs. Since they are equipped with very high speed backbone, WANs use very expensive network equipment.



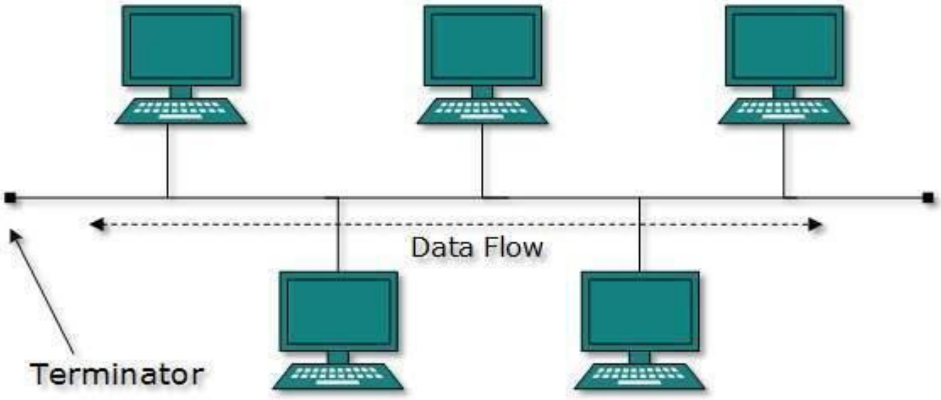
WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET). WAN may be managed by multiple administrations.

2. EXPLAIN NETWORK TOPOLOGIES. [CO1 – L2 NOV/DEC 2015]

A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

Bus Topology

In case of Bus topology, all devices share single communication line or cable. Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.

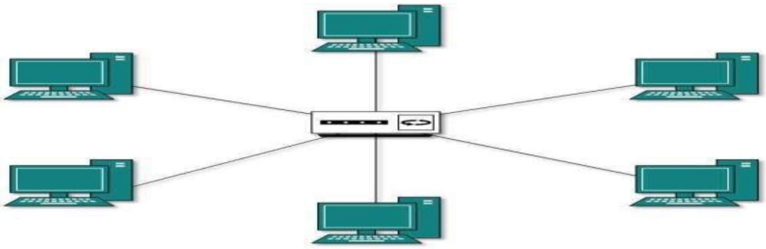


Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

Star Topology

All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

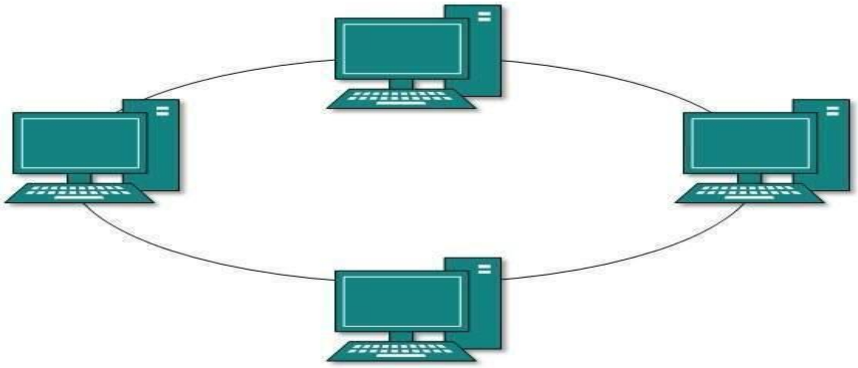
Layer-1 device such as hub or repeater
Layer-2 device such as switch or bridge
Layer-3 device such as router or gateway



As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. Every communication between hosts, takes place through only the hub. Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

Ring Topology

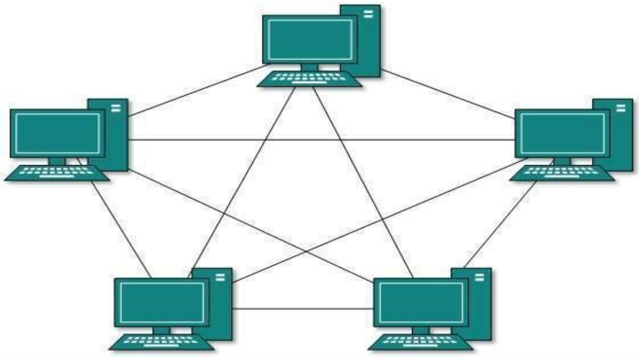
In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.



Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.

Mesh Topology

In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.



Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

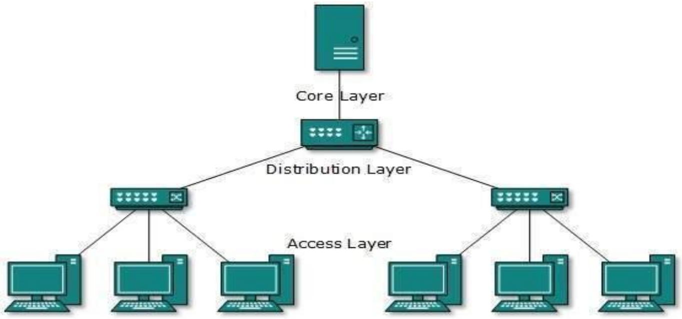
Full Mesh: All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.

Partially Mesh: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

Tree Topology

Also known as Hierarchical Topology, this is the most common form of network topology in use presently. This topology imitates as extended Star topology and inherits properties of bus topology.

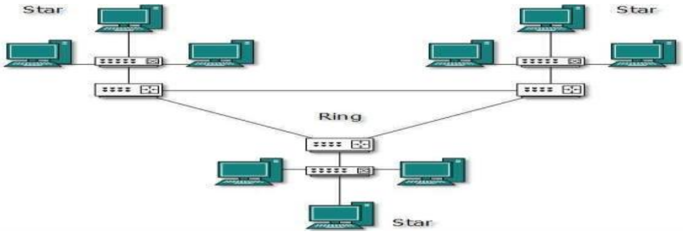
This topology divides the network in to multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices. The lowermost is access-layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.



All neighboring hosts have point-to-point connection between them. Similar to the Bus topology, if the root goes down, then the entire network suffers even though it is not the single point of failure. Every connection serves as point of failure, failing of which divides the network into unreachable segment.

Hybrid Topology

A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.



The above picture represents an arbitrarily hybrid topology. The combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies. Most WANs are connected by means of Dual-Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology

3. EXPLAIN VARIOUS TRANSMISSION MEDIA. [CO1 – L2]

The media, over which the information between two computer systems is sent, called transmission media. Transmission media comes in two forms.

Guided Media

All communication wires/cables are guided media, such as UTP, coaxial cables, and fibre Optics. In this media, the sender and receiver are directly connected and the information is send (guided) through it. Ex. Twisted pair, Coaxial Cable, Fibre Optics

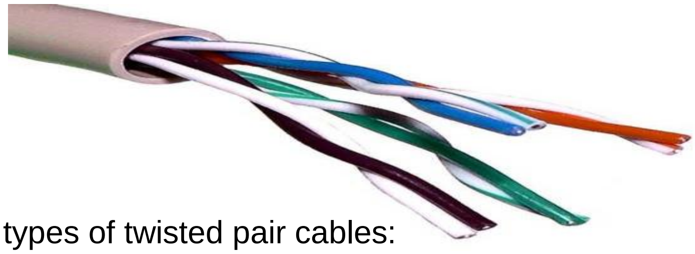
Unguided Media

Wireless or open air space is said to be unguided media, because there is no connectivity between the sender and receiver. Information is spread over the air, and anyone including the actual recipient may collect the information. Ex. Satellite Communication.

Guided Media

Twisted Pair Cable

A twisted pair cable is made of two plastic insulated copper wires twisted together to form a single media. Out of these two wires, only one carries actual signal and another is used for ground reference. The twists between wires are helpful in reducing noise (electro-magnetic interference) and crosstalk.



There are two types of twisted pair cables:

Shielded Twisted Pair (STP) Cable

Unshielded Twisted Pair (UTP) Cable

STP cables comes with twisted wire pair covered in metal foil. This makes it more indifferent to noise and crosstalk.

UTP has seven categories, each suitable for specific use. In computer networks, Cat-5, Cat-5e, and Cat-6 cables are mostly used. UTP cables are connected by RJ45 connectors.

Coaxial Cable

Coaxial cable has two wires of copper. The core wire lies in the centre and it is made of solid conductor. The core is enclosed in an insulating sheath. The second wire is wrapped around over the sheath and that too in turn encased by insulator sheath. This all is covered by plastic cover.

Because of its structure, the coax cable is capable of carrying high frequency signals than that of twisted pair cable. The wrapped structure provides it a good shield against noise and cross talk. Coaxial cables provide high bandwidth rates of up to 450 mbps.

There are three categories of coax cables namely, RG-59 (Cable TV), RG-58 (Thin Ethernet), and RG-11 (Thick Ethernet). RG stands for Radio Government.

Cables are connected using BNC connector and BNC-T. BNC terminator is used to terminate the wire at the far ends.

Power Lines

Power Line communication (PLC) is Layer-1 (Physical Layer) technology which uses power cables to transmit data signals. In PLC, modulated data is sent over the cables. The receiver on the other end de-modulates and interprets the data.

Because power lines are widely deployed, PLC can make all powered devices controlled and monitored. PLC works in half-duplex.

There are two types of PLC:

Narrow band PLC

Broad band PLC

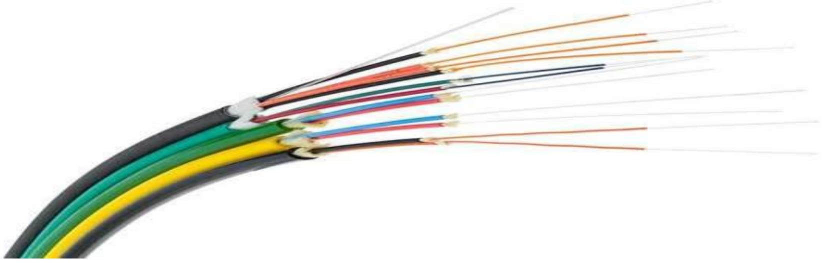
Narrow band PLC provides lower data rates up to 100s of kbps, as they work at lower frequencies (3-5000 kHz).They can be spread over several kilometres.

Broadband PLC provides higher data rates up to 100s of Mbps and works at higher frequencies (1.8 – 250 MHz).They cannot be as much extended as Narrowband PLC.

Fiber Optics

Fiber Optic works on the properties of light. When light ray hits at critical angle it tends to refracts at 90 degree. This property has been used in fiber optic. The core of fiber optic cable is made of high quality glass or plastic. From one end of it light is emitted, it travels through it and at the other end light detector detects light stream and converts it to electric data.

Fiber Optic provides the highest mode of speed. It comes in two modes, one is single mode fiber and second is multimode fiber. Single mode fiber can carry a single ray of light whereas multimode is capable of carrying multiple beams of light.



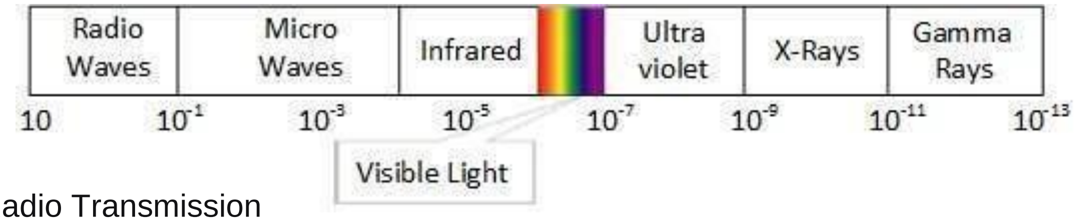
Fiber Optic also comes in unidirectional and bidirectional capabilities. To connect and access fiber optic special type of connectors are used. These can be Subscriber Channel (SC), Straight Tip (ST), or MT-RJ.

Unguided (Wireless Transmission)

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

A little part of electromagnetic spectrum can be used for wireless transmission.



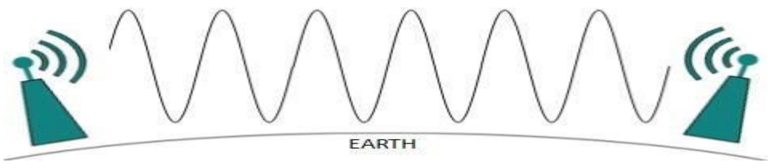
Radio Transmission

Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and structures alike. Radio waves can have wavelength from 1mm– 100,000 km and have frequency ranging from 3 Hz (Extremely Low Frequency) to 300 GHz (Extremely High Frequency). Radio frequencies are sub-divided into six bands.

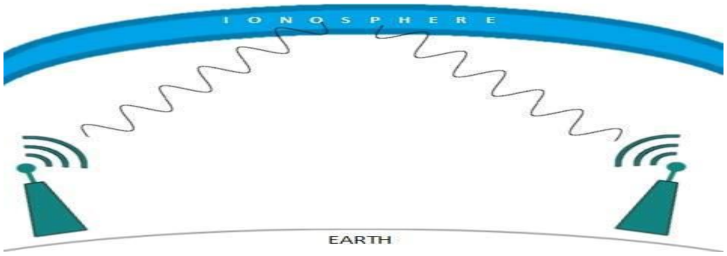
Radio waves at lower frequencies can travel through walls whereas higher RF can travel in straight line and bounce back.

The power of low frequency waves decreases sharply as they cover long distance. High frequency radio waves have more power.

Lower frequencies such as VLF, LF, MF bands can travel on the ground up to 1000 kilometers, over the earth's surface.



Radio waves of high frequencies are prone to be absorbed by rain and other obstacles. They use Ionosphere of earth atmosphere. High frequency radio waves such as HF and VHF bands are spread upwards. When they reach Ionosphere, they are refracted back to the earth.



Microwave Transmission

Electromagnetic waves above 100 MHz tend to travel in a straight line and signals over them can be sent by beaming those waves towards one particular station. Because Microwaves travels in straight lines, both sender and receiver must be aligned to be strictly in line-of-sight.

Microwaves can have wavelength ranging from 1 mm – 1 meter and frequency ranging from 300 MHz to 300 GHz.

Microwave antennas concentrate the waves making a beam of it. As shown in picture above, multiple antennas can be aligned to reach farther. Microwaves have higher frequencies and do not penetrate wall like obstacles.

Microwave transmission depends highly upon the weather conditions and the frequency it is using.

Infrared Transmission

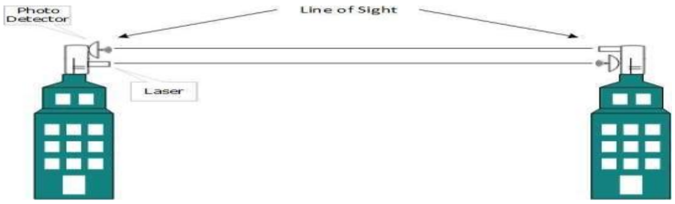
Infrared wave lies in between visible light spectrum and microwaves. It has wavelength of 700-nm to 1-mm and frequency ranges from 300-GHz to 430-THz.

Infrared wave is used for very short range communication purposes such as television and it’s remote. Infrared travels in a straight line hence it is directional by nature. Because of high frequency range, Infrared cannot cross wall-like obstacles.

Light Transmission

Highest most electromagnetic spectrum which can be used for data transmission is light or optical signaling. This is achieved by means of LASER.

Because of frequency light uses, it tends to travel strictly in straight line.Hence the sender and receiver must be in the line-of-sight. Because laser transmission is unidirectional, at both ends of communication the laser and the photo-detector needs to be installed. Laser beam is generally 1mm wide hence it is a work of precision to align two far receptors each pointing to lasers source.



Laser works as Tx (transmitter) and photo-detectors works as Rx (receiver).

Lasers cannot penetrate obstacles such as walls, rain, and thick fog. Additionally, laser beam is distorted by wind, atmosphere temperature, or variation in temperature in the path.

Laser is safe for data transmission as it is very difficult to tap 1mm wide laser without interrupting the communication channel.

Multiplexing

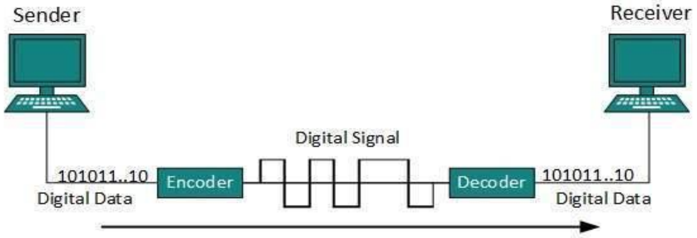
Multiplexing is a technique to mix and send multiple data streams over a single medium. This technique requires system hardware called multiplexer (MUX) for multiplexing the streams and sending them on a medium, and de-multiplexer (DMUX) which takes information from the medium and distributes to different destinations.

4. EXPLAIN VARIOUS ENCODING METHODS IN DETAIL. [CO1 – L2] Digital-to-Digital Conversion

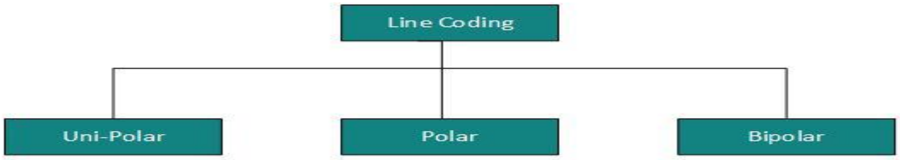
This section explains how to convert digital data into digital signals. It can be done in two ways, line coding and block coding. For all communications, line coding is necessary whereas block coding is optional.

Line Coding

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format. It is represented (stored) internally as series of 1s and 0s.



Digital signal is denoted by discreet signal, which represents digital data. There are three types of line coding schemes available:



Uni-polar Encoding

Unipolar encoding schemes use single voltage level to represent data. In this case, to represent binary 1, high voltage is transmitted and to represent 0, no voltage is transmitted. It is also called Unipolar-Non-return-to-zero, because there is no rest condition i.e. it either represents 1 or 0.

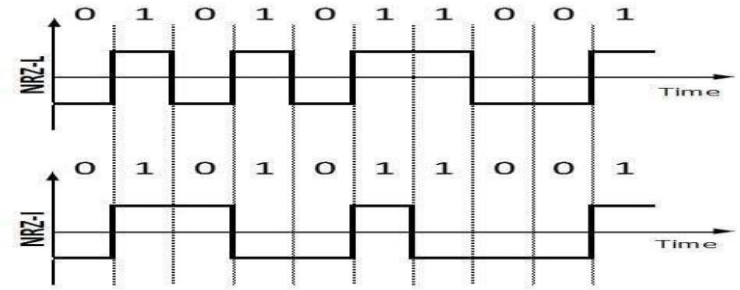
Polar Encoding

Polar encoding scheme uses multiple voltage levels to represent binary values. Polar encodings is available in four types:

Polar Non-Return to Zero (Polar NRZ)

It uses two different voltage levels to represent binary values. Generally, positive voltage represents 1 and negative value represents 0. It is also NRZ because there is no rest condition.

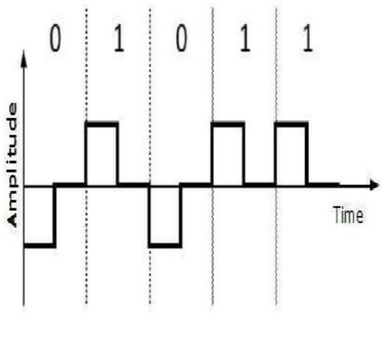
NRZ scheme has two variants: NRZ-L and NRZ-I.



NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I changes voltage when a 1 is encountered.

Return to Zero (RZ)

Problem with NRZ is that the receiver cannot conclude when a bit ended and when the next bit is started, in case when sender and receiver's clock are not synchronized.



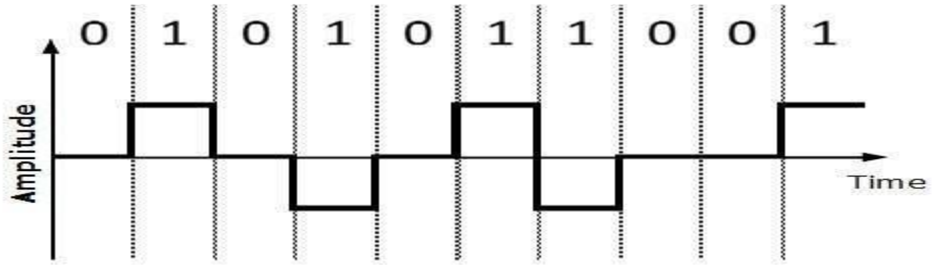
RZ uses three voltage levels, positive voltage to represent 1, negative voltage to represent 0 and zero voltage for none. Signals change during bits not between bits.

Manchester

This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transits in the middle of the bit and changes phase when a different bit is encountered.

Differential Manchester
This encoding scheme is a combination of RZ and NRZ-I. It also transit at the middle of the bit but changes phase only when 1 is encountered.

Bipolar Encoding
Bipolar encoding uses three voltage levels, positive, negative and zero. Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.



Block Coding
To ensure accuracy of the received data frame redundant bits are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even. This way the original number of bits is increased. It is called Block Coding.
Block coding is represented by slash notation, mB/nB.Means, m-bit block is substituted with n-bit block where n > m. Block coding involves three steps:

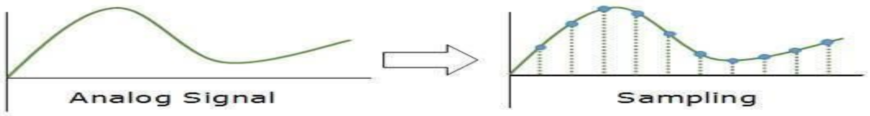
Division,
Substitution
Combination.

After block coding is done, it is line coded for transmission.

Analog-to-Digital Conversion
Microphones create analog voice and camera creates analog videos, which are treated is analog data. To transmit this analog data over digital signals, we need analog to digital conversion.

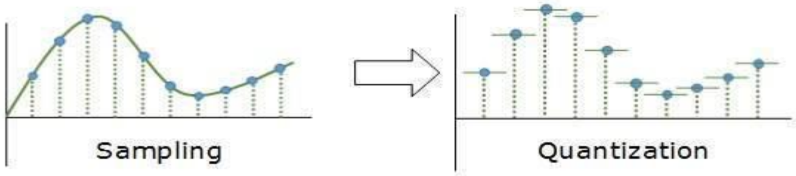
Analog data is a continuous stream of data in the wave form whereas digital data is discrete. To convert analog wave into digital data, we use Pulse Code Modulation (PCM).PCM is one of the most commonly used methods to convert analog data into digital form. It involves three steps:
Sampling
Quantization
Encoding.

Sampling



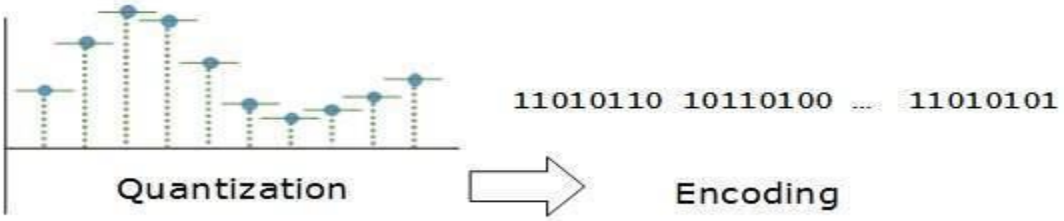
The analog signal is sampled every T interval. Most important factor in sampling is the rate at which analog signal is sampled. According to Nyquist Theorem, the sampling rate must be at least two times of the highest frequency of the signal.

Quantization



Sampling yields discrete form of continuous analog signal. Every discrete pattern shows the amplitude of the analog signal at that instance. The quantization is done between the maximum amplitude value and the minimum amplitude value. Quantization is approximation of the instantaneous analog value.

Encoding



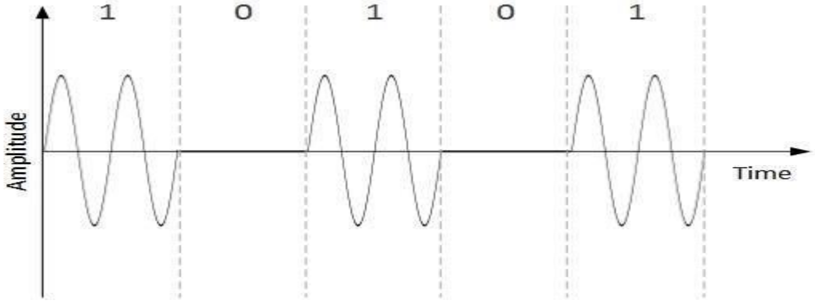
In encoding, each approximated value is then converted into binary format.

Digital-to-Analog Conversion

When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data. An analog signal is characterized by its amplitude, frequency, and phase. There are three kinds of digital-to-analog conversions:

Amplitude Shift Keying

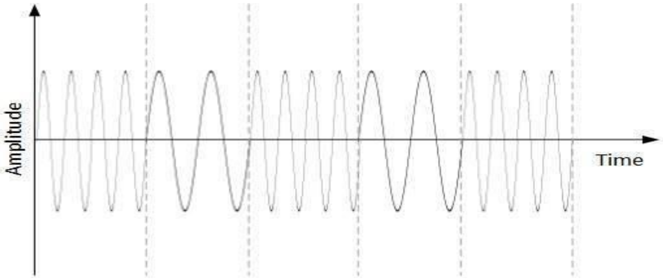
In this conversion technique, the amplitude of analog carrier signal is modified to reflect binary data.



When binary data represents digit 1, the amplitude is held; otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal.

Frequency Shift Keying

In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data.



This technique uses two frequencies, f1 and f2. One of them, for example f1, is chosen to represent binary digit 1 and the other one is used to represent binary digit 0. Both amplitude and phase of the carrier wave are kept intact.

Phase Shift Keying

In this conversion scheme, the phase of the original carrier signal is altered to reflect the binary data.

When a new binary symbol is encountered, the phase of the signal is altered.

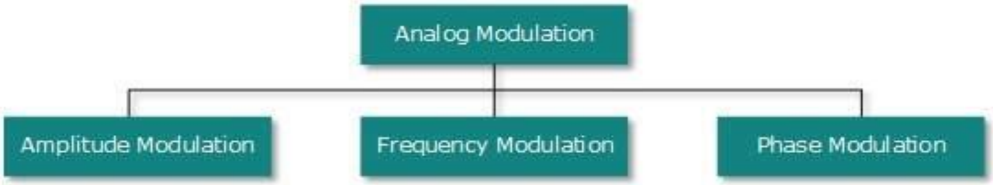
Amplitude and frequency of the original carrier signal is kept intact.

Quadrature Phase Shift Keying

QPSK alters the phase to reflect two binary digits at once. This is done in two different phases. The main stream of binary data is divided equally into two sub-streams. The serial data is converted in to parallel in both sub-streams and then each stream is converted to digital signal using NRZ technique. Later, both the digital signals are merged together.

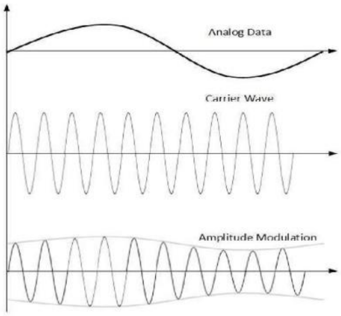
Analog-to-Analog Conversion

Analog signals are modified to represent analog data. This conversion is also known as Analog Modulation. Analog modulation is required when bandpass is used. Analog to analog conversion can be done in three ways:



Amplitude Modulation

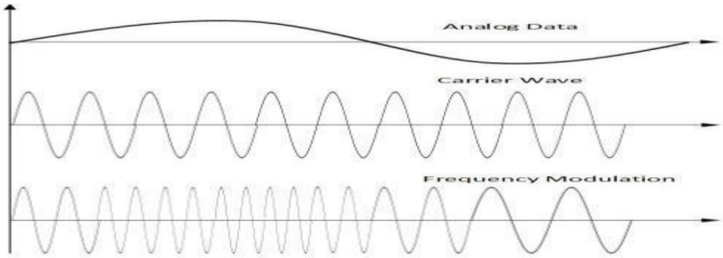
In this modulation, the amplitude of the carrier signal is modified to reflect the analog data.



Amplitude modulation is implemented by means of a multiplier. The amplitude of modulating signal (analog data) is multiplied by the amplitude of carrier frequency, which then reflects analog data.The frequency and phase of carrier signal remain unchanged.

Frequency Modulation

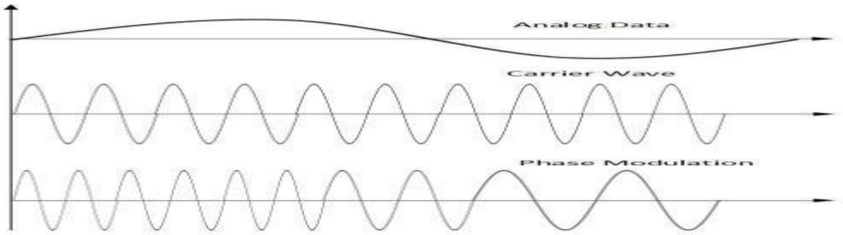
In this modulation technique, the frequency of the carrier signal is modified to reflect the change in the voltage levels of the modulating signal (analog data).



The amplitude and phase of the carrier signal are not altered.

Phase Modulation

In the modulation technique, the phase of carrier signal is modulated in order to reflect the change in voltage (amplitude) of analog data signal.



Phase modulation is practically similar to Frequency Modulation, but in Phase modulation frequency of the carrier signal is not increased. Frequency of carrier is signal is changed (made dense and sparse) to reflect voltage change in the amplitude of modulating signal.

5. EXPLAIN VARIOUS MULTIPLEXING TECHNIQUES. [CO1 – L2]

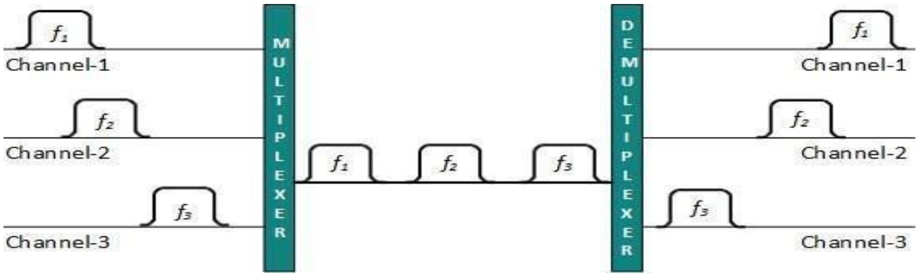
Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.

Communication is possible over the air (radio frequency), using a physical media (cable), and light (optical fiber). All mediums are capable of multiplexing.

When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium, identifies each, and sends to different receivers.

Frequency Division Multiplexing

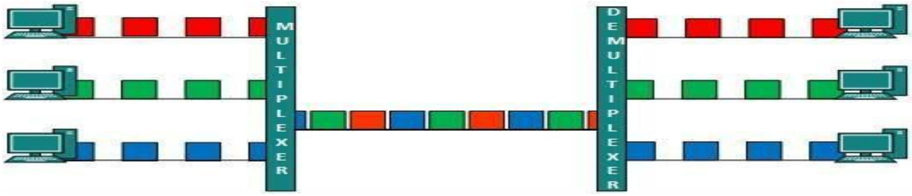
When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.



Time Division Multiplexing

TDM is applied primarily on digital signals but can be applied on analog signals as well. In TDM the shared channel is divided among its user by means of time slot. Each user can transmit data within the provided time slot only. Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.

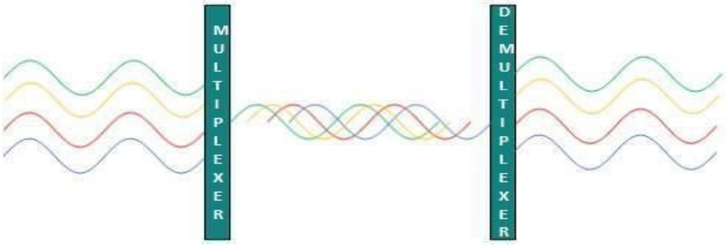
TDM works in synchronized mode. Both ends, i.e. Multiplexer and De-multiplexer are timely synchronized and both switch to next channel simultaneously.



When channel A transmits its frame at one end, the De-multiplexer provides media to channel A on the other end. As soon as the channel A's time slot expires, this side switches to channel B. On the other end, the De-multiplexer works in a synchronized manner and provides media to channel B. Signals from different channels travel the path in interleaved manner.

Wavelength Division Multiplexing:

Light has different wavelength (colors). In fiber optic mode, multiple optical carrier signals are multiplexed into an optical fiber by using different wavelengths. This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.



Further, on each wavelength time division multiplexing can be incorporated to accommodate more data signals.

Code Division Multiplexing

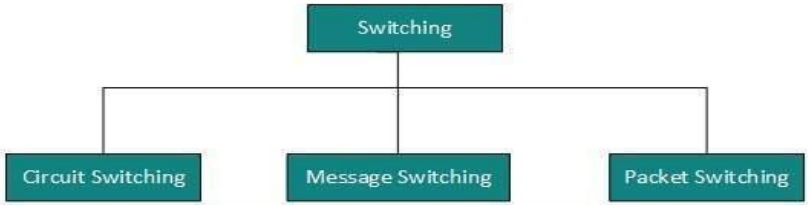
Multiple data signals can be transmitted over a single frequency by using Code Division Multiplexing. FDM divides the frequency in smaller channels but CDM allows its users to full bandwidth and transmit signals all the time using a unique code. CDM uses orthogonal codes to spread signals.

Each station is assigned with a unique code, called chip. Signals travel with these codes independently, inside the whole bandwidth. The receiver knows in advance the chip code signal it has to receive.

6. EXPLAIN SWITCHING METHODS IN DETAIL. [CO1 – L2]

Switching is a mechanism by which data/information sent from source towards destination which are not directly connected. Networks have interconnecting devices, which receives data from directly connected sources, stores data, analyze it and then forwards to the next interconnecting device closest to the destination.

Switching can be categorized as:



At broad level, switching can be divided into two major categories:
Connectionless: The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.

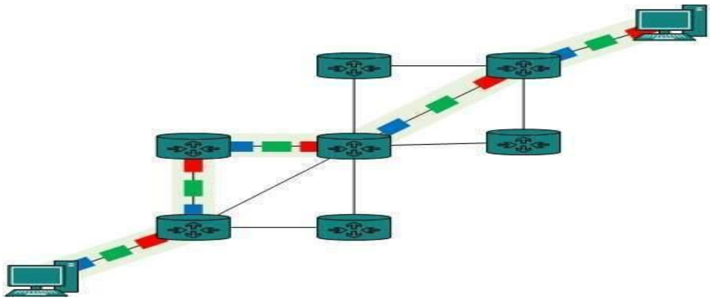
Connection Oriented: Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

Circuit Switching

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There 'is a need of pre-specified route from which data will travel and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.

Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:

Establish a circuit
Transfer the data
Disconnect the circuit



Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and called is established over the network.

Packet Switching

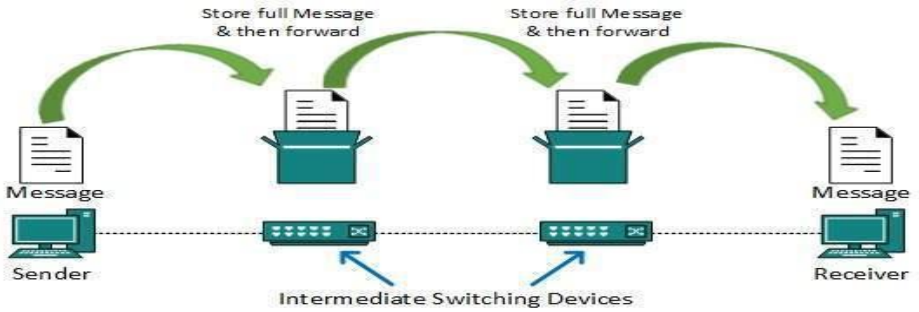
Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.

It is easier for intermediate networking devices to store small size packets and they do not take many resources either on carrier path or in the internal memory of switches.
Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

Message Switching

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.

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

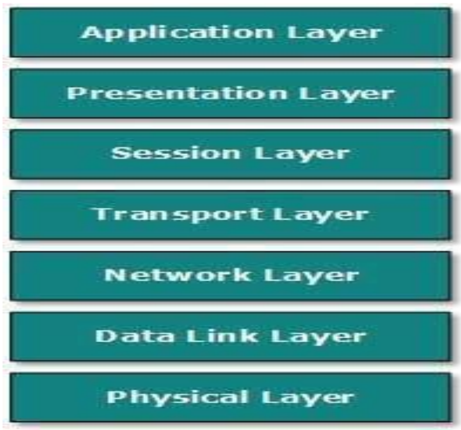

Store full Message & then forward
Store full Message & then forward
Message
Message
Sender
Receiver
Intermediate Switching Devices

This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching. Message switching has the following drawbacks:

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

7. DISCUSS IN DETAIL ABOUT THE LAYERS OF OSI MODEL WITH A NEAT DIAGRAM. [CO1 – H1 MAY/JUNE 2016]

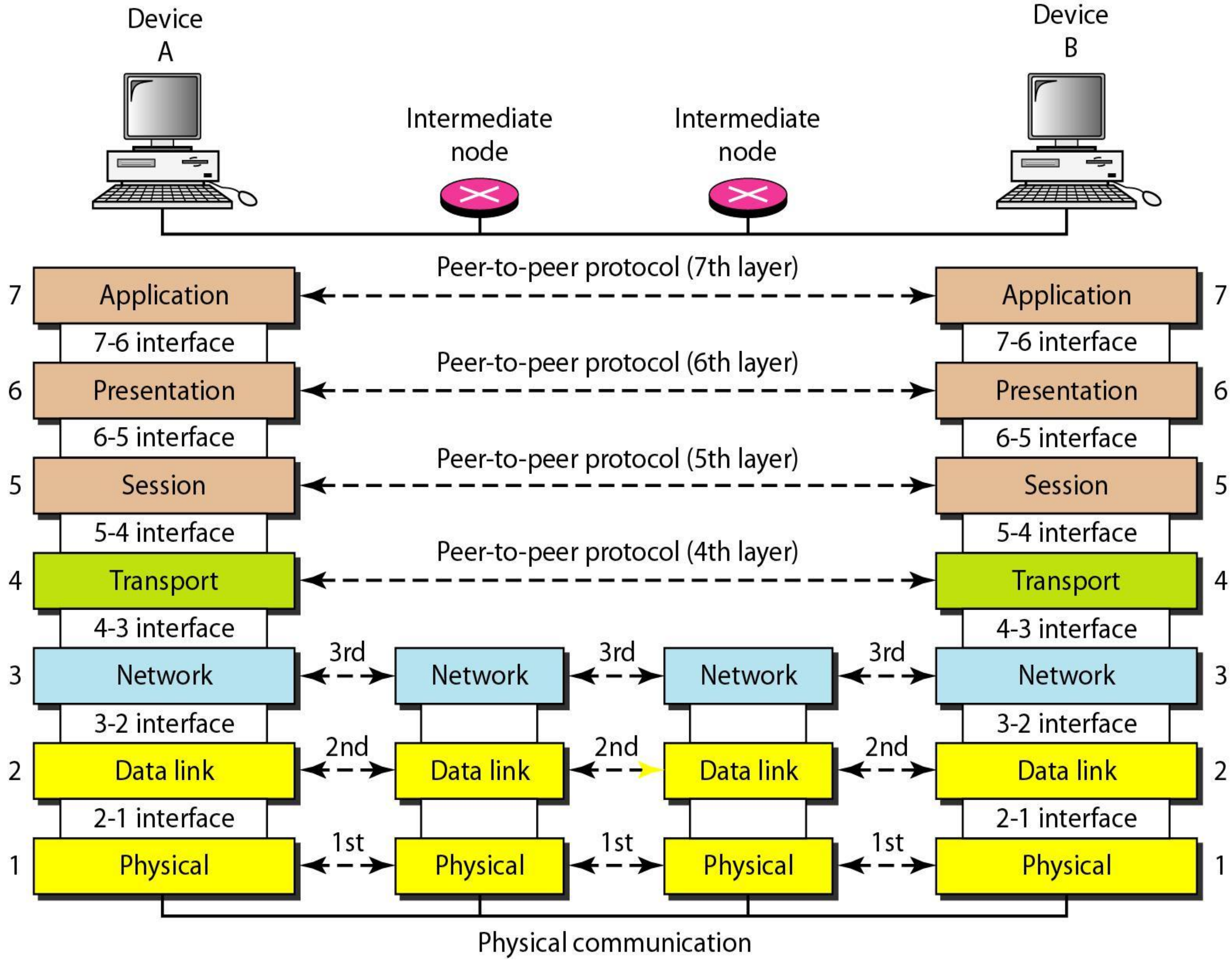
Open System Interconnect is an open standard for all communication systems. OSI model is established by International Standard Organization (ISO). This model has seven layers:



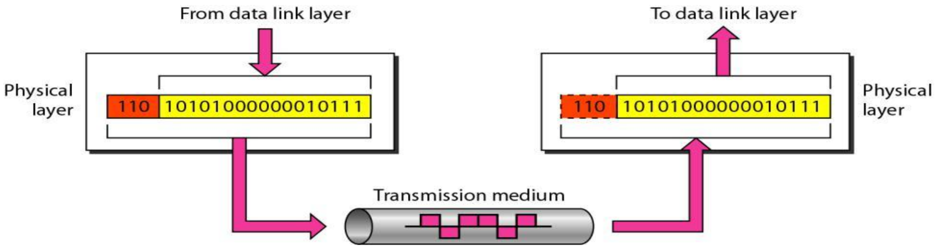
Application Layer: This layer is responsible for providing interface to the application user. This layer encompasses protocols which directly interact with the user.

Presentation Layer: This layer defines how data in the native format of remote host should be presented in the native format of host.

Session Layer: This layer maintains sessions between remote hosts. For example, once user/password authentication is done, the remote host maintains this session for a while and does not ask for authentication again in that time span.
Transport Layer: This layer is responsible for end-to-end delivery between hosts.
Network Layer: This layer is responsible for address assignment and uniquely addressing hosts in a network.
Data Link Layer: This layer is responsible for reading and writing data from and onto the line. Link errors are detected at this layer.
Physical Layer: This layer defines the hardware, cabling wiring, power output, pulse rate etc.

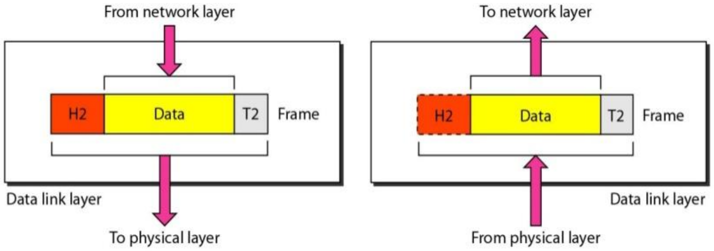


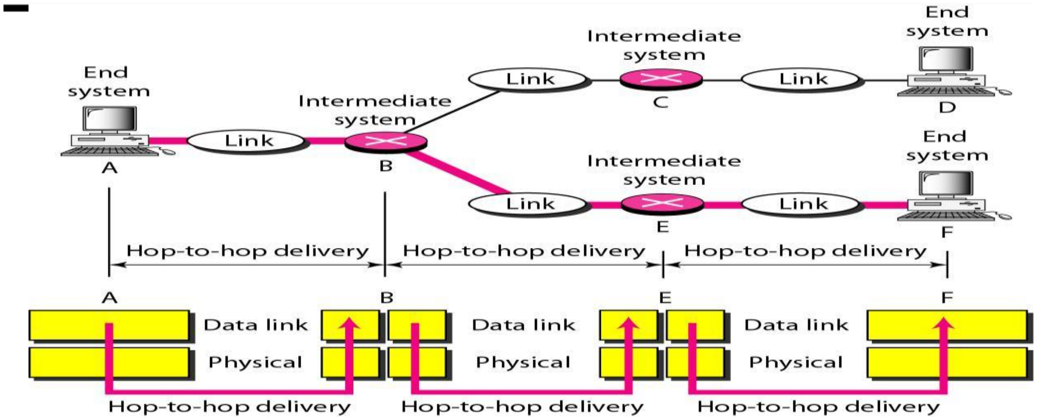
Physical Layer



It coordinates the functions required to carry a bit stream over a physical medium.
Encoding—To be transmitted, bits must be encoded into signals, electrical or optical.
Data rate—It defines the transmission rate (number of bits sent per second).
Physical topology—It defines how devices are connected (mesh, star, ring, bus or hybrid)
Transmission mode defines the direction of transmission between two devices: Simplex, half-duplex, or full-duplex

Data Link Layer

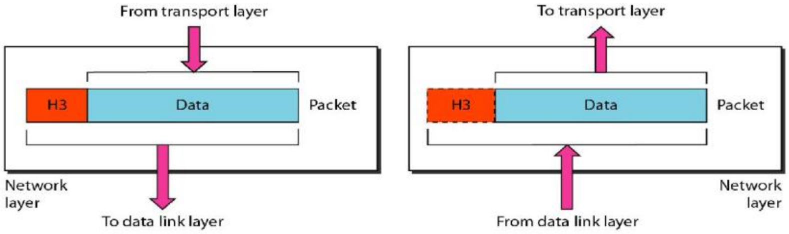


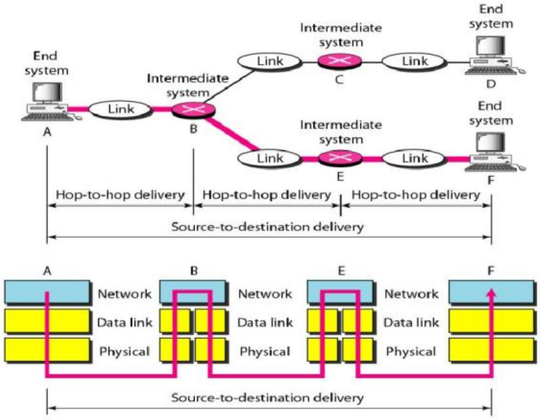


The data link layer transforms a raw transmission facility to a reliable link.
Framing—The bit stream is divided into manageable data units called frames.
Physical addressing—Header contains physical address of sender and receiver
Flow control—If receiving rate is less than the transmission rate, flow control mechanism avoids sender overwhelming the receiver.
Error control—Redundant information is put as trailer to detect and retransmit damaged/lost frames and to recognize duplicate frames.

Access control—When two or more devices are connected to the same link, link layer protocols determines which device has control over the link at any given time.

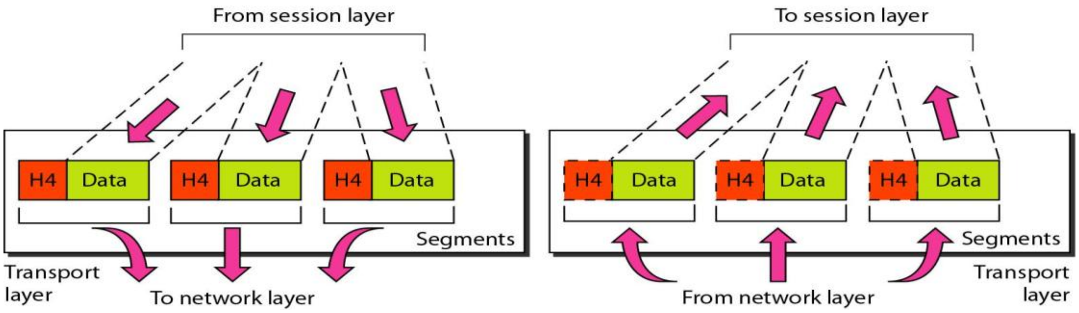
Network Layer





It is responsible for source-to-destination delivery of a data unit called *packet*.
Logical addressing—A packet is identified across the network using logical addressing system provided by network layer and is used to identify the end systems.
Routing—Routers prepare routing table to send packets to their destination.

Transport Layer
Transport layer is responsible for *process-to-process* delivery of the entire message.

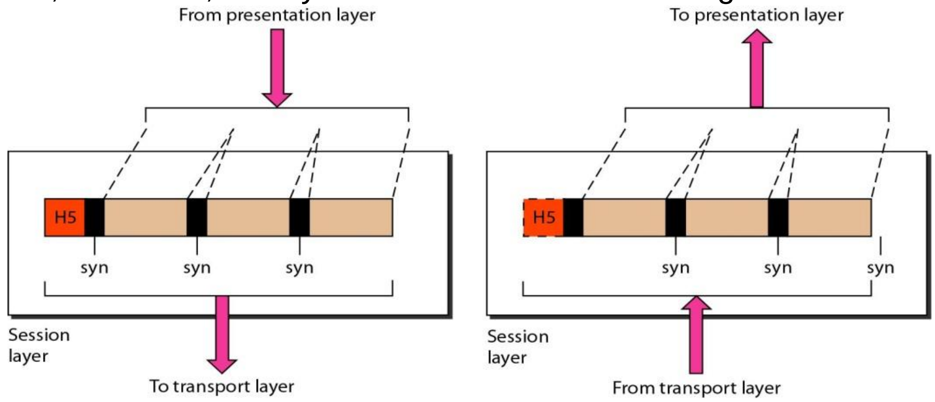


Port addressing—It includes a service-point or *port* address so that a process from one computer communicates to a specific process on the other computer.

Segmentation and reassembly—A message is divided into transmittable *segments*, each containing a sequence number. These numbers enable the transport layer to reassemble the message correctly at the destination and to identify which were lost / corrupted. *Connection control*—Protocols can be either connectionless or connection-oriented.

Session Layer

It establishes, maintains, and synchronizes interaction among communicating systems.



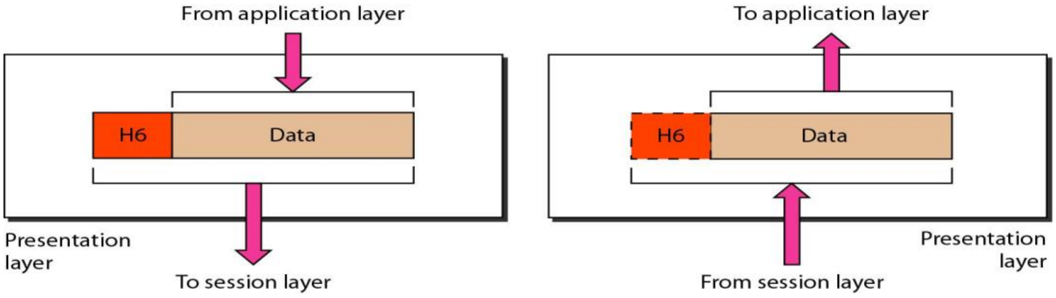
Dialog control—It allows two systems to enter into a dialog and communicate

Synchronization—allows adding checkpoints to a stream of data. In case of a crash data is retransmitted from the last checkpoint.

Binding—binds together the different streams that are part of a single application. For example, audio and video stream are combined in a teleconferencing application.

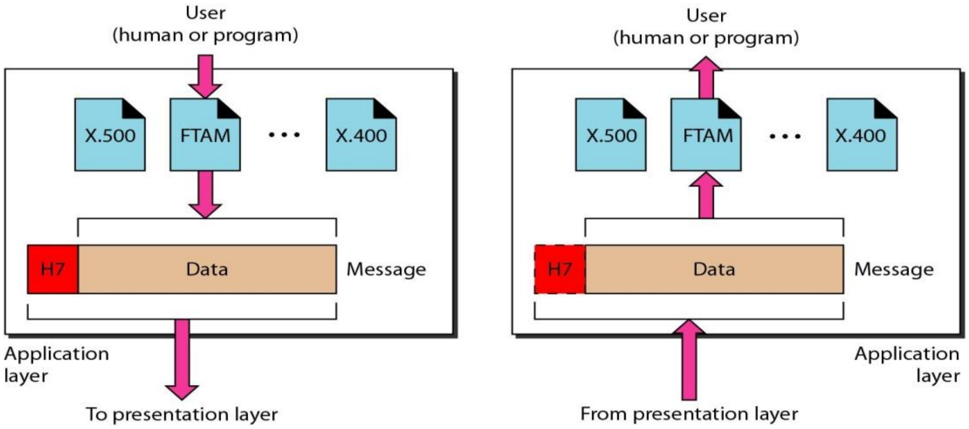
Presentation Layer

It is concerned with syntax and semantics of the information exchanged between peers.



Translation—because different computers use different encoding systems, the presentation layer is responsible for interoperability between these encoding methods.
Encryption—to carry sensitive information, a system ensures privacy by encrypting the message before sending and decrypting at the receiver end.
Compression—Data compression reduces the number of bits contained in the information. It is particularly important in multimedia transmission.

Application Layer

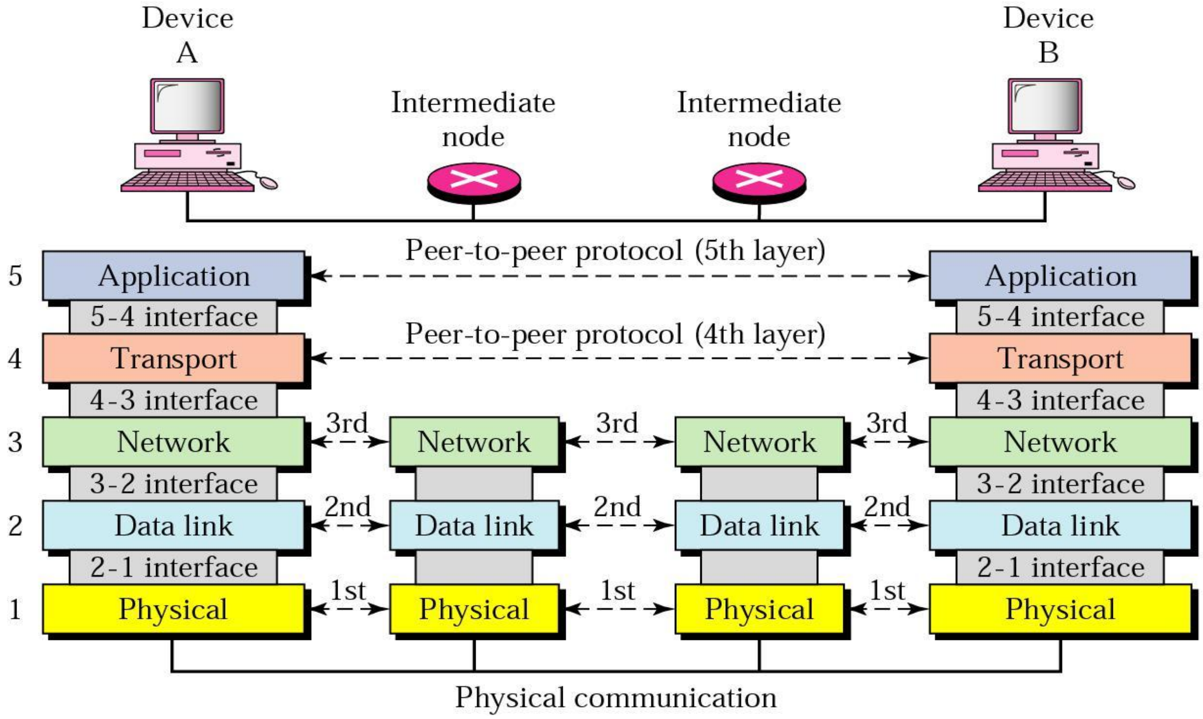


The application layer enables the user, whether human or software, to access the network. It provides user interface and support for services such as electronic mail, remote file access, shared database management and several types of distributed services. It composes a host of application protocols.

8. EXPLAIN THE LAYERS OF TCP/IP (OR) INTERNET ARCHITECTURE IN DETAIL. [CO1 – L2]

Internet uses TCP/IP protocol suite, also known as Internet suite. This defines Internet Model
which contains four layered architecture. OSI Model is general communication model but
Internet Model is what the internet uses for all its communication. The internet is independent
of its underlying network architecture so is its Model. This model has the following layers:

Application Layer: This layer defines the protocol which enables user to interact with the network.For example, FTP, HTTP etc.
Transport Layer: This layer defines how data should flow between hosts. Major protocol at this layer is Transmission Control Protocol (TCP). This layer ensures data delivered between hosts is in-order and is responsible for end-to-end delivery.
Internet Layer: Internet Protocol (IP) works on this layer. This layer facilitates host addressing and recognition. This layer defines routing.
Link Layer: This layer provides mechanism of sending and receiving actual data.Unlike its OSI Model counterpart, this layer is independent of underlying network architecture and hardware.



9. EXPLAIN NETWORK SOFTWARE. [CO1 – L2]

How to implement network software is an essential part of understanding computer networks. In many respects, network applications and network protocols are very similar—the way an application engages the services of the network is pretty much the same as the way a high-level protocol invokes the services of a low-level protocol.

Application Programming Interface (Sockets)

Most network protocols are implemented in software (especially those high in the protocol stack), and nearly all computer systems implement their network protocols as part of the operating system, when we refer to the interface “exported by the network,” we are generally referring to the interface that the OS provides to its networking subsystem. This interface is often called the network *application programming interface* (API).

The advantage of industry-wide support for a single API is that applications can be easily ported from one OS to another, and that developers can easily write applications for multiple OSs. Just because two systems support the same network API does not mean that their file system, process, or graphic interfaces are the same. Still, understanding a widely adopted API like UNIX sockets gives us a good place to start. Each protocol provides a certain set of *services*, and the API provides a *syntax* by which those services can be invoked in this particular OS.

```
int socket(int domain, int type, int protocol)
int bind(int socket, struct sockaddr *address, int addr_len)
int listen(int socket, int backlog)
int accept(int socket, struct sockaddr *address, int *addr_len)
int connect(int socket, struct sockaddr *address, intaddr_len)
int send(int socket, char *message, int msg_len, int flags)
int recv(int socket, char *buffer, int buf_len, int flags)
```

Example Application

The implementation of a simple client/server program that uses the socket interface to send messages over a TCP connection is discussed. The program also uses other Unix networking utilities, Our application allows a user on one machine to type in and send text to a user on another machine. It is a simplified version of the Unix talk program, which is similar to the program at the core of a web chat room. Client program :

```
#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#define SERVER_PORT 5432
#define MAX_LINE 256
int
main(int argc, char * argv[])
{
FILE *fp;
struct hostent *hp;
struct sockaddr_in sin;
char *host;
char buf[MAX_LINE];
int s;
int len;
if (argc==2) {
host = argv[1];
}
else {
fprintf(stderr, "usage: simplex-talk host\n");
exit(1);
}
/* translate host name into peer’s IP address */
hp = gethostbyname(host);
if (!hp) {
fprintf(stderr, "simplex-talk: unknown host: %s\n", host);
exit(1);
}
/* build address data structure */
bzero((char *)&sin, sizeof(sin));
sin.sin_family = AF_INET;
bcopy(hp->h_addr, (char *)&sin.sin_addr, hp->h_length);
sin.sin_port = htons(SERVER_PORT);
/* active open */
if ((s = socket(PF_INET, SOCK_STREAM, 0)) < 0)
{perror("simplex-talk: socket"); exit(1);
}
if (connect(s, (struct sockaddr *)&sin, sizeof(sin)) < 0) {
perror("simplex-talk: connect"); close(s);
exit(1);
}
/* main loop: get and send lines of text */
while (fgets(buf, sizeof(buf), stdin)) {
buf[MAX_LINE-1] = ’\0’;
len = strlen(buf) + 1;
send(s, buf, len, 0);
}
}
```

Server Program :

```
#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#define SERVER_PORT 5432
#define MAX_PENDING 5
#define MAX_LINE 256
int
main()
{
struct sockaddr_in sin;
char buf[MAX_LINE];
int len;
int s, new_s;
/* build address data structure */
bzero((char *)&sin, sizeof(sin));
sin.sin_family = AF_INET;
sin.sin_addr.s_addr = INADDR_ANY;
sin.sin_port = htons(SERVER_PORT);
/* setup passive open */
if ((s = socket(PF_INET, SOCK_STREAM, 0)) < 0) {
perror("simplex-talk: socket"); exit(1);
}
if ((bind(s, (struct sockaddr *)&sin, sizeof(sin))) < 0) {
perror("simplex-talk: bind"); exit(1);
}
listen(s, MAX_PENDING);
/* wait for connection, then receive and print text */
while(1) {
```

```
if ((new_s = accept(s, (struct sockaddr *)&sin, &len)) < 0) {
perror("simplex-talk: accept"); exit(1);
}
while (len = recv(new_s, buf, sizeof(buf), 0))
fputs(buf, stdout);
close(new_s);
}
}
```

10. DISCUSS THE FACTORS THAT AFFECT PERFORMANCE OF THE NETWORK. [CO1 – H1]

Bandwidth and Latency

Performance of a network is measured in terms of *bandwidth* and *latency*.

Bandwidth refers to number of bits that can be transmitted over the network within a certain period of time (*throughput*).Bandwidth also determines how *long* it takes to transmit each bit.

For example, each bit on a 1-Mbps link is 1µs wide, whereas each bit on a 2-Mbps link is 0.5µs wide.

Latency refers to how long it takes for the message to travel to the other end (*delay*). It is a factor of propagation delay, transmission time and queuing delay

$$\text{Latency} = \text{Propagation} + \text{Transmit} + \text{Queue}$$

Speed of light propagation depends on medium (vacuum/copper cable/optical fiber) in which it travels and distance.

$$\text{Propagation} = \text{Distance} / \text{Speed of Light}$$

Transmission time depends upon bandwidth and packet size.

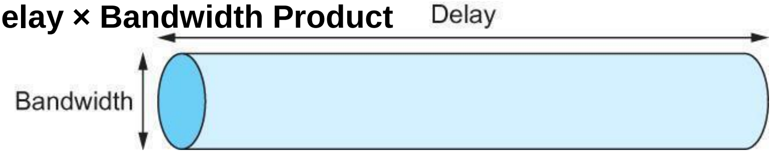
$$\text{Transmit} = \text{Size} / \text{Bandwidth}$$

Queuing delay occurs at switches and routers, since packets are stored before forwarded.

Round Trip Time (RTT) is time taken for the message to travel to the other end and get back.

For applications that have minimal data transfer, latency dominates performance, whereas for bulk data transfers, bandwidth dominates performance.

Delay × Bandwidth Product



Consider a pipe, in which bandwidth is given by diameter and delay corresponds to length of the pipe.

The delay × bandwidth product specifies the number of bits in transit. It corresponds to how much the sender should transmit before the first bit is received at the other end. If receiver signals the sender to stop, it would still receive RTT × bandwidth of data.

For example, for a cross-country fiber with 10 Gbps bandwidth, distance of 4000 km, the RTT is 40 ms and RTT × bandwidth is 400 Mb.

11. DISCUSS ABOUT THE ISSUES IN THE DATA LINK LAYER. [CO1 – H1]

It has several functions like

Data link layer is one of the OSI layers which define the packet format exchanged between the nodes.

Framing
Link access
Flow control
Reliable delivery
Error detection
Error correction
Half duplex
Full duplex

Data link layer design issues:

The data link layer has a number of specific functions it can carry out. These functions include

1. Providing a well defined service interface to the network layer
2. Dealing with transmission errors.
3. Regulating the flow of data. So, that slow receivers are not swamped by fast senders.

To achieve these goals, the data link layer takes the packets it gets from the network layer and encapsulates them into frames for transmission.
Each frame contains a frame header, a payload field for holding the packet and a frame trailer. The relationship between packets and frames is represented below:

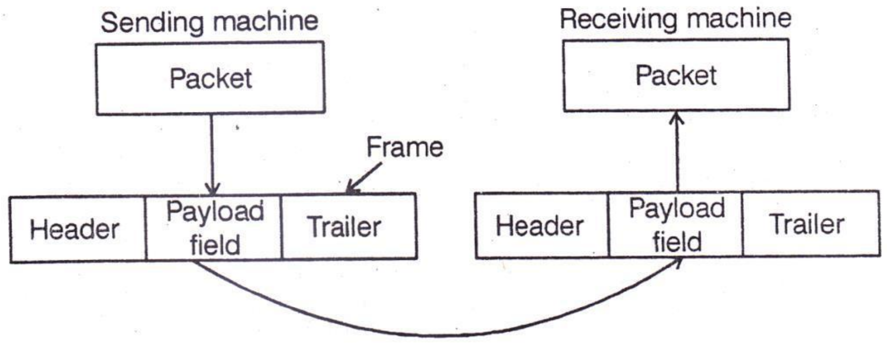


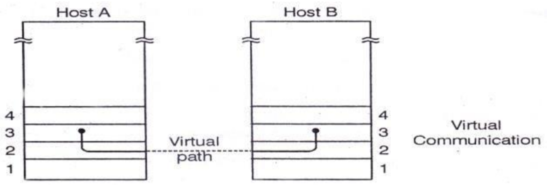
Figure 1.5. Relationship between packets and Frames

Some of the issues in the data link layer are

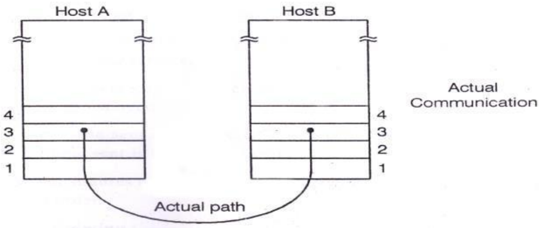
1. Services provided to the network layer
2. Framing
3. Error control
4. Flow control

(a) Services provided to the network layer
The function of the data link layer is to provide services to the network Layer.
The principal service is transferring data from the network layer on the source machine to network layer on the destination machine. On the source machine is an entity, call it a process in the network layer for transmission to the destination.

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.



The actual transmission is given as



The data link layer can be designed to offer various services. The actual services offered can vary from system to system.

The possibilities that are commonly provide are

1. Unacknowledged connectionless service.
2. Acknowledged connectionless service.
3. Acknowledged connection oriented service.

1. Unacknowledged connectionless service:
It consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledge them.

No logical connection is established beforehand or released afterward.

If a frame is lost due to noise on the line, no attempt is made to detect the loss recover from it in the data link layer.

Most LANs use unacknowledged connectionless service in the data link layer.

2. Acknowledged connectionless service:
When this service is offered, there are still no logical connections used. But each frame sent is individually acknowledged. In this way, the sender knows whether a frame has arrived correctly. If it has not arrived within a specified time interval, it can be sent again. This service is useful over unreliable channels like wireless systems.

3. Acknowledged connection oriented service:

The most sophisticated service the data link layer can provide to the network layer connection oriented service. With this service, the source and destination machines establish a connection before any data are transferred. Each frame sent over the connection is numbered and the data link layer guarantee that each frame sent is indeed received. Also, it assures that each frame is received exactly once and that all frames are received in the right order.

(b) Framing:
The incoming data unit from network layer is splitted into more number of small data units.

(c) Error control:
It is provided as a function in order to find the error and to resend the lost or damaged data frame. Also error control is used to overcome the duplication problem.

(d) Flow control:
If the rate at which data are taken by the destination entity is less than sender rate then a flow
control concept is employed to stop the overwhelming or destination entity.

12. EXPLAIN THE CONCEPT OF FRAMING IN DETAIL. [CO1 – L2] Framing
To transmit frames over the node it is necessary to mention start and end of each frame. There are three techniques to solve this frame
Byte-Oriented Protocols (BISYNC, PPP, DDCMP)
Bit-Oriented Protocols (HDLC)
Clock-Based Framing (SONET)

Byte Oriented protocols
In this, view each frame as a collection of bytes (characters) rather than a collection of bits. Such a byte-oriented approach is exemplified by the BISYNC (Binary Synchronous Communication) protocol and the DDCMP (Digital Data Communication Message Protocol)

Sentinel Approach

The BISYNC protocol illustrates the sentinel approach to framing; its frame format is

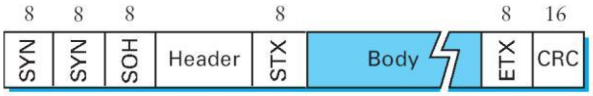


Fig: BISYNC Frame format

The beginning of a frame is denoted by sending a special SYN (synchronization) character.

The data portion of the frame is then contained between special sentinel characters: STX (start of text) and ETX (end of text).

The SOH (start of header) field serves much the same purpose as the STX field.

The frame format also includes a field labeled CRC (cyclic redundancy check) that is used to detect transmission errors.

The problem with the sentinel approach is that the ETX character might appear in the data portion of the frame. BISYNC overcomes this problem by “escaping” the ETX character by preceding it with a DLE (data-link-escape) character whenever it appears in the body of a frame; the DLE character is also escaped (by preceding it with an extra DLE) in the frame body. This approach is called character stuffing.

Point-to-Point Protocol (PPP)

The more recent Point-to-Point Protocol (PPP). The format of PPP frame

is

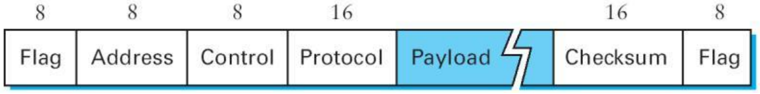


Fig: PPP Frame Format

The Flag field has 01111110 as starting sequence.

The Address and Control fields usually contain default values

The Protocol field is used for demultiplexing.

The frame payload size can he negotiated, but it is 1500 bytes by default.

The PPP frame format is unusual in that several of the field sizes are negotiated rather than fixed.

Negotiation is conducted by a protocol called LCP (Link Control Protocol).

LCP sends control messages encapsulated in PPP frames—such messages are denoted by an LCP identifier in the PPP Protocol.

Byte-Counting Approach

The number of bytes contained in a frame can he included as a field in the frame header. DDCMP protocol is used for this approach. The frame format is

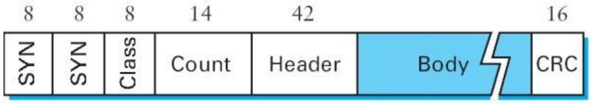


Fig: DDCMP frame format

COUNT Field specifies how many bytes are contained in the frame’s body.

Sometime count field will be corrupted during transmission, so the receiver will accumulate as
many bytes as the COUNT field indicates. This is sometimes called a framing error.

The receiver will then wait until it sees the next SYN character.

Bit-Oriented Protocols (HDLC)

In this, frames are viewed as collection of bits. High level data link protocol is used. The format is

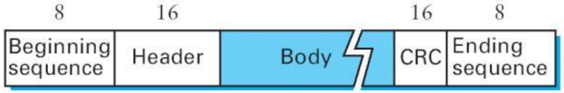


Fig: HDLC Frame Format

HDLC denotes both the beginning and the end of a frame with the distinguished bit sequence 01111110.

This sequence might appear anywhere in the body of the frame, it can be avoided by bit stuffing.

On the sending side, any time five consecutive 1's have been transmitted from the body of the message (i.e., excluding when the sender is trying to transmit the distinguished 01111110 sequence), the sender inserts a 0 before transmitting the next bit.

On the receiving side, five consecutive 1's arrived, the receiver makes its decision based on the next bit it sees (i.e., the bit following the five is).

If the next bit is a 0, it must have been stuffed, and so the receiver removes it. If the next bit is a 1, then one of two things is true, either this is the end-of-frame marker or an error has been introduced into the bit stream.
By looking at the next bit, the receiver can distinguish between these two cases: If it sees a 0 (i.e., the last eight bits it has looked at are 01111110), then it is the end-of-frame marker.

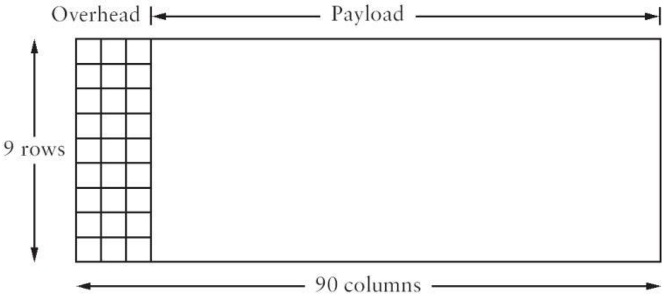
If it sees a 1 (i.e., the last eight bits it has looked at are 01111111), then there must have been an error and the whole frame is discarded.

Clock-Based Framing (SONET)

Synchronous Optical Network Standard is used for long distance transmission of data over optical network.

It supports multiplexing of several low speed links into one high speed links.

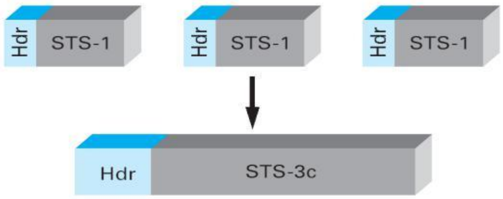
An STS-1 frame is used in this method.



It is arranged as nine rows of 90 bytes each, and the first 3 bytes of each row are overhead, with the rest being available for data.

The first 2 bytes of the frame contain a special bit pattern, and it is these bytes that enable the receiver to determine where the frame starts.

The receiver looks for the special bit pattern consistently, once in every 810 bytes, since each frame is 9 x 90 = 810 bytes long.



The STS-N frame can he thought of as consisting of N STS-1 frames, where the bytes from these frames are interleaved; that is, a byte from the first frame is transmitted, then a byte from the second frame is transmitted, and so on.

Payload from these STS-1 frames can he linked together to form a larger STS-N payload, such a link is denoted STS-Nc. One of the bits in overhead is used for this purpose.

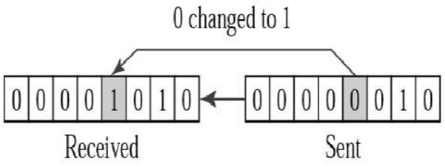
12. EXPLAIN IN DETAIL ERROR DETECTION AND ERROR CORRECTION TECHNIQUE. [CO1 – L2]

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

Types of Errors

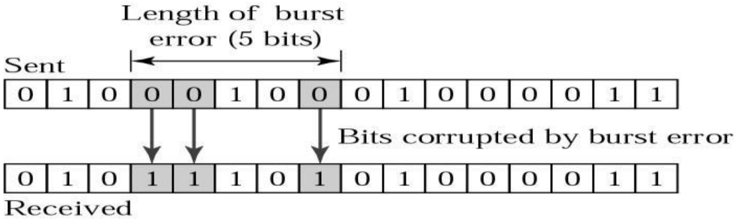
Single-bit error

The term Single-bit error means that only one bit of a given data unit (such as byte, character, data unit or packet) is changed from 1 to 0 or from 0 to 1.



Burst Error

The term Burst Error means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1.



Redundancy

One method is to send every data twice, so that receiver checks every bit of two copies and detect error.

Drawbacks

Sends n-redundant bits for n-bit message.

Many errors are undetected if both the copies are corrupted. Instead of adding entire data, some bits are appended to each unit.

This is called redundant bit because the bits added will not give any new information. These bits are called error detecting codes.

The three error detecting techniques are:
Parity check
Check sum algorithm
Cyclic Redundancy Check

Parity Check

Simple parity check

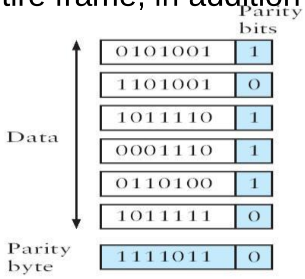
Only one redundant bit, called parity bit is added to every data unit so that the total number of 1's in unit become even (or odd).

Two Dimensional Parity

It is based on simple parity.

It performs calculation for each bit position across each byte in the frame.

This adds extra parity byte for entire frame, in addition to a parity bit for each byte.



Data	0101001	1
	1101001	0
	1011110	1
	0001110	1
	0110100	1
	1011111	0
Parity byte	1111011	0

Fig: Two-dimensional parity

For example frame containing 6 bytes of data. In this third bit of the parity byte is 1 since there are an odd number of 1's is in the third bit across the 6 bytes in the frame.

In this case, 14 bits of redundant information are added with original information.

Check sum algorithm

In the sender side all the words are added and then transmit the result of sum called checksum with the data.

The receiver performs the same calculation on the received data and compares the result with the received checksum.

If any transmitted data, including the checksum itself, is corrupted, then the results will not match, so the receiver knows that an error occurred.

Instead of sending the checksum as such, one's complement of that sum will be send to the receiver. If the receiver gets the result as zero then it will be the correct one.

In this, we can represent unsigned number from 0 to 2^n using n bits.

If the number has more than n bits, the extra leftmost bits need to be added to the n rightmost bits.

Data can be divided in to 16 bit word and the Checksum is initialized to zero.

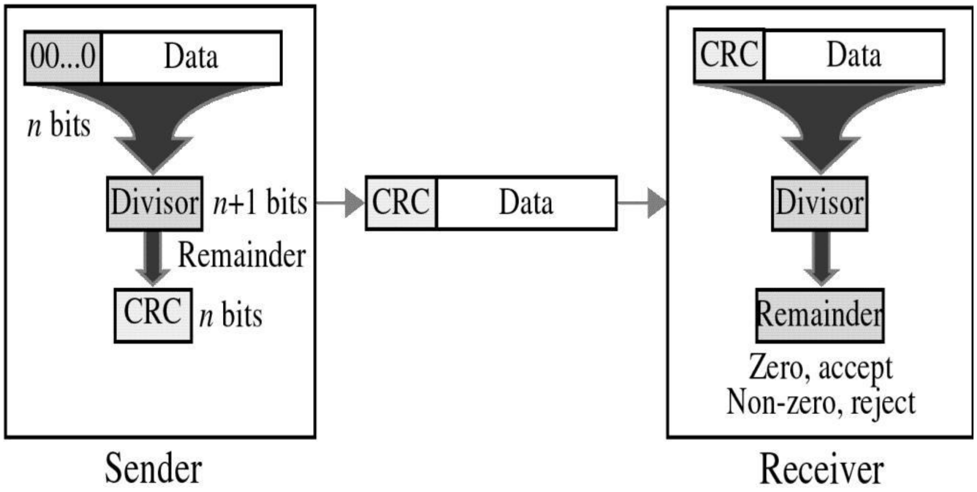
Cyclic Redundancy Check

It uses small number of redundant bits to detect errors.

Divisor is calculated by the polynomial functions under two conditions

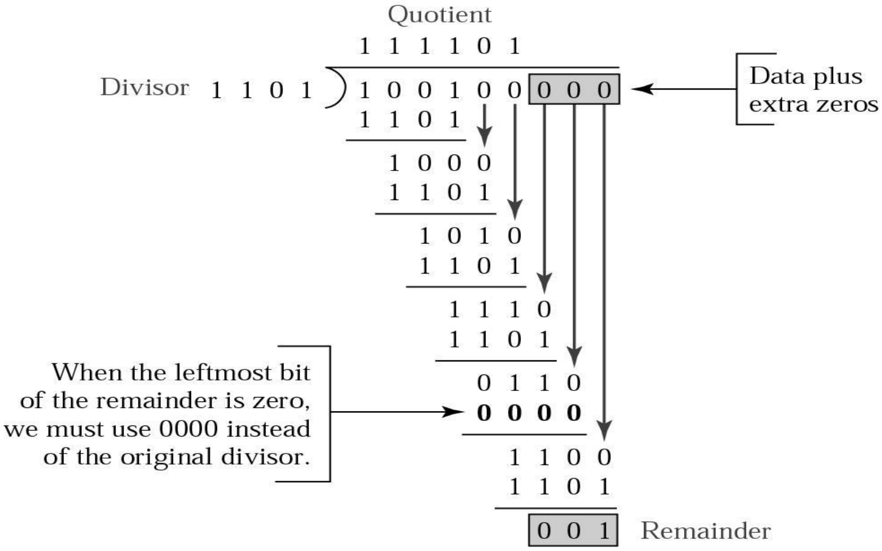
a. It should not be divisible by x
b. It should be divisible by x+1

Consider the original message as M(x) - n+1 bits
Divisor C(x) – K bits
Original sent message = M(x) + k-1 bits



Steps
Append k-1 zeros with M(x) – P(x)
Divide P(x) by C(x)
Subtract the remainder from T(x)
Subtraction is made by making XOR operation

Eg: 100100 by 1101



Error Correction
Error Correction can be handled in two ways

1. When an error is discovered, the receiver can have the sender to retransmit the entire data unit.
2. A receiver can use an error correcting code, which automatically correct certain errors.

Error correcting codes are more sophisticated than error-detection codes and require more redundancy bits.In single bit error detection only two states are sufficient.

1) error
2) no error

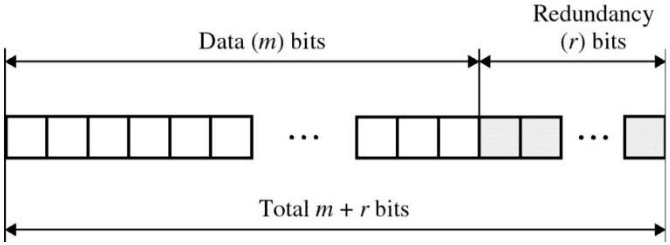
Two states are not enough to detect an error but not to correct it.

Redundancy Bits

To calculate the number of redundancy bit(r) required to correct a given number of data bits (m), we must find a relationship between m and r.

Add m bits of data with r bits. The length of the resulting code is m+r.

Data and Redundancy bits



If the total number of bits are m+r, then r must be able to indicate at least m+r+1 different states. r bits can indicate 2^r different states. Therefore, 2^r must be equal to or greater than m+r+1

$$2^r >= m+r+1$$

For example if the value of m is 7 the smallest r value that can satisfy this equation is 4.

Relationship between data and redundancy bits

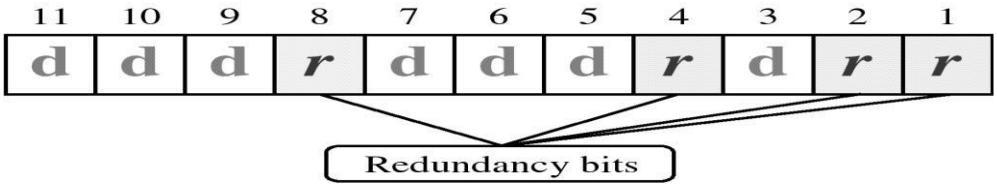
Number of Data Bits (m)	Number of redundancy Bits(r)	Total bits (m+r)
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11

Hamming Code
R.W. Hamming provides a practical solution for the error correction.

Positioning the Redundancy Bits

For example, a seven-bit ASCII code requires four redundancy bits that can be added to the end of the data or intersperse with the original data bits. These redundancy bits are placed in positions 1, 2, 4 and 8. We refer these bits as r1, r2, r3 and r4

Position of redundancy bits in Hamming code



The combination used to calculate each of the four r values for a seven-bit data sequence are as follows

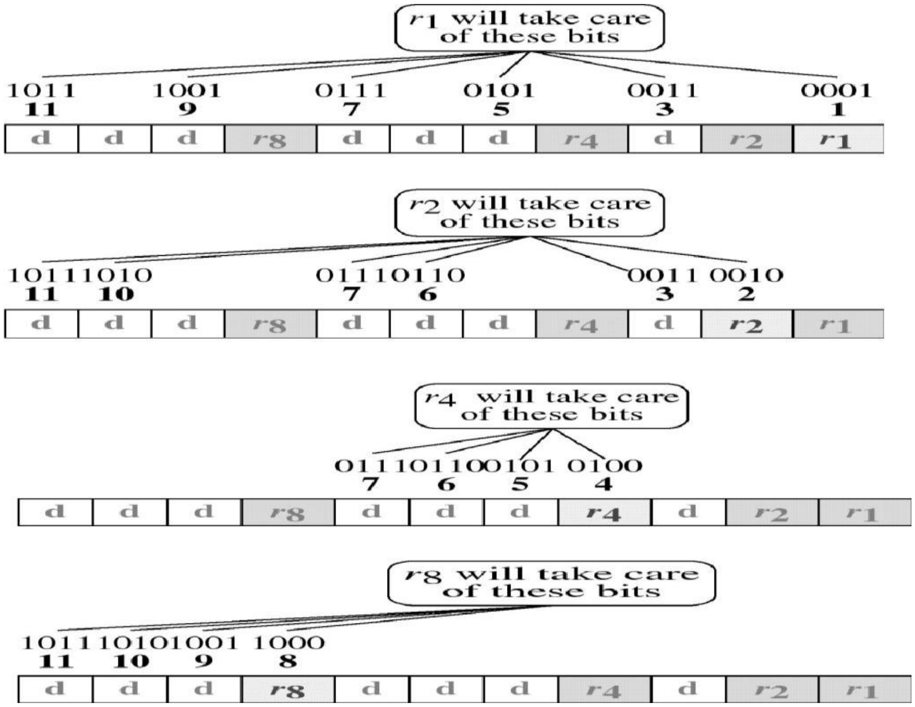
The r1 bit is calculated using all bits positions whose binary representation include a 1 in the rightmost position

r2 is calculated using all bit position with a 1 in the second position and so on

r1: bits 1,3,5,7,9,11
r2: bits 2, 3, 6, 7, 10, 11
r3: bits 4, 5, 6, 7

r4: bits 8, 9, 10, 11

Redundancy bits calculation


r1 will take care of these bits
1011
11
1001
9
0111
7
0101
5
0011
3
0001
1
d d d r8 d d d r4 d r2 r1
r2 will take care of these bits
1011 1010
11 10
0111 0110
7 6
0011 0010
3 2
d d d r8 d d d r4 d r2 r1
r4 will take care of these bits
0111 0110 0101 0100
7 6 5 4
d d d r8 d d d r4 d r2 r1
r8 will take care of these bits
1011 1010 1001 1000
11 10 9 8
d d d r8 d d d r4 d r2 r1

Calculating the r values

Place each bit of the original character in its appropriate position in the 11-bit unit.

Calculate the even parities for the various bit combination.

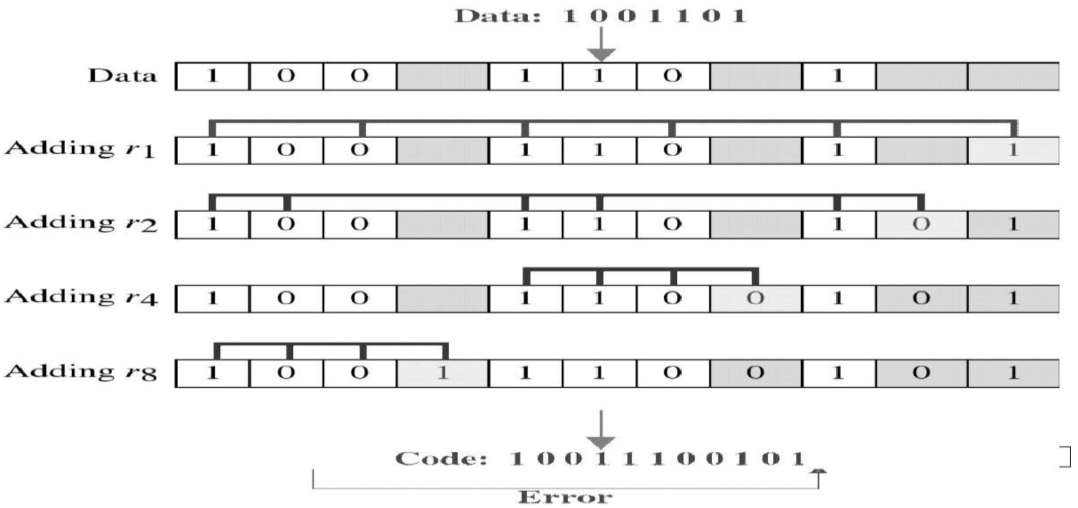
The parity value for each combination is the value of the corresponding r bit. For example,

The value of r1 is calculated to provide even parity for a combination of bits 3,5,7,9 and 11.

The value of r2 is calculated to provide even parity with bits 3, 6, 7, 10 and 11.

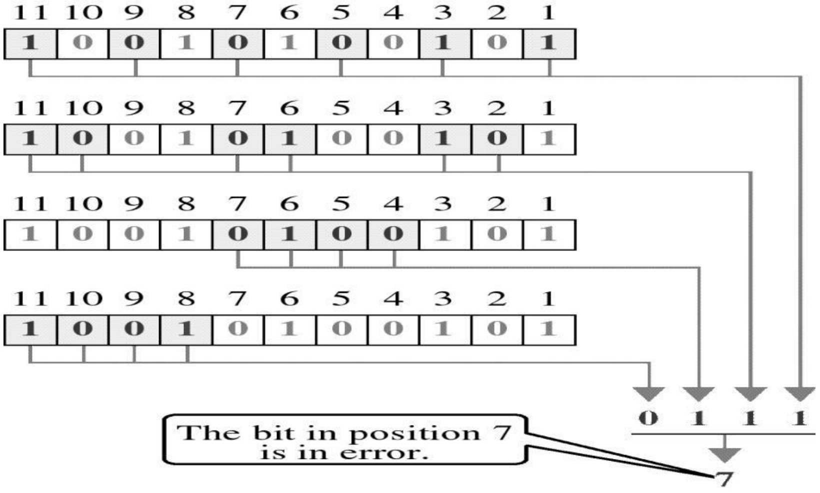
The value of r3 is calculated to provide even parity with bits 4, 5, 6 and 7.

The value of r4 is calculated to provide even parity with bits 8, 9, 10 and 11.


Data: 1 0 0 1 1 0 1
Data 1 0 0 1 1 0 1
Adding r1 1 0 0 1 1 0 1 1
Adding r2 1 0 0 1 1 0 1 0 1
Adding r4 1 0 0 1 1 0 0 1 0 1
Adding r8 1 0 0 1 1 1 0 0 1 0 1
Code: 1 0 0 1 1 1 0 0 1 0 1
Error

The receiver takes the transmission and recalculates four new data using the same set of bits used by the sender plus the relevant parity (r) bit for each set.

Error detection



Then it assembles the new parity values into a binary number in order of r position (r8, r4, r2, r1).

This step gives us the binary number 0111(7 in decimal) which is the precise location of the bit in error.

Once the bit is identified, the receiver can reverse its value and correct the error. Hamming Distance

One of the central concepts in coding for error control is the idea of the Hamming distance.

The Hamming distance between two words (of the same size) is the number of differences between the corresponding bits. The Hamming distance between two words *x* and *y* is *d(x, y).*

The Hamming distance can be found by applying the XOR operation on the two words and count the number of 1’s in the result.

In a set of words, the minimum Hamming distance is the smallest Hamming distance between all possible pairs. We use dmin to define the minimum Hamming distance in a coding scheme.

13. EXPLAIN FLOW CONTROL OF DATA LINK LAYER. [CO1 – L2]

When a data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.

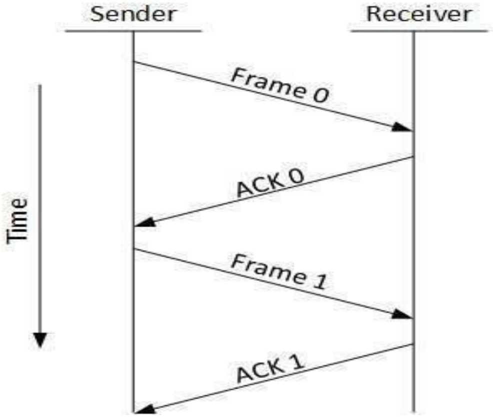
The two flow control mechanisms are

Stop and wait Flow Control

Sliding Window Flow Control

Stop and Wait

This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



Sliding Window

In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

The sender can transmit several frames before needing an acknowledgement.

Frames can be sent one right after another meaning that the link can carry several frames at once and it s 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

Sliding Window refers to imaginary boxes at both the sender and the receiver.

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 are numbered modulo-n which means they are numbered from o to n-1

For eg. If n=8 the frames are numbered 0,1,2,3,4,5,6,7. i.e the size of the window is n -1.

When the receiver sends ACK it includes the number of the next frame it expects to receive.

When the sender sees an ACK with the number 5, it knows that all frames up through number 4 have been received.

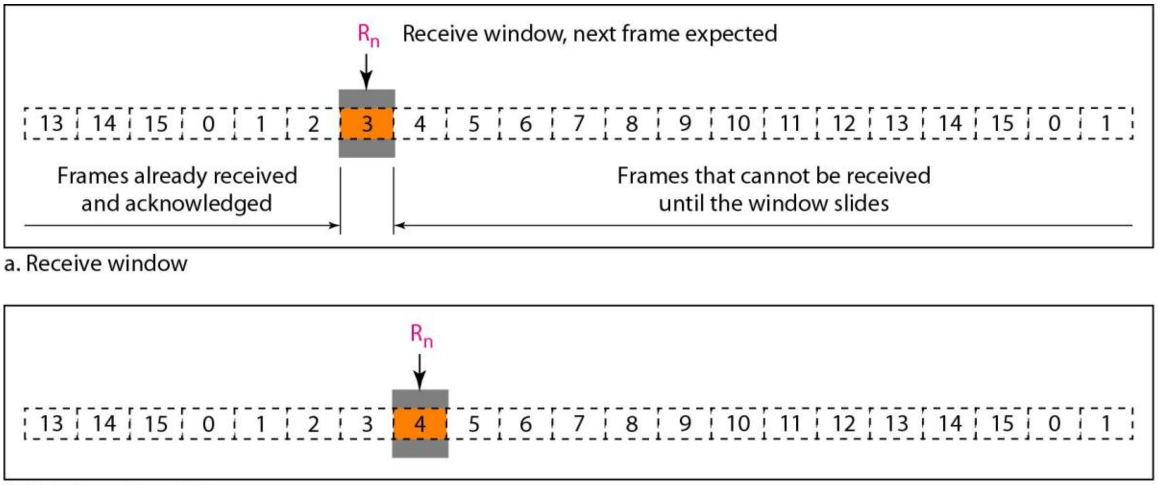
There are two methods to retransmit the lost frames

GO-Back N
Selective Repeat

Go – Back N Method

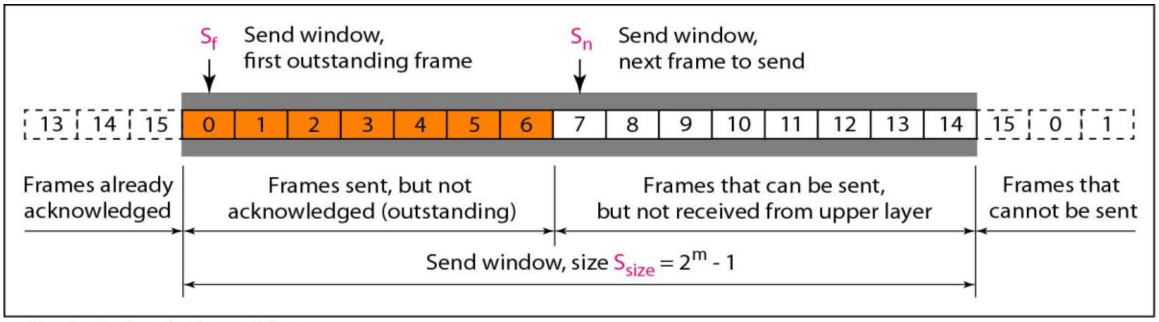
Sender Window
At the beginning of transmission, the sender window contains n-1 frames. As frames are sent out, the left boundary of the window moves inward, shrinking the size of the window
If size of window is W if three frames have been transmitted since the last acknowledgement then the number of frames left in the window is w -3.
Once an ACK arrives, the window expands to allow in a number of new frames equal to the number of frames acknowledged by that ACK.

Receiver Window
The receive window is an abstract concept defining an imaginary box of size 1 with one single variable Rn.
The window slides when a correct frame has arrived, sliding occurs one slot at a time.


R_n
Receive window, next frame expected
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already received and acknowledged
Frames that cannot be received until the window slides
R_n
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1

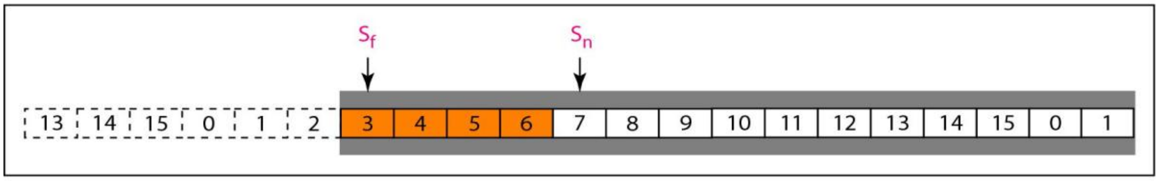
a. Receive window

b. Window after sliding



S_f Send window, first outstanding frame
S_n Send window, next frame to send
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already acknowledged
Frames sent, but not acknowledged (outstanding)
Frames that can be sent, but not received from upper layer
Frames that cannot be sent
Send window, size $S_{size} = 2^m - 1$

a. Send window before sliding

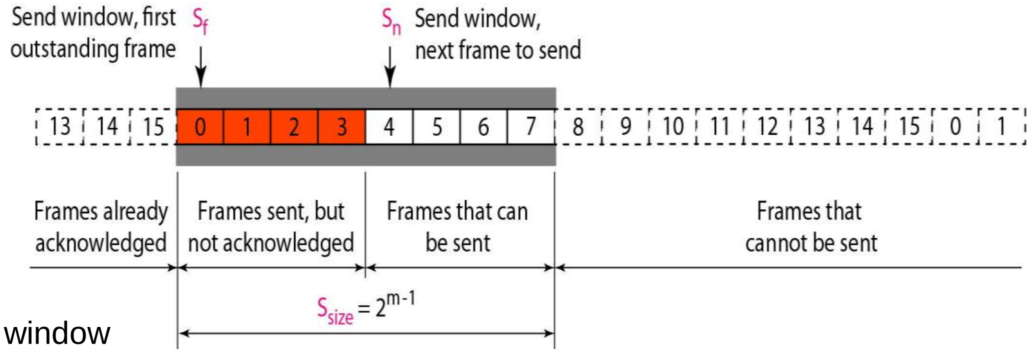


b. Send window after sliding

When the timer expires, the sender resends all outstanding frames. For example, suppose the sender has already sent frame 6, but the timer for frame 3 expires. This means that frame 3 has not been acknowledged; the sender goes back and sends frames 3, 4,5, and 6 again. That is why the protocol is called *Go-Back-N*.

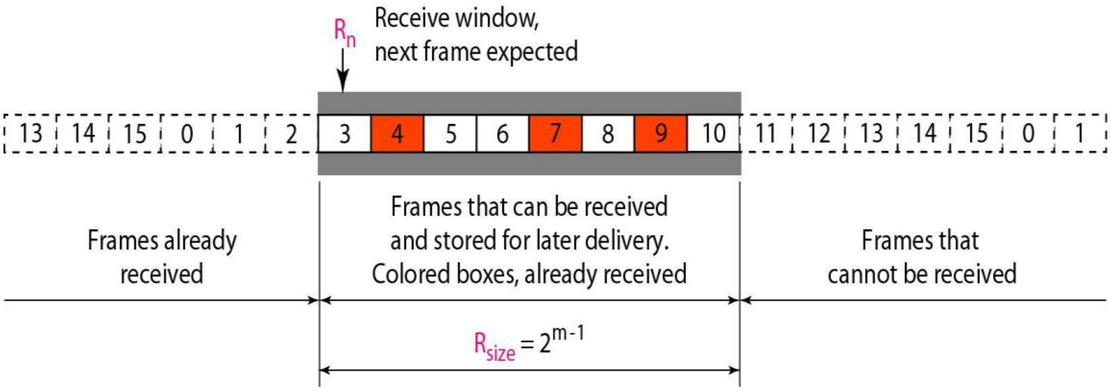
Selective Repeat

Sender Window



Send window, first outstanding frame S_f
S_n Send window, next frame to send
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already acknowledged
Frames sent, but not acknowledged
Frames that can be sent
Frames that cannot be sent
$S_{size} = 2^{m-1}$

Receiver window



R_n Receive window, next frame expected
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already received
Frames that can be received and stored for later delivery. Colored boxes, already received
Frames that cannot be received
$R_{size} = 2^{m-1}$

- The Selective Repeat Protocol allows as many frames as the size of the receive window to arrive out of order and be kept until there is a set of in-order frames to be delivered to the network layer.
- Because the sizes of the send window and receive window are the same, all the frames in the send frame can arrive out of order and be stored until they can be delivered.
- If any frame lost, sender has to retransmit only that lost frames.

15. HOW DATA LINK LAYER PERFORMS ERROR CONTROL? [CO1 – L2]

When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss. In such case, both sender and receiver are equipped with some protocols which helps them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

Requirements for error control mechanism:

Error detection - The sender and receiver, either both or any, must ascertain that there is some error in the transit.

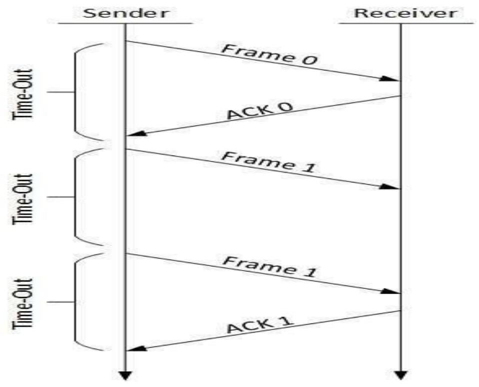
Positive ACK - When the receiver receives a correct frame, it should acknowledge it.

Negative ACK - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.

Retransmission: The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

There are three types of techniques available which Data-link layer may deploy to control the errors by Automatic Repeat Requests (ARQ):

Stop-and-wait ARQ



The following transition may occur in Stop-and-Wait ARQ:

The sender maintains a timeout counter.

When a frame is sent, the sender starts the timeout counter.

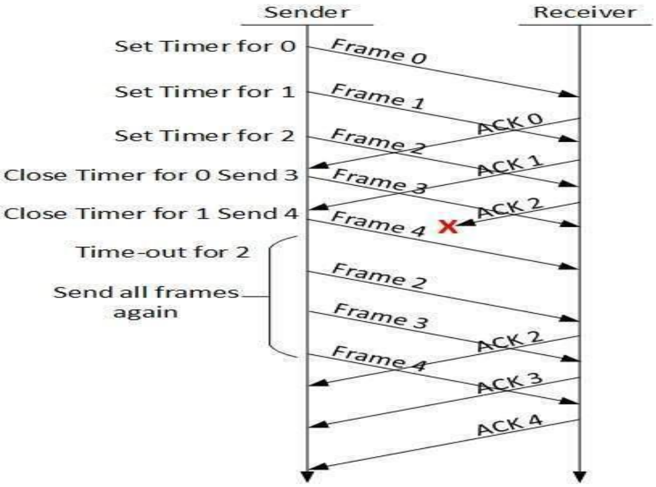
If acknowledgement of frame comes in time, the sender transmits the next frame in queue.

If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.

If a negative acknowledgement is received, the sender retransmits the frame.

Go-Back-N ARQ

Stop and wait ARQ mechanism does not utilize the resources at their best.
When the acknowledgement is received, the sender sits idle and does nothing.
In Go-Back-N ARQ method, both sender and receiver maintain a window.

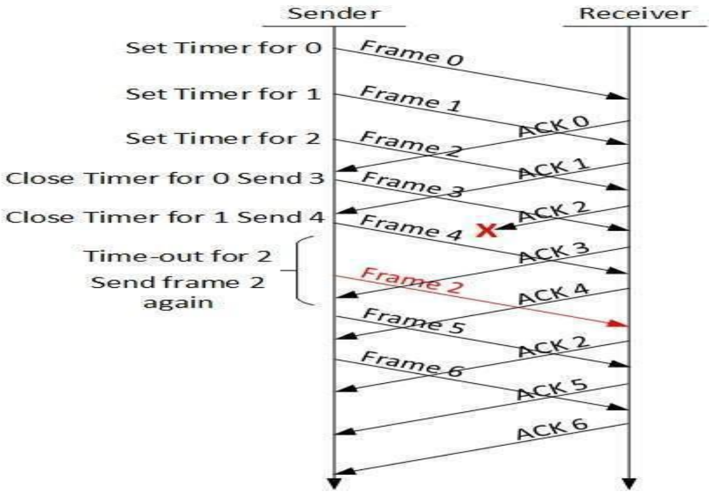


The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame’s sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not received any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

Selective Repeat ARQ

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.



UNIT II
MEDIA ACCESS & INTERNETWORKING

PART-A

1. What are the functions of MAC? [CO4 – L1]

MAC sub layer resolves the contention for the shared media. It contains synchronization, flag, flow and error control specifications necessary to move information from one place to another, as well as the physical address of the next station to receive and route a packet.

2. What are the functions of LLC? [CO4 – L1]

The IEEE project 802 models take the structure of an HDLC frame and divides it into 2 sets of functions. One set contains the end user portion of the HDLC frame – the logical address, control information, and data. These functions are handled by the IEEE 802.2 logical link control (LLC) protocol.

3. What is Ethernet? [CO4 – L1 MAY/JUNE 2016]

Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link.

4. Define the term carrier sense in CSMA/CD. [CO4 – L1]

All the nodes can distinguish between idle and a busy-link and “collision detect” means that a node listens as it transmits and can therefore detect when a frame it is transmitting has interfered (collided) with a frame transmitted by another node.

5. Define Repeater. [CO4 – L1]

A repeater is a device that forwards digital signals, much like an amplifier forwards analog signals. However, no more than four repeaters may be positioned between any pairs of hosts, meaning that an Ethernet has a total reach of only 2,500m.

6. Define collision detection. [CO4 – L1]

In Ethernet, all these hosts are competing for access to the same link, and as a consequence, they are said to be in the same collision detection.

7. Why Ethernet is said to be I-persistent protocol? [CO4 – L1]

An adaptor with a frame to send, transmits with probability “1” whenever a busy line goes idle.

8. What is exponential back off? [CO4 – L1]

Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again. Each time it tries to transmit but fails, the adaptor doubles the amount of time it waits before trying again. This strategy of doubling the delay interval between each transmission attempt is a general technique known as exponential back off.

9. What is token holding time (THT)? [CO4 – L1]
It defines that how much data a given node is allowed to transmit each time it possesses the token or equivalently, how long a given node is allowed to hold the token.

8. What are the two classes of traffic in FDDI? [CO4 – L1]
Synchronous
Asynchronous

9. What are the four prominent wireless technologies? [CO4 – L1 MAY/JUNE 2016]
Bluetooth
Wi-Fi(formally known as 802.11)
WiMAX(802.16)
Third generation or 3G cellular wireless.

10. Define Bluetooth. [CO4 – L1]
Bluetooth fills the niche of very short-range communication between mobile phones, PDAs, notebook computers, and other personal or peripheral devices. For example, Bluetooth can be used to connect mobile phones to a headset, or a notebook computer to a printer.

13. What are the four steps involves in scanning? [CO4 – L1]
The node sends a Probe frame.
All APs within reach reply with a Probe Response frame.
The node selects one of the access points, and sends that AP an Association Request frame.
The AP replies with an Association Response frame.

14. Explain the term handoff. [CO4 – L2]
If the phone is involved in a call at the time , the call must be transferred to the new base station in what is called a hand off.

15. Define satphones. [CO4 – L1]
Satphones use communication satellites as base stations, communicating on frequency bands that have been reserved internationally for satellite use.

16. How to mediate access to a shared link? [CO4 – L2]
Ethernet and token ring media access protocols have no central arbitrator of access. Media access in wireless networks is made more complicated by the fact that some nodes may be hidden from each other due to range limitations of radio transmission.

17. Define Aggregation points. [CO4 – L1]
They collect and process the data they receive from neighboring nodes, and then transmit the processed data. By processing the data incrementally, instead of forwarding all the raw data to the base station, the amount of traffic in the network is reduced.

18. Define Beacons. [CO4 – L1]

Beacon to determine their own absolute locations based on GPS or manual configuration. The majority of nodes can then derive their absolute location by combining an estimate of their position relative to the beacons with the absolute location information provided by the beacons.

19. What is the use of Switch? [CO4 – L1]

It is used to forward the packets between shared media LANs such as Ethernet. Such switches are sometimes known by the obvious name of LAN switches.

20. Explain Bridge. [CO4 – L2]

Bridge is a layer 2 connecting device. Bridge connects segments of same LAN.

21. What is Spanning tree? [CO4 – L1]

It is for the bridges to select the ports over which they will forward frames.

22. What are the three pieces of information in the configuration messages? [CO4 – L1]

The ID for the bridge that is sending the message.
The ID for what the sending bridge believes to the root bridge.
The distance, measured in hops, from the sending bridge to the root bridge.

23. What is broadcast? [CO4 – L1]

Each bridge forwards a frame with a destination broadcast address out on each active (selected) port other than the one on which the frame was received.

24. What is multicast? [CO4 – L1]

Sending the data to group of nodes (one to many).

25. How does a given bridge learn whether it should forward a multicast frame over a given port? [CO4 – L2]

It learns exactly the same way that a bridge learns whether it should forward a by Unicast frame over a particular port observing the source addresses that it receives over that port.

26. What are the limitations of bridges? [CO4 – L1]

Scale
heterogeneity

27. Classify the various protocols used for medium access. [CO4 – L2]

Random access	*Controlled access*	*Channelization*
Aloha CSMA CSMA/CA CSMA/CD	Reservation Polling Token passing	FDMA TDMA CDMA

PART-B

1. EXPLAIN ABOUT CSMA WITH THEIR VERSIONS. [CO4 – L2]

There are many versions in the carrier sense protocols.

They are:

1. 1_Persistent CSMA
2. Non persistent CSMA
3. P-persistent CSMA

1_Persisitent CSMA

This is the first carrier sense protocol. When a station holds data to transmit, this first listens to the channel to check if any other is sending at that time.

(a) If the channel is busy, then the station waits until it becomes idle.
(b) When the channel is free, the station sends a frame.

Suppose if a collision happens then the station waits a random amount of time and starts all over again. This protocol is said to be l persistent, because the station sends with a probability of l when it detects the channel as free. After a station is sending, another station will become ready to send and sense the channel.

When the first station’s signal has not yet reached the second one, the later will sense the idle channel. Also it sends the frames. This results in collision. If the propagation delay is zero then there will be collisions. When the 2 stations become ready in the middle of a third station’s transmission, both will wait until the transmission is over. After that both will start to transmit exactly at the same time. This also results collision.

Non persistent CSMA

This is the second carrier sense protocol. Here it senses a channel before sending the frames.

(a)if there is no other transmission, it starts to send the frames.
(b) else if the channel is already in use then it waits a random amount of time and then do the same algorithmic steps again. It does not continuously sense the channel for the purpose of seizing it immediately upon detecting the end of previous transmission.

P-persistent CSMA

This applies to slotted channels. If a station wants to send then first it senses the channel.

(a)When the channel is free, the station sends frames with a probability p. With a probability q=l-p, it defers until the next slot; when finding that slot is also idle, it may either sends or defers again with the probabilities of p & q until either the frame has been transmitted or another station has started the transmission, this process is repeated.

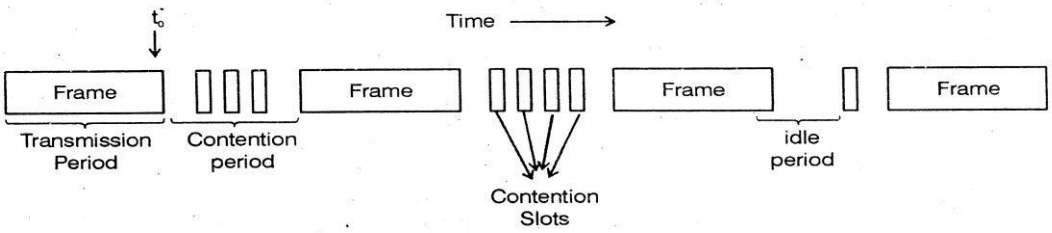
When the station finds the channel as busy, it waits until the next slot and applies the same algorithm.

CSMA with Collision Detection

This protocol is widely used on LANs in the MAC sub layer.

It is the basis of the popular Ethernet LAN. When the 2 stations sense the channel to be idle and start transmitting at the same time, they will find the collision immediately. They should stop transmitting as soon as the collision is detected.

If immediately stops the damaged frames then it saves the time and bandwidth. It refers CSMA with collision Detection. This employs the conceptual model given below.



CSMA / CD can be in any one of the states like contention, transmission or idle From the figure, a station ends its transmission at ‘t0’. Any other station may send now. Suppose if more than I station wants to send the frames at the same time then there will be a collision.

After a collision is detected, the station aborts its transmission and waits for a random amount of time.

2. EXPLAIN IN DETAIL ABOUT TYPES OF ETHERNET. [CO4 – L2]

Switched Ethernet

As more and more stations are added to an Ethernet, the traffic will go up. Eventually, the LAN will saturate. One way out is to go to a higher speed, say, from 10 Mbps to 100 Mbps. But with the growth of multimedia, even a 100 – Mbps or 1-Gbps Ethernet can become saturated.

Fast Ethernet: Three choices

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100m	Uses category 3 UTP
100Base-TX	Twisted pair	100m	Full duplex at 100 Mbps
100Base-FX	Fiber optics	2000m	Full duplex at 100 Mbps; long runs

IEEE 802.3 100 BASE-T Physical Layer Medium Alternatives

	100BASE-TX		**100BASE - FX**	**100BASE – T4**
Transmission medium	2 pair, STP	2 pair, Category 5 UTP	2 Optical Fiber	4pair, category3,4
Signaling technique	MLT-3	MLT-3	4B5B, NRZI	8B6T, NRZ
Data rate	100 Mbps	100 Mbps	100 Mbps	100 Mbps
Maximum segment length	100 m	100 m	100 m	100 m
Network span	200 m	200 m	400 m	200 m

Fast Ethernet Details

UTP Cable has a 30MHz limit
→ Not feasible to use clock encoding (i.e., NO Manchester encoding)

Instead use bit encoding schemes with sufficient transitions for receiver to maintain clock synchronization.

100 BASE T4

- Can use four separate twisted pairs of cat 3 UTP
- Utilize three pair in both directions (at 33 1/ 3 Mbps) with other pair for carrier sense/ collision detection.
- Three – level ternary code is used8B/6T.
  Prior to transmission each set 8 bits is converted into 6 ternary symbols.
- To reduce latency, ternary symbols are sent staggered on the three lines.
  - 100 BASE T4
- Ethernet Interframe gap of 9.6 microseconds becomes 960 nanoseconds in Fast Ethernet.
- 100m. max distance to hub; 200 meters between stations.
- Maximum of two class II repeaters.

100 Base TX

- Uses two pair of twisted pair, one pair for transmission and one pair for reception.
- Use either STP or Cat 5 UTP.
- Uses MTL-3 signaling scheme that involves three voltages.
- Uses 4B/5B encoding.

There is a guaranteed signal transition at least every two bits.

100 Base FX

- Uses two optical fibers, one for transmission and one for reception.
- Uses FDDI technology of converting 4B/5B to NRZI code group streams into optical signals.

Fast Ethernet Repeaters and Switches

- Class I Repeater – supports unlike physical media segments (only one per collision domain)
- Class II Repeater – limited to single physical media type (there may be two repeaters per collision domain)
- Switches – to improve performance can add full-duplex and have auto negotiation for speed mismatches.
- Gigabit Ethernet:

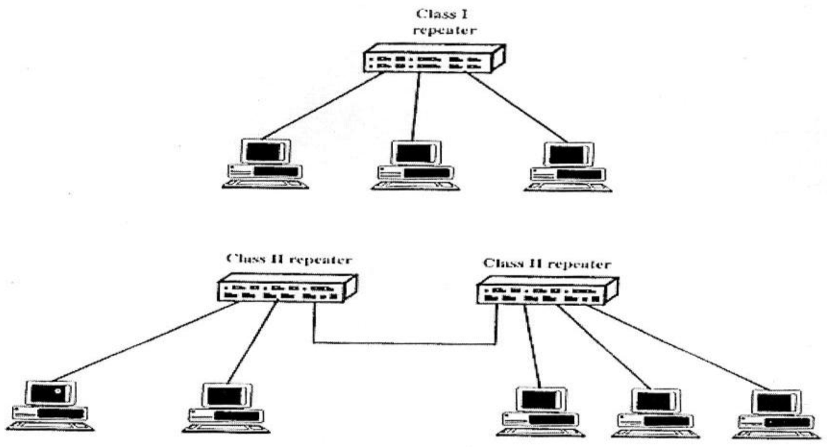


Figure 7.10 100BASE-T Repeater Types

Gigabit Ethernet (1000 BASE X)

- Provides speeds of 1000 Mbps (i.e., one billion bits per second capacity) for half-duplex and full-duplex operation.
- Uses Ethernet frame format and MAC technology.
- Uses 802.3x flow control.

All Gigabit Ethernet configurations are poin-to-point!

Gigabit Ethernet Technology

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550m	Multimode fiber (50,62.5 microns)
1000Base-LX	Fiber optics	5000m	Single(10µ) or multimode(50,6.2.5µ)
1000Base-CX	2 Pairs of STP	25m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100m	Standard category 5 UTP

Gigabit Ethernet (1000 BASE-T)

1000 BASE SX
Short wavelength

- Supports duplex links up to 275 meters.
- 770-860 nm range; 850 nm laser wavelength
- (FC) Fiber Channel technology
- PCS (Physical Code Sub layer) includes 8B/10B encoding with 1.25 Gbps line.
- Only multimode fiber

1000 BASE LX
Long wavelength

- Supports duplex links up to 550 meters.
- 1270-1355 nm range; 1300 nm wavelength using lasers.
- Fiber Channel technology

1000 BASE CX
‘Short haul’ copper jumpers

- Shielded twisted pairs
- PCS (physical code sub layer) includes 8B/10B encoding with 1.25Gbps line.
- Each link is composed of a separate shielded twisted pair running in each direction.

1000 BASE T
Twisted Pair

- Four pairs of Category 5 UTP.
- IEEE 802.3ab ratified in June 1999.
- Category 5, 6 and 7 copper up to 100 meters.
- This requires extensive signal processing.

Gigabit Ethernet

- Viewed as LAN solution while ATM is WAN solution.
- Gigabit Ethernet can be shared (hub) or switched.
- Shared Hub
  - Half duplex: CSMA/CD with MAC changes:
    - Carrier extension
    - Frame Bursting
- Switch
  - Full duplex: Buffered repeater called {Buffered Distributor}
- Gigabit Ethernet

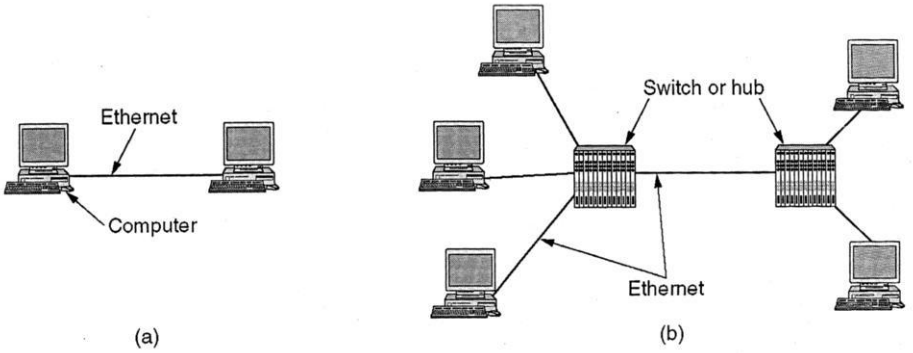


Figure 4-22. (a) A two-station Ethernet. (b) A multistation Ethernet.

3. EXPLAIN THE FUNCTIONING OF WIRELESS LAN OR IEEE 802.11 IN DETAIL. [CO4 – L2 NOV/DEC 2015]

Wireless LAN or WLAN or Wi-Fi is designed for use in a limited area (office, campus, building, etc). It is standardized as IEEE 802.11

Physical Properties

WLAN runs over free space based on *FHSS* (frequency hopping over 79 1-MHz-wide frequency bandwidth) and DSSS (11-bit chipping sequence) with data rate of 2 Mbps.

Variants of 802.11 are:

- 802.11b operates in 2.4-GHz frequency band with data rate of 11 Mbps.
- 802.11a/g runs in 5-GHz band using orthogonal FDM (OFDM) at 54Mbps
- 802.11n uses multiple antennas (multiple input/output) and offers up to 100 Mbps

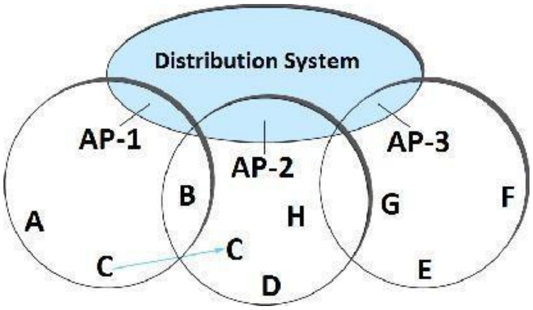
Optimal bit rate for transmission is based on signal-to-noise ratio (SNR) in environment.

Distribution System

In wireless network, nodes are mobile and the set of reachable nodes change with time.

Mobile nodes are connected to a wired network infrastructure called *access points* (AP)

Access points are connected to each other by a *distribution system* (DS) such as Ethernet.



- Nodes communicate directly with each other if they are reachable (eg, *A* and *C*)
- Communication between two nodes in different APs occurs via two APs (eg, *A* and *E*)
- Whenever a mobile node joins a network, it selects an AP. This is called *active scanning.*

    Node sends a Probe frame.
    All APs within reach reply with a Probe Response frame.
    Node selects an AP and sends an Association Request frame. o
    Corresponding AP replies with an Association Response frame

- Access points periodically send a Beacon frame advertising its features such as transmission rate. This is known as *passive scanning.*

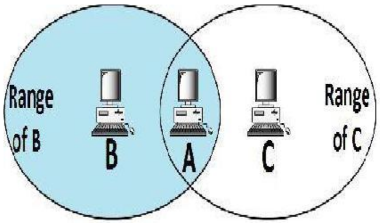
Hidden / Exposed Node Problem

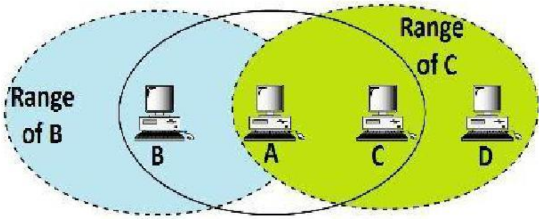
- All nodes are not within the reach of each other.
- Carrier sensing may fail because of hidden node and exposed node problem.

Hidden Node

- Suppose node *B* is sending data to *A*. At the same time, node *C* also wishes to send to *A*.
- Since node *B* is not within the range of *C*, *C* finds the medium free and transmits to *A.*
- Frames from nodes *B* and *C* sent to *A* collide with each other*.*

Thus nodes *B* and *C* are *hidden* from each other.





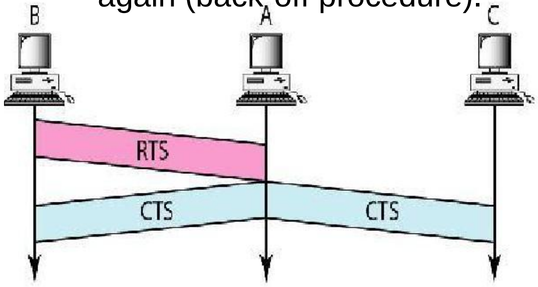
Hidden Node *Exposed Node*

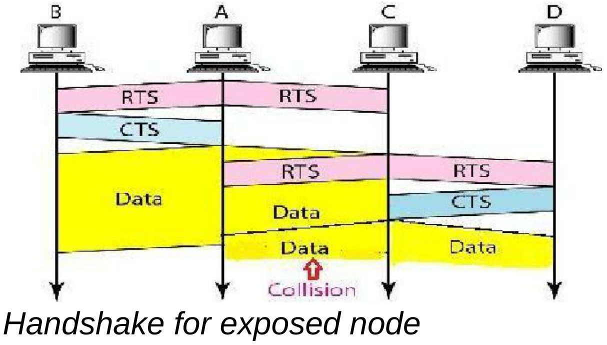
Exposed Node

- Suppose node *A* is transmitting to node *B* and node *C* has some data to be sent to node *D*.
- Node *C* finds the medium busy, since it hears the transmission from node *A* and refrains from sending to node *D*, even though its transmission to *D* would not interfere.
- Thus node *C* is *exposed* to transmission from node *A* to *B*

Multiple Access with Collision Avoidance (MACA)

- Sender and receiver exchange *control frames* to reserve access, so that nearby nodes avoid transmission during duration of a data frame. Control frames used to avoid collision are *Request to Send* (RTS) and *Clear to Send* (CTS).
- Sender sends RTS frame to the receiver containing sender/receiver address and transmission duration.
- Nodes that receive RTS frame are close to sender and wait for CTS to be transmitted back.
- Receiver acknowledges and sends a CTS frame containing sender address and duration. Nodes that receive CTS remain silent for the upcoming data transmission. Nodes that receive RTS but not CTS, is away from the receiver and is free to transmit.
- Receiver sends an ACK frame to the sender after successfully receiving data frames.
- If RTS frames from two or more nodes collide, then they do not receive CTS. Each node waits for a random amount of time and then tries to send RTS again (back-off procedure).





Handshake for hidden node *Handshake for exposed node*

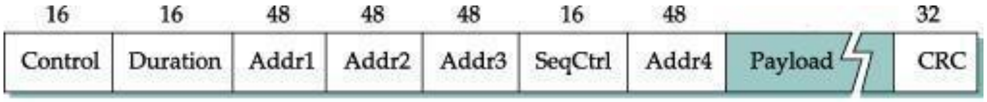
Handshake for Hidden node

- Node B has frames for A and sends RTS to A. It reaches A, but not C.
- Node A sends CTS frame to B, which is also received by node C.
- Node B starts to transmit data frames to node A.
- Node C knows of upcoming transmission from B to A and refrains from transmitting.

Handshake for Exposed node

- Assume that node A is transmitting to node B after exchanging control frames.
- Node C sends RTS to node D which is also sent to node A.
- Node D replies with CTS to C, whereas node A does not reply, since it is transmitting.
- Node C infers that there is no interference and transmits data frames to node D.

Frame Format



- Control—indicates frame type (RTS, CTS, ACK or data) and 1-bit To DS / From DS
- Duration—specifies duration of frame transmission.
- Addresses—The four address fields depend on value of To DS and From DS subfield

ToDS	FromDS	Addr1	Addr2	Addr3	Addr4	*Description*
0	0	Destinati	Source			Sent directly
0	1	Destinati on	Sending AP	Source		Frame is coming from a distribution system
1	0	Receiving AP	Source	Destination		Frame is going to a distribution system
1	1	Receiving AP	Sending AP	Destination	Source	Frame is going from one AP to another AP

- Sequence Control—defines sequence number of the frame
- Payload—contains a maximum of 0–2312 bytes.
- CRC—contains CRC-32 error detection sequence.

4. WRITE SHORT NOTES ON BLUETOOTH. [CO4 – L1]

Bluetooth technology, standardized as IEEE 802.15.1 is a personal area network (PAN). It is used for short-range wireless communication (maximum 10 m) between mobile phones, PDAs, notebook and other peripheral devices.

Uses low power transmission, operates in 2.45 GHz band with data rate up to 3 Mbps.

Bluetooth Special Interest Group has specified a set of protocols for a range of application, known as *profiles*. For instance, a profile synchronizes PDA and PC.

Bluetooth network configuration is known as *piconet*. A piconet can have up to eight stations, one of which is called the master and the rest are called slaves.

Slaves do not directly communicate with each other, but via the master.

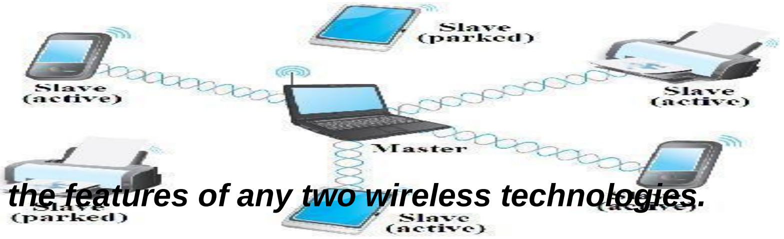
Bluetooth uses FHSS (79 channels, each 625 μs) for transmission.

Master transmits in odd-numbered slots, whereas slave respond in even slots.

Slaves in *parked* or inactive state cannot communicate, until it is activated by the master.

Maximum of 255 devices can be in parked state.

Bluetooth hardware and software is simpler and cheaper.



List and compare the features of any two wireless technologies.

	Bluetooth	WiFi	WiMax	3G
IEEE standard	802.15.1	802.11	802.16	
Link length	10 m	100 m	10 km	Tens of km
Bandwidth	2.1 Mbps (shared)	54 Mbps (shared)	70 Mbps	384 Kbps
Usage	Link a peripheral to a computer	Link a computer to a wired base	Link a building to a wired tower	Link a cell phone to a wired tower

5. EXPLAIN THE DIFFERENT SWITCHING TECHNIQUES IN DETAIL. [CO4 – L2]

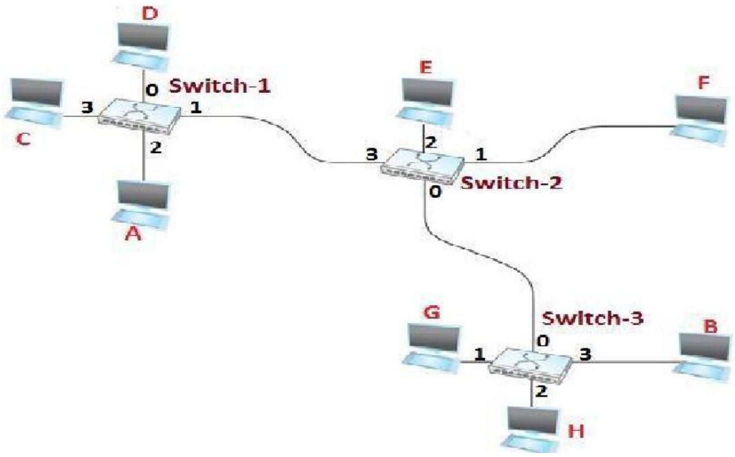
Datagram

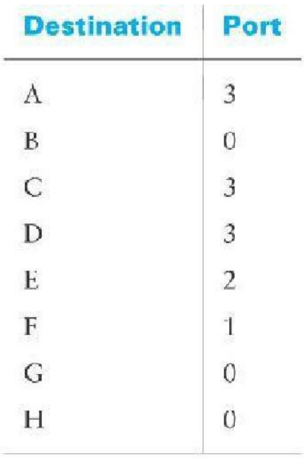
- Datagram approach is a *connectionless* network. No connection state is maintained.
- Resources such as bandwidth are *not reserved* for a packet but allocated on *demand*.
- Lack of reservation creates *delay*.

- Packets can be *dropped* due to lack of resources.
- Each packet is routed *independently* of previous packets.
- A switch or link *failure* does not have adverse effect.

Routing table

- Each switch has a *forwarding* table that contains destination address and output port.
- When a switch examines a packet, the destination address is *looked-up* in the table to determine the corresponding output port, onto which the packet is forwarded.



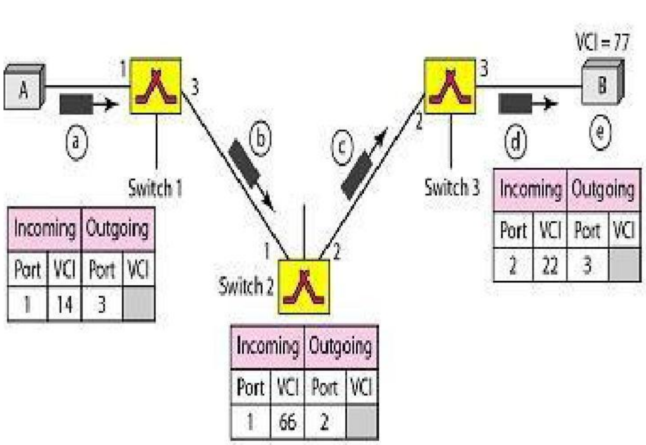


Destination	Port
A	3
B	0
C	3
D	3
E	2
F	1
G	0
H	0

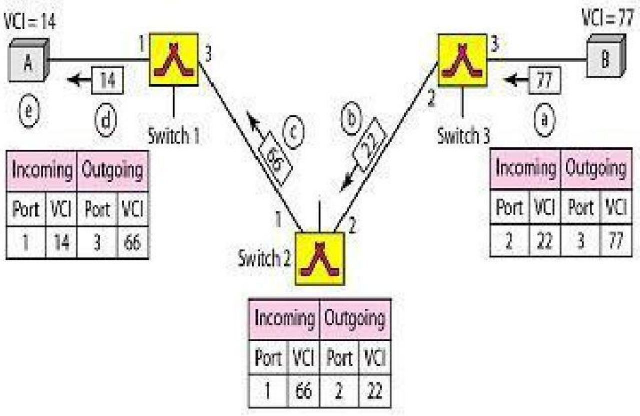
Example Network Forwarding table for Switch-2

Virtual Circuit Switching

- Virtual-circuit is a *connection-oriented* model. A *virtual connection* from source to the destination is established before any data is sent.
- Each switch contains VC table with each entry containing incoming port, incoming VCI, outgoing port and outgoing VCI.
- *Virtual Circuit Identifier* (VCI) uniquely identifies a connection. It has *link local scope*.
- Incoming and outgoing VCI is always distinct.
- VCI and interface on which it was received, uniquely identifies a virtual connection.
- Connection state set by the administrator is known as Permanent virtual circuit (PVC).
- Hosts can set virtual circuit through signaling (SVC). It consist of two phases: Setup Request and Acknowledgement



Setup Request



Acknowledgement

Setup Request

- Switch *1* receives connection setup request frame from host *A*.
  - ✓ It knows that frames for host *B* should be forwarded on port *3*. o Creates an entry in its VC table for the new connection with
    incoming port=*1* and
    outgoing port=*3*.
  - ✓ Chooses an unused VCI for frames to host *B*, say *14* as incoming VCI.
  - ✓ Outgoing VCI is unknown (left *blank*) and the frame is forwarded to *switch 2*.
- Similarly entries are made at other switches as frame is forwarded to destination.
- Destination *B* accepts the setup request frame. Assigns an unused VCI, say *77,* for frames that come from host *A*.

Acknowledgment

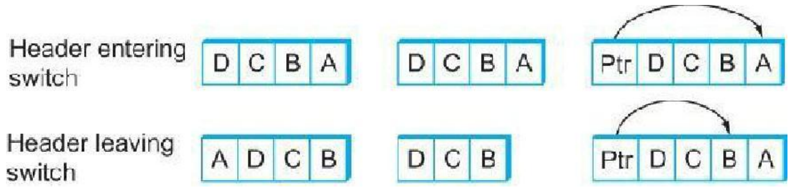
- Host *B* sends an acknowledgment to *switch 3*.
  - ✓ The ACK frame carries source & destination addresses and chosen VCI by host *B*.
  - ✓ Switch *3* uses this VCI, i.e., *77* as outgoing VCI and completes VC table entry.
- Similarly other switches fill up outgoing VCI and forward the ACK.
- Finally switch *1* sends an acknowledgment to source host *A* containing VCI as *14*.
- Source host *A* uses *14* as its outgoing VCI for data frames to be sent to destination *B*.

- ✓ Data transfer starts after connection establishment
- ✓ Resources are reserved, therefore QoS is guaranteed by the network
- ✓ In case of switch/link failure, old connection is torn and new one needs to be established.

- All information about network topology required to route a packet to the destination is provided by the *source* host.
- Header contains ordered list of intermediate hosts, through which packet must traverse. Hence headers are of variable length.
- Headers can be handled either by rotation or stripping or pointer-based approach.
- Source routing is classified as either *strict* or *loose*.

✓Strict source route specifies every node along the path

✓Loose source route specifies set of nodes to be traversed



Rotation *Stripping* *Pointer*

- When a frame arrives, the bridge performs a *look-up* on the table.
- Outgoing port for the destination is obtained and the frame is sent on that port.

6. HOW LEARNING (TRANSPARENT) BRIDGE BUILDS FORWARDING TABLE? EXPLAIN WITH AN EXAMPLE. [CO4 – L2]

Learning bridges builds forwarding table gradually by learning from frame movements. Forwarding table is *empty* when the bridge boots up.

Bridge uses *source* address to add entries and *destination* address to forward frames.

Source address and incoming port is *appended* to the table, if an entry does not exist.

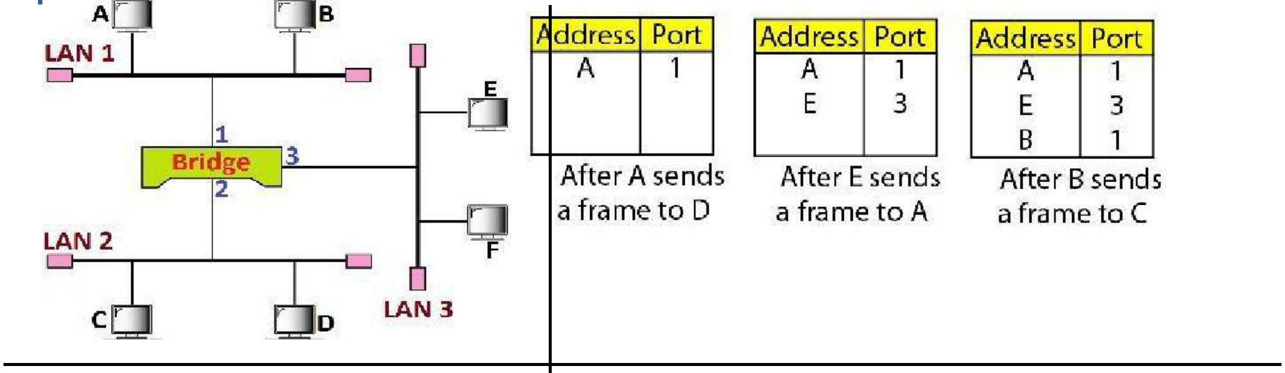
Forwarding table is looked up for destination address:

o If source and destination are from same LAN, then the frame is *dropped*.

o If an entry exists, then frame is *forwarded* on the corresponding port. o Otherwise, the frame is *flooded* on all other ports.

Learning process continues as bridge forwards frames and optimizes forwarding decision.

Example



Address	Port
A	1

After A sends a frame to D

Address	Port
A	1
E	3

After E sends a frame to A

Address	Port
A	1
E	3
B	1

After B sends a frame to C

Bridged network *Forwarding Table*

When host *A* sends a frame to *D*:

o Bridge has no entry for either station *D* or *A*

- o From source address, the bridge learns that station *A* is located on the LAN connected to port *1*, i.e., frames destined for *A* must be sent out through port *1*.
- o Bridge *appends* entry to the table and *floods* the frame on all other ports.

When host *E* sends a frame to *A*:

- p Bridge has an entry for host *A*, so it forwards the frame only to port *1*.
- o It adds source address of the frame, i.e., *E*, to the table.

When host *B* sends a frame to *C*:

- p Bridge has no entry for station *C.*
- o It floods the network and adds one more entry to the table.

When does learning bridge fail?

Learning bridge works fine as long as there is *no loop*.

Loops are formed when *redundant* bridges are introduced to improve reliability. When loop exists, multiple copies of the frame exists as they are flooded by bridges.

7. EXPLAIN THE WORKING OF SPANNING TREE ALGORITHM WITH AN EXAMPLE. [CO4 – L2]

IEEE 802.1 mandates bridges to use *spanning tree algorithm* to create loop-less topology.

Spanning tree algorithm creates a sub-graph that has no loops, i.e., each LAN can be reached from any other LAN through one path only.

Each bridge decides the ports on which it is willing to forward frames

Some ports are removed, reducing the extended LAN to an acyclic graph.

Spanning tree algorithm is *dynamic*, i.e., bridges reconfigure the spanning tree due to some failure or additions or deletions.

Algorithm

Each bridge has a unique identifier.

Bridges exchange configuration message (Y, d, X), known as bridge protocol data unit

(BPDU) to decide on root/designated bridge, where:

o *Y*—id of the root bridge according to sending bridge.
o *d*—distance in hops from sending bridge to root
bridge. o *X*—id of the bridge that is sending the
message.

System stabilizes with the selection of root bridge and designated bridges.

Root Bridge

Initially each bridge considers itself as root and broadcasts BPDU with distance 0.

A bridge accepts another bridge as root, if it receives a BPDU that has:

- o a root with a *smaller id.*
- o a root with an equal id but *shorter distance.*
- o root id and distance are equal, but *sending bridge* has a smaller id.

Once a bridge accepts another bridge as root, it

- p *Stops* generation of its own messages

- Forwards messages after incrementing *distance-to-root* field

Eventually, bridge with the smallest id is selected as the root bridge.
Root bridge always floods frames on all ports.
Absence of periodical message from root, forces bridges to elect a new root bridge.

Designated Bridge

All bridges connected to a LAN *elect* a designated bridge.

Each bridge computes *shortest* path to the root and notes the port on the path.

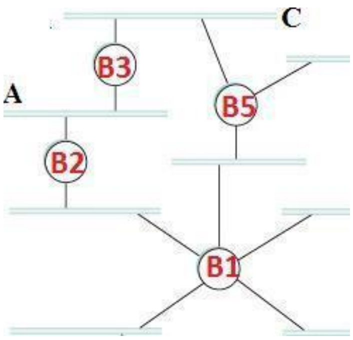
Each LAN's designated bridge is the one that is *closest* to the root.

If two or more bridges are equally close to root, then bridge with smallest *id* is chosen.

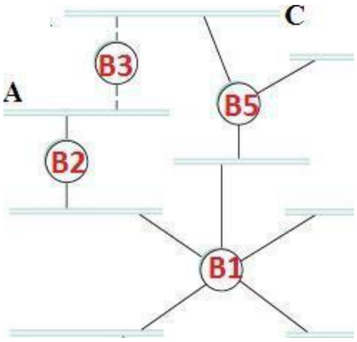
Designated bridge is responsible for *forwarding* frames to the root bridge.

A bridge *stops* sending messages over a port, when it's not designated bridge for that port

Example



Extended LAN with loop



Loop-less topology at B3

B3 receives (B2, 0, B2). B3 accepts B2 as root, since B2 is the lower id.
B3 increments the distance advertised by B2 and sends (B2, 1, B3) towards B5.
B2 accepts B1 as root because it has the lower id and sends (B1, 1, B2) to B3.
B5 accepts B1 as root and sends (B1, 1, B5) to B3.
B3 accepts B1 as root, and knows that both B2 and B5 are closer to the root than itself.
B3 stops forwarding messages on both its interfaces.
B2 and B5 are chosen as the designated bridges for LAN A and C respectively.

8. WRITE SHORT NOTES ON VLAN. [CO4 – L1]

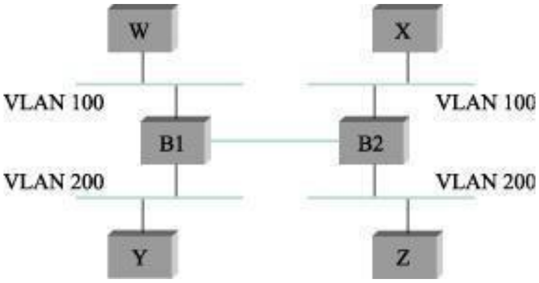
An extended LAN is partitioned into several LANs, configured by *software*, not by physical wiring, known as virtual LAN (VLAN).

VLANs group stations belonging to one or more physical LANs into broadcast domains.

Stations in a VLAN communicate with one another as though they belonged to the same physical segment. Each VLAN is a *workgroup* in the organization.

In VLAN, it is possible to change the logical topology without moving any wires or changing any address. Changes are made in bridge configuration.

Each VLAN is assigned an *identifier* and packets can only travel from one segment to another if both segments have the same identifier.



Example
Hosts *W* and *X* are configured as *VLAN 100*, hosts *Y* and *Z* as *VLAN 200*.

When a packet sent by host *X* arrives at bridge *B2*, the bridge inserts a VLAN header between Ethernet header and its payload with VLAN ID as *100*.

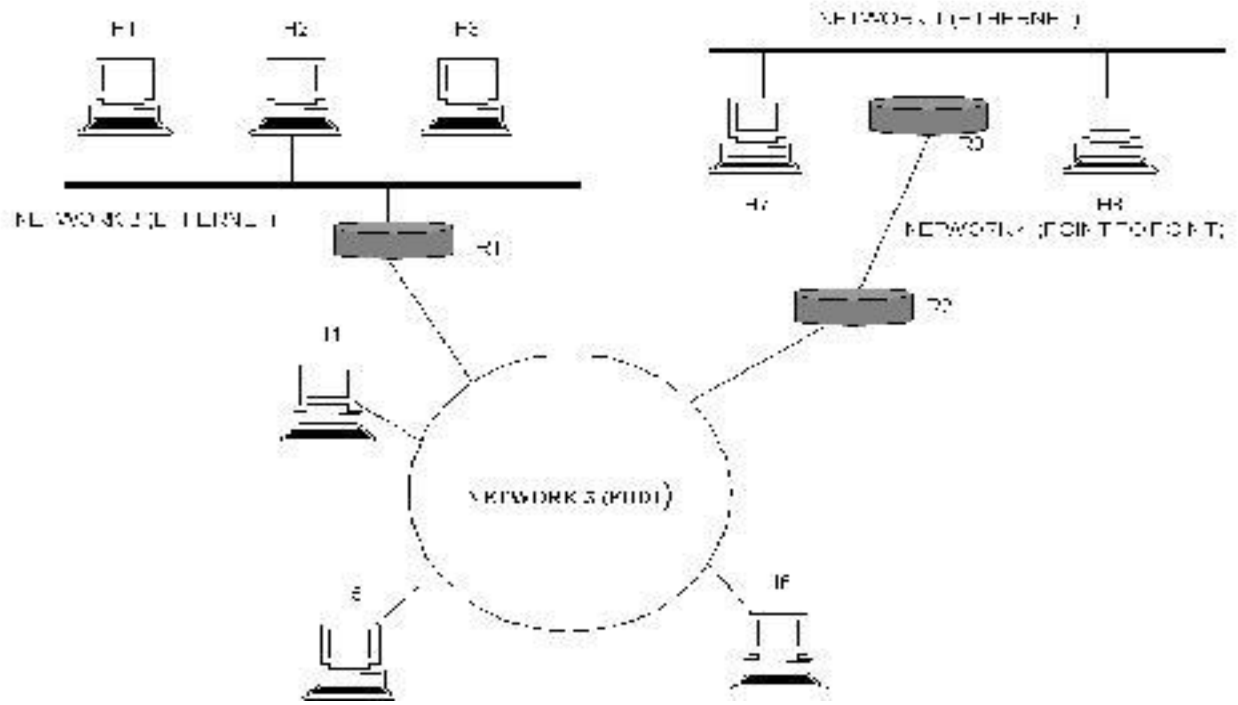
Bridge forwards the packet, only on interfaces that is part of *VLAN 100*.

Packet is forwarded to bridge *B1*, which forward the packet to host *W* but not to *Y*.

Advantages of VLAN.
VLANs reduce the migration cost of stations moving from one group to another.
VLANs can reduce traffic if the multicasting capability of IP was used.
Broadcast messages of one group will not be received by other group members.

9. DISCUSS INTERNETWORKING IN DETAIL: [CO4 – H1]

An internetwork is often referred to as a network of networks because it is made up of lots of smaller networks. The nodes that interconnect the networks are called routers. They are also sometimes called gateways, but since this term has several other connotations, we restrict our usage to router. The internet protocol is the key tool used today to build scalable, heterogeneous internetwork



Service Model

The main concern in defining a service model for an internetwork is that we can provide a host-to-host service only if this service can somehow be provided over each of the underlying physical networks. For Example, it would be no good deciding that our internetwork service model was going to provide guaranteed delivery of every packet in 1 ms or less if there were underlying network technologies that could arbitrarily delay packets.

The IP service model can be thought of as having two parts: an addressing scheme, which provides a way to identify all hosts in the internetwork, and a datagram (connectionless) model of data delivery. This service model is sometimes called best effort because, although IP makes every effort to delivery datagram, it makes no guarantees.

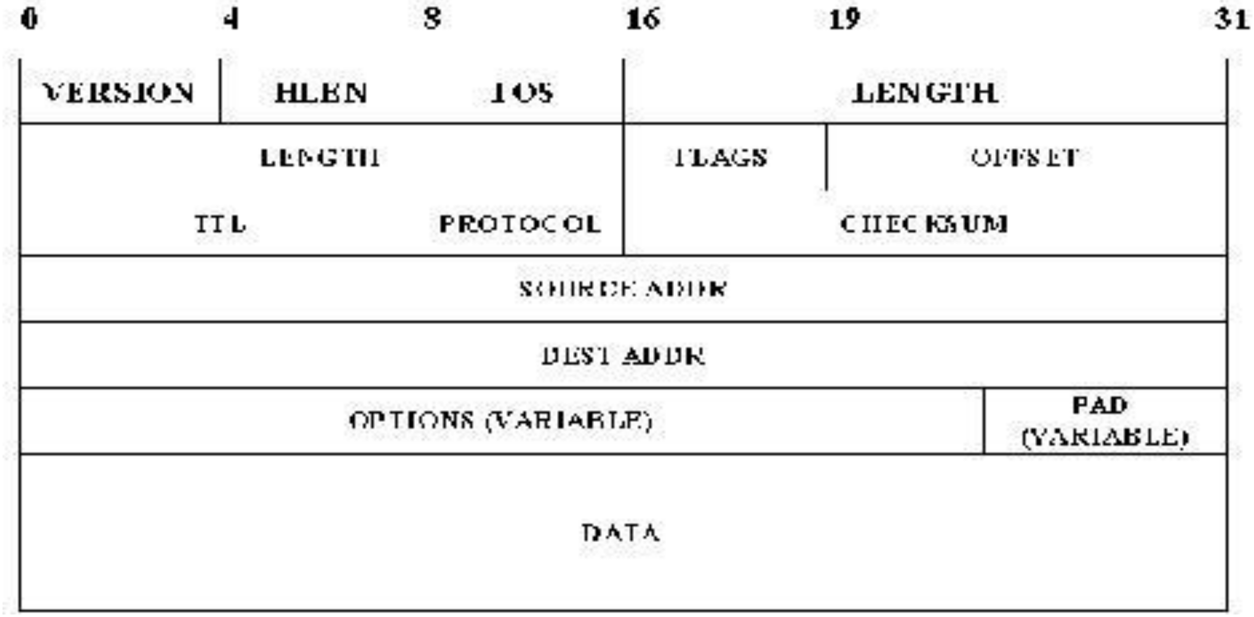
Datagram Delivery

A datagram is a type of packet that happens to be sent in a connectionless manner over a network. Every datagram carries enough information to let network forward the packet to its correct destination; there is no need for any advance setup mechanism to tell the network what to do when the packet arrives. The network makes its best effort to get it to the desired destination. The best-effort part means that if something goes wrong and the packet gets lost, corrupted, misdelivered,or in any way fails to reach its intended destination, the network does nothing-it made its best effort, and that is all it had to do. It does not make any attempt to recover from the failure. This is sometimes called an unreliable service.

PACKET FORMAT

The IP datagram, like most packets, consists of a header followed by a number of bytes of data.

The Version field specifies the version of IP. The current version of IP is 4, and it is sometimes called IPv4^2.putting this field right at the start of the datagram makes it easy for everything else in the packet format to be redefined in subsequent versions; the header processing software starts off by looking at the version and then branches off to process the rest of the packet according to the appropriate format.



The next field, HLEN, specifies the length of the header in 32-bit words. When there are no options, which is most of the time, the header is 5 words (20 bytes) long. The 8_bit type of service (TOS) field has had a number of different definitions over the years, but its basic function is to allow packets to be treated differently based on application needs. For example, the TOS value might determine whether or not a packet should be placed in a special queue that receives low delay.

The next 16-bit of the header contain the Length of the datagram, including the header. Unlike the HLEN field, the Length field counts bytes rather than words. Thus, the maximum size of an IP datagram is 65,535 bytes. The physical network, over which IP is running, however, may not support such long packets. For this reason, IP supports a fragmentation and reassembly process, the second word of the header contains information about fragmentation. The next byte is the time to live (TTL) field. The intent of the field is to catch packets that have been going around in routing loops and discard them, rather than let them consume resources indefinitely.

The Protocol field is simply a demultiplexing key that identifies the higher-level protocol to which this packet should be passed. These are values defined for TCP (6), UDP (17), and many other protocols that may sit above IP in the protocol graph.

The Checksum is calculated by considering the entire IP header as a sequence of 16-bit words, adding them up using ones complement arithmetic, and taking the ones complement of the result.

The last two required fields in the header are the SourceAddr and the DestinationAddr for the packet. The latter is the key to datagram delivery: every packet contains a full address for its intended destination so that forwarding decisions can be made at each router. The source address is required tom allow recipients to decide if they want to accept the packet and to enable them to reply.

Finally, there may be a number of options at the end of the header. The presence or absence of options may be determined by examining the header length (HLen) field. While options are used fairly rarely, a complete IP implementation must handle them all.

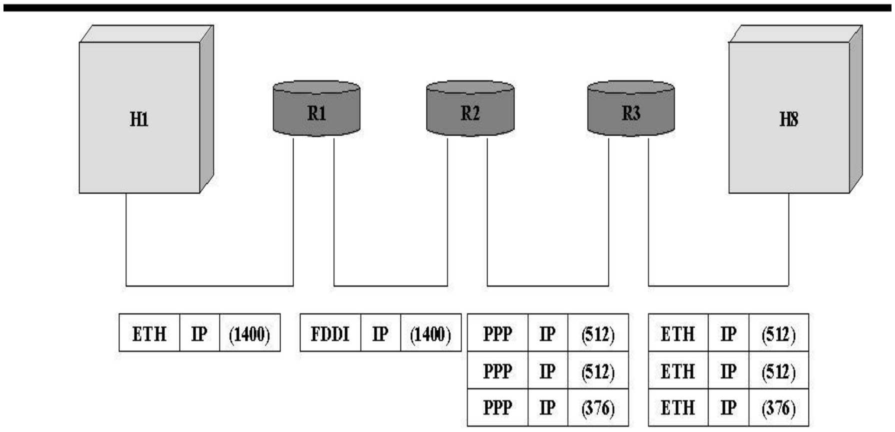
FRAGMENTATION AND REASSEMBLY:

One of the problems of providing a uniform host-to-host service model over a heterogeneous collection of network is that each network technology tends to have its own idea of how large a packet can be. For example, an Ethernet can accept packets up to 1,500 bytes long, while FDDI packets may be 4,500 bytes long.

This leaves two choices for the IP service model: make sure that all IP datagram are small enough to fit inside one packet on any network technology, or provide a means by which packets can be fragmented and reassembled when they are too big to go over a given network technology.

The latter turns out to be a good choice, especially when you consider the fact that new network technologies are always turning up, and IP needs to run over all of them; this would make it hard to pick a suitably small bound on datagram size.

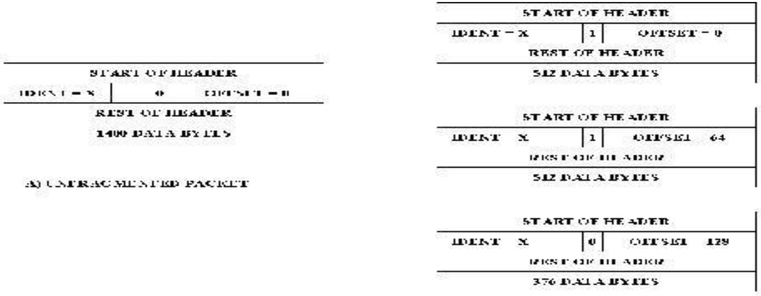
This also means that a host will not send needlessly small packets, which wastes bandwidth and consumes processing resources by acquiring more headers per byte of data sent. For example, two hosts connected to FDDI networks that are interconnected by a point-to-point link would not need to send packets small enough to fit on an Ethernet.



The central idea here is that every network type has a maximum transmission unit (MTU), which is the largest IP datagram that it can carry in a frame.

The unfragmented packet has 1,400 bytes of data and a 20-byte IP header. When the packet arrives at the R2, which has an MTU of 532 bytes, it has to be fragmented. A 532-byte MTU leaves 512 bytes for data after the 20-byte IP header, so the first fragment contains 512 bytes of data. The router sets the M bit in the Flags field, meaning that there are more fragments to follow, and it sets the offset to 0,since this fragmented contains the first part of the original datagram.

The data carried in the second fragment starts with the 513th byte of the original data, so the Offset field in this header is set to 64, which is 512/8. Why the division by 8? Because the designers of IP decided that fragmentation should always happen on 8-byte boundaries, which means that the Offset field counts 8-byte chunks, not bytes. The third fragment contains the last 376 bytes of data, and the offset is now 2*512/8=128. since this is the last fragment, the M bit is not set.



A) UNFRAGMENTED PACKET

B) FRAGMENTED PACKET

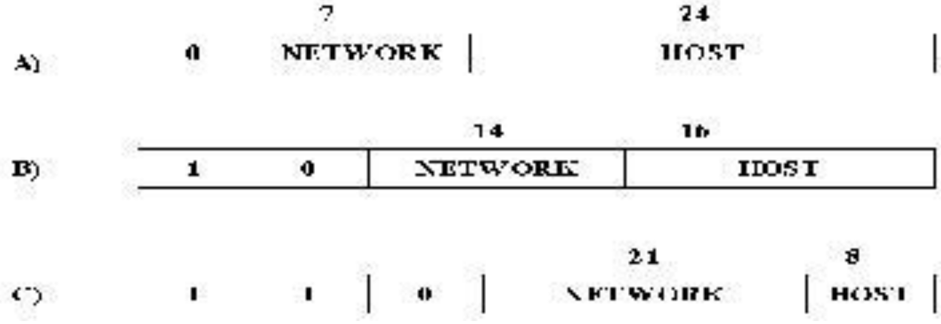
GLOBAL ADRESSES:

Global uniqueness is the first property that should be provided in an addressing scheme. Ethernet addresses are globally unique but not sufficient to address entire network. And also they are flat that is no structure in addressing.

IP addresses are hierarchical. They made up of two parts, they are a network part and a host part. The network part identifies the network to which the host is connected. All hosts which are connected to the same network have same network part in their IP address. The host part then identifies each host on the particular network.

The routers are host but they are connected with two networks. So they need to have an address on each network, one for each interface.
IP addresses are divided into three different classes. They are,

1. Class A
2. Class B
3. Class C

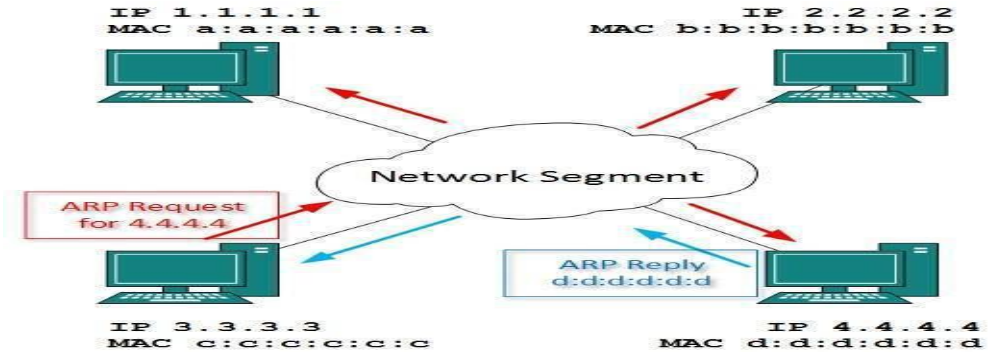


The class of an IP address is identified in the most significant few bits. If the first bit is 0, it is a class A address. If the first bit is 1 and the second bit is 0, it is a class B address. If the first two bits are 1 and the third bit is 0, t is a class C address.
Class A addresses have 7 bits for network part and 24 bits for host part. The 0 and 127 are reserved.
Class B addresses have 14 bits for network part and 16 bits for host part.
Class C addresses have 21 bits for network part and 8 bits for host part. The 0 and 127 are reserved. There are approximately 4 billion possible IP addresses, one half for class A, one quarter for class B and one-eighth for class C address.

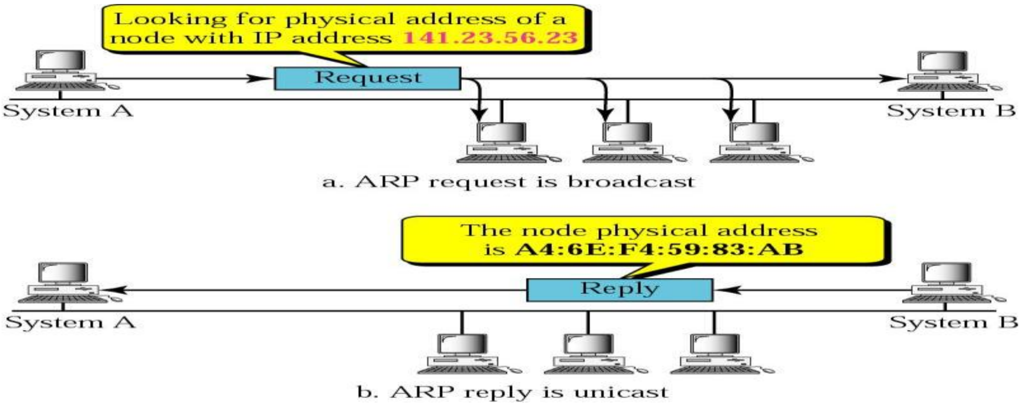
There are also class D and class E are there. But class D for multicast and class E are currently unused. IP addresses are written as four decimal integers separated via dots. Each integer represents the decimal value contained in 1 byte of the address, starting at the most significant.

10. EXPLAIN ADDRESS RESOLUTION PROTOCOL WITH HEADER FORMAT. [CO4 – L2]

While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.
On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. This way, for Layer-2 communication to take place, a mapping between the two is required.

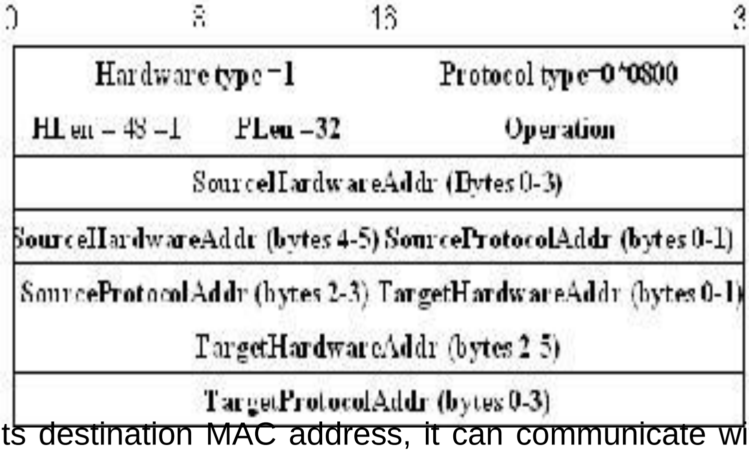


To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking, “Who has this IP address?” Because it is a broadcast, all hosts on the network segment (broadcast domain) receive this packet and process it. ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.


Looking for physical address of a node with IP address 141.23.56.23
Request
System A
System B
The node physical address is A4:6E:F4:59:83:AB
Reply
System A
System B

a. ARP request is broadcast

b. ARP reply is unicast



0	8	16	31
Hardware type -1		Protocol type-0x0800	
HLen – 48 –1	PLen –32	Operation	
SourceHardwareAddr (Bytes 0-3)			
SourceHardwareAddr (bytes 4-5)		SourceProtocolAddr (bytes 0-1)	
SourceProtocolAddr (bytes 2-3)		TargetHardwareAddr (bytes 0-1)	
TargetHardwareAddr (bytes 2 5)			
TargetProtocolAddr (bytes 0-3)			

Once the host gets destination MAC address, it can communicate with remote host using Layer-2 link protocol. This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they require to communicate, they can directly refer to their respective ARP cache.

Reverse ARP is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

11. EXPLAIN INTERNET CONTROL MESSAGE PROTOCOL (ICMP) [CO4 – L2]

Internet Control Message Protocol (ICMP) is used to report error messages to source host and diagnose network problems. ICMP message is encapsulated within an IP packet

Error reporting

Destination Unreachable—When a router cannot route a datagram, the datagram is discarded and sends a destination unreachable message to source host.

Source Quench—When a router or host discards a datagram due to congestion, it sends a source-quench message to the source host. This message acts as flow control.

Time Exceeded—Router discards a datagram when TTL field becomes 0 and a time- exceeded message is sent to the source host.

Parameter Problem—If a router discovers ambiguous or missing value in any field of the datagram, it discards the datagram and sends parameter problem message to source.

Redirection—Redirect messages are sent by the default router to inform the source host to update its forwarding table when the packet is routed on a wrong path.

Query Messages

Echo Request & Reply—The combination of echo-request and echo-reply messages determines whether two systems can communicate at the IP level.

Timestamp Request & Reply—Two machines can use the timestamp request and timestamp reply messages to determine the round-trip time (RTT).

Address Mask Request & Reply—A host to obtain its subnet mask, sends an address mask request message to the router, which responds with an address mask reply message.

Router Advertisement—A host broadcasts a router solicitation message to know about the router. Router broadcasts its routing information with router advertisement message.

12. EXPLAIN DHCP-DYNAMIC HOST CONFIGURATION PROTOCOL. [CO4 – L2]

It allows a host to have an IP address automatically and also to learn the additional information.

The additional information like

- Its subnet mask
- Address of its first top router
- Address of its level DNS server

Generally IP address has

- Network part
- host part

Network part should be the same for all hosts on the network.

There occur drawbacks in manual IP configuration.

Drawbacks

1. Two host getting same IP address.
2. Host gets correct n/w number.

To resolve such issues there is a need of automated configuration methods. DHCP protocol is used. DHCP relies on the existence of a DHCP server that is responsible for providing configuration information to hosts. It must have at least 1DHCP server for an administrative domain.

DHCP Server

DHCP Server works as a central respiratory for host configuration information.

For every host , the configuration information is stored in the DHCP server.

So whenever the host is booted it will automatically retrieves the address.

Advantages:

1. It saves the n/w administrator from having to assign address to individual hosts.
2. Maintains the list of address of individual host & minimizes the manual configuration.

Operations of DHCP

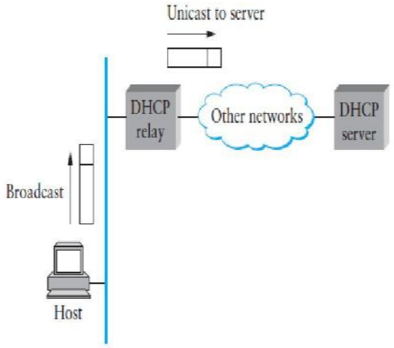


Fig :A DHCP relay agent receives a broadcast DHCPDISCOVER message from a host and sends a Unicast DHCPDISCOVER to the DHCP server

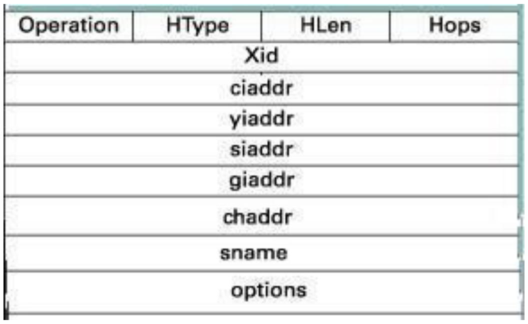
DHCP server maintains list of address which it hands out to hosts on demand.

1. To contact a DHCP server, a newly booted or attached host sends a DHCPDISCOVER message to a special IP address (255.255.255.255) that is an IP broadcast address. This means it will be received by all hosts and routers on that network.
2.The server would then reply to the host that generated the discovery message(all the other nodes would ignore it).
3. DHCP Server will reply for the request.

Another approach is

1. DHCP uses the concept of a *relay agent*. There is at least one relay agent on each network, and it is configured with just one piece of information: the IP address of the DHCP server.
2. When a relay agent receives a DHCPDISCOVER message, it unicasts it to the DHCP server and awaits the response, which it will then send back to the requesting client.The process of relaying a message from a host to a remote DHCP server is shown in Figure(Sir attach the figure from charulatha book).

DHCP Protocol Format:



Operation	HType	HLen	Hops
Xid			
ciaddr			
yiaddr			
siaddr			
giaddr			
chaddr			
sname			
options			

Operation—specifies type of DHCP packet.
Xid—specifies the transaction id.
ciaddr—specifies client IP address in case of DHCPREQUEST
yiaddr— known as *your IP address*, filled by DHCP server.
siaddr—contains IP address of the DHCP server.
giaddr—contains IP address of the Gateway or relay agent.
chaddr—contains hardware (physical) address of the client.
options—contains information such as lease duration, default route, DNS server, etc.

Dynamic Address Allocation

1. DHCP server is configured with range of addresses to be assigned to hosts on demand.

To contact DHCP server, client broadcasts a DHCPDISCOVER message with IP address 255.255.255.255 and it's physical address placed in chaddr field.

2. DHCP server selects an unassigned IP address for yiaddr field and adds an entry to dynamic database along with client's physical address.
3. DHCP server sends DHCPOFFER message containing client's IP and physical address, server IP address and options.
4. Client sends a DHCPREQUEST message, requesting the offered address.
5. Based on transaction id, the DHCP server acknowledges with a DHCPACK message.
6. When lease period expires, client attempts to renew. It’s up to server to accept or reject it.

Disadvantage:

It introduces some more complexity into network management, since it makes the binding between physical hosts and IP addresses much more dynamic.

13. WRITE SHORT NOTES ON CIDR OR SUPERNETING. [CO4 – L1]

1. Subnetting does not prevent an organization opting for Class B. Address efficiency for Class B can be as low as 0.39% (256 / 65535).

If Class C addresses were given instead of Class B, then routing tables gets larger.

Classless Interdomain Routing (CIDR) tries to balance between minimize the number of routing table entries and handling addresses space efficiently.

CIDR aggregates routes, by which an entry in forwarding table is used to reach multiple networks. It collapses multiple addresses into a single supernet, i.e., supernetting.

Example
Consider an organization with 16 Class C networks.

Instead of providing 16 addresses at random, a block of contiguous Class C address is given. For example, from 192.4.16 to 192.4.31

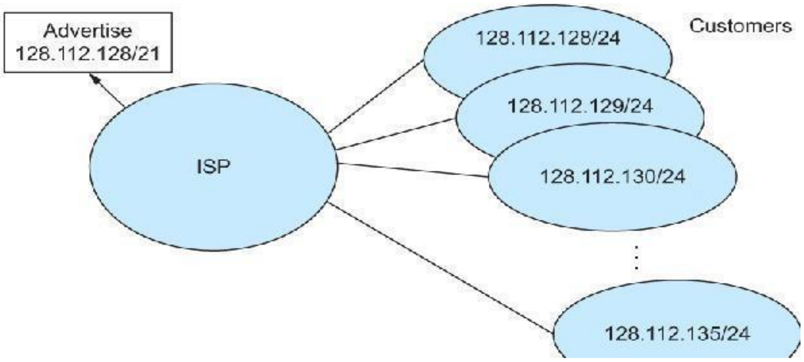
Bitwise analysis show 20 MSBs (11000000 00000100 0001) are same. Thus a 20-bit network number is created, i.e., range between Class B and C network.

Thus higher address efficiency is achieved by providing small chunks of address, smaller than Class B network. Thus a single network prefix is used in forwarding table.

CIDR uses a new type of notation to represent network numbers or prefixes.

It is represented as /X, where X is the prefix length in bits. For example, 192.4.16/20
Addresses in a block must be contiguous and number of addresses must be powers of 2.

Example



When different customers are connected to a service provider, prefixes can be assigned such that they share a common, further aggregation can be achieved.

Consider an ISP providing internet connectivity to 8 customers. All customer prefix starts with the same 21 bits.
Since all customers are reachable through the same provider network, a single route is advertised by ISP with common 21-bit prefix that all customers share.

UNIT III
ROUTING

PART-A

1. Define packet switching. [CO4 – L1 NOV/DEC 2015, MAY/JUNE 2016]

A packet switch is a device with several inputs and outputs leading to and from the hosts that the switch interconnects.

2. What is a virtual circuit? [CO4 – L1]

A logical circuit made between the sending and receiving computers. The connection is made after both computers do handshaking. After the connection, all packets follow the same route and arrive in sequence.

3. What are datagrams? [CO4 – L1]

In datagram approach, each packet is treated independently from all others. Even when one packet represents just a place of a multi packet transmission, the network treats it although it existed alone. Packets in this technology are referred to as datagram.

4. What is meant by switched virtual circuit? [CO4 – L1]

Switched virtual circuit format is comparable conceptually to dial-up line in circuit switching. In this method, a virtual circuit is created whenever it is needed and exits only for the duration of specific exchange.

5. What is meant by Permanent virtual circuit? [CO4 – L1]

Permanent virtual circuits are comparable to leased lines in circuit switching. In this method, the same virtual circuit is provided between two uses on a continuous basis. The circuit is dedicated to the specific uses.

6. What are the properties in star topology? [CO4 – L1]

Even though a switch has a fixed number of inputs and outputs, which limits the number of hosts that can be connected to a single switch, large networks can be built by interconnecting a number of switches.

We can connect switches to each other and to hosts using point-to point links, which typically means that we can build networks of large geographic scope.

7. What is VCI? [CO4 – L1]

Virtual Circuit Identifier that uniquely identifies the connection at this switch, and which will be carried inside the header of the packets that belongs to this connection.

8. What is hop-by-hop flow control? [CO4 – L1]

Each node is ensured of having the buffers it needs to queue the packets that arrive on that circuit. This basic strategy is usually called hop-by-hop flow control.

9. Explain the term best-effort. [CO4 – L2]

If something goes wrong and the packet gets lost, corrupted, misdelivered, or in any way fails to reach its intended destination, the network does nothing.

10. What is maximum transmission unit? [CO4 – L1]

MTU- which is the largest IP datagram that it can carry in a frame.

11. Define Routing. [CO4 – L1]

Routing is the process of finding the shortest path and delivering the data through shortest path.

12. Define ICMP. [CO4 – L1]

Internet Control Message Protocol is a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP datagram successfully.

13. Write the keys for understanding the distance vector routing. [CO4 – L1]

The three keys for understanding the algorithm are,

- Knowledge about the whole networks
- Routing only to neighbors
- Information sharing at regular intervals

14. Write the keys for understanding the link state routing. [CO4 – L1]

Knowledge about the neighborhood.
Routing to all neighbors.
Information sharing when there is a range.

15. How the packet cost is referred in distance vector and link state routing? [CO4 – L2]

In distance vector routing, cost refer to hop count while in case of link state routing, cost is a weighted value based on a variety of factors such as security levels, traffic or the state of the link.

16. Define Reliable flooding. [CO4 – L1]

It is the process of making sure that all the nodes participating in the routing protocol get a copy of the link state information from all the other nodes.

17. What are the features in OSPF? [CO4 – L1]

Authentication of routing messages.
Additional hierarchy.
Load balancing.

18. Define Subnetting. [CO4 – L1]

Subnetting provides an elegantly simple way to reduce the total number of network numbers that are assigned. The idea is to take a single IP network number and allocate the IP address with that network to several physical networks, which are now referred to as subnets.

19. What are the different types of AS? [CO4 – L1]

Stub AS
Multi homed AS, Transit AS

20. What is an Area? [CO4 – L1]
An Area is a set of routers that are administratively configured to exchange link-state information with each other. There is one special area- the backbone area, also known as area 0.

21. What is Source Specific Multicast? [CO4 – L1]
SSM , a receiving host specifies both a multicast group and a specific host .the receiving host would then receive multicast addressed to the specified group, but only if they are from the special sender.

22. What is meant by congestion? [CO4 – L1]
Congestion in a network occurs if user sends data into the network at a rate greater than that allowed by network resources.

23. Why the congestion occurs in network? [CO4 – L1]
20.
Congestion occurs because the switches in a network have a limited buffer size to store arrived packets.

24. What is LSP? [CO4 – L1]
In link state routing, a small packet containing routing information sent by a router to all other routers is called link state packet.

PART-B

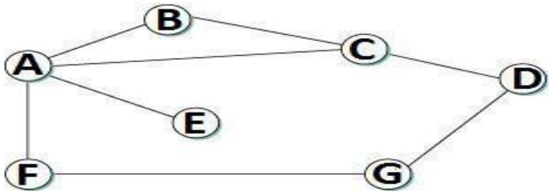
1. EXPLAIN DISTANCE VECTOR ROUTING (OR) ROUTING INFORMATION PROTOCOL (OR) BELLMAN-FORD ALGORITHM. [CO4 – L2 NOV/DEC 2015]

Each node knows the distance (cost) to each of its directly connected neighbors.

Nodes construct a vector (Destination, Cost, NextHop) and distributes to its neighbors.

Nodes compute routing table of minimum distance to every other node via NextHop using information obtained from its neighbors.

Initial State



In given network, cost of each link is 1 hop.

Each node sets a distance of 1 (hop) to its immediate neighbor and cost to itself as 0.

Distance for non-neighbors is marked as unreachable with value ∞ (infinity).

For node A, nodes B, C, E and F are reachable, whereas nodes D and G are unreachable.

Destination	Cost	NextHop
A	0	A
B	1	B
C	1	C
D	∞	—
E	1	E
F	1	F
G	∞	—

Node A's initial table

Destination	Cost	NextHop
A	1	A
B	1	B
C	0	C
D	1	D
E	∞	—
F	∞	—
G	∞	—

Node C's initial table

Destination	Cost	NextHop
A	1	A
B	∞	—
C	∞	—
D	∞	—
E	∞	—
F	0	F
G	1	G

Node F's initial table

Sharing & Updation

- ➢ Each node *sends* its initial table (distance vector) to neighbors and receives their estimate.
- ➢ Node *A* sends its table to nodes *B*, *C*, *E* & *F* and receives tables from nodes *B*, *C*, *E* & *F*.
- ➢ Each node *updates* its routing table by comparing with each of its neighbor's table
- ➢ For each destination, Total Cost is computed as:

  Total Cost = Cost (*Node* to *Neighbor*) + Cost (*Neighbor* to *Destination*)
- ➢ If Total Cost < Cost then Cost = Total Cost and NextHop = *Neighbor*
- ➢ Node *A learns* from *C*'s table to reach node *D* and from *F*'s table to reach node *G*.

  Total Cost to reach node *D* via *C* = Cost (*A* to *C*) + Cost(*C* to *D*) = 1 + 1=2

  - ✓ Since 2 < ∞, entry for destination *D* in *A*'s table is changed to (*D*, 2, *C*)

  Total Cost to reach node *G* via *F* = Cost(*A* to *F*) + Cost(*F* to *G*) = 1 + 1=2

  - ✓ Since 2 < ∞, entry for destination *G* in *A*'s table is changed to (*G*, 2, *F*)
- ➢ Each node builds *complete* routing table after few exchanges amongst its neighbors.

Destinatio	Cos	NextHo
A	0	A
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	2	F

Node A's final routing table

- □ System stabilizes when all nodes have complete routing information, i.e., *convergence*.
- □ Routing tables are exchanged *periodically* (every 30 sec.) and in case of *triggered* update.

Triggered Update

Link failure is assumed, if a node does not receive periodic updates from a neighbor. Infinite cost is assigned to that neighbor and immediately shares with other neighbors.

Neighbors update their neighbors and so on. This is known as triggered update.

Assume that node F detects that its link to G has failed.

- ✓ Node *F sets* distance to *G* as ∞ and shares its table with *A*.

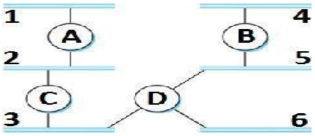
- ✓ Node *A updates* its distance to *G* as ∞.
- ✓ Meanwhile, node *A* receives *periodic* update from *C* with distance to *G* as 2 hops.
- ✓ Node *A updates* its distance to *G* as 3 hops via *C* and shares it with *F*.
- ✓ Eventually node *F* is updated to reach *G* via *A* in 4 hops.

Network stabilizes after few updates, when an alternate path is found.

Routing Information Protocol (RIP)

RIP is an intra-domain routing protocol based on distance-vector algorithm.

Example Network



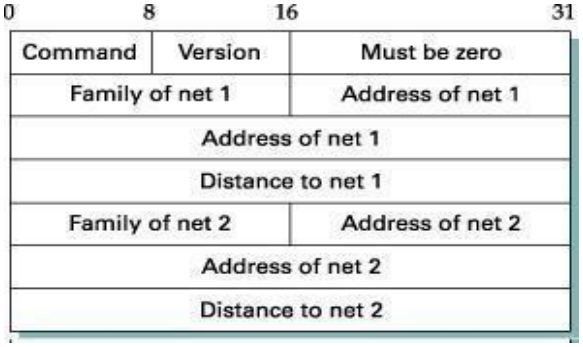
Routers advertise the cost of reaching networks. Cost of reaching each link is 1 hop. For example, router C advertises to A that it can reach network 2, 3 at cost 0 (directly connected), networks 5, 6 at cost 1 and network 4 at cost 2.

Each router updates cost and next hop for each network number.

Infinity is defined as 16, i.e., any route cannot have more than 15 hops. Therefore RIP can be implemented on small-sized networks only.

Advertisements are sent every 30 seconds or in case of triggered update.

RIP packet format (version 2) contains (network address, distance) pairs.



<table>
<tr><th>0</th><th>8</th><th>16 31</th></tr>
<tr><td>Command</td><td>Version</td><td>Must be zero</td></tr>
<tr><td colspan="2">Family of net 1</td><td>Address of net 1</td></tr>
<tr><td colspan="3">Address of net 1</td></tr>
<tr><td colspan="3">Distance to net 1</td></tr>
<tr><td colspan="2">Family of net 2</td><td>Address of net 2</td></tr>
<tr><td colspan="3">Address of net 2</td></tr>
<tr><td colspan="3">Distance to net 2</td></tr>
</table>

2. EXPLAIN LINK STATE ROUTING (OR) OSPF PROTOCOL (OR) SHORTEST PATH ALGORITHM WITH AN EXAMPLE. [CO4 – L2]

Each node knows state of link to its neighbors and cost.

Nodes create an update packet called link-state packet (LSP) that contains:

- o ID of the node
- o List of neighbors for that node and associated cost

- 64-bit Sequence number
- Time to live

Link-state routing protocols rely on two mechanisms:

- Reliable dissemination of link-state information to all other nodes Route calculation from the accumulated link-state knowledge

Reliable Flooding

Each node sends its LSP out on each of its directly connected links.

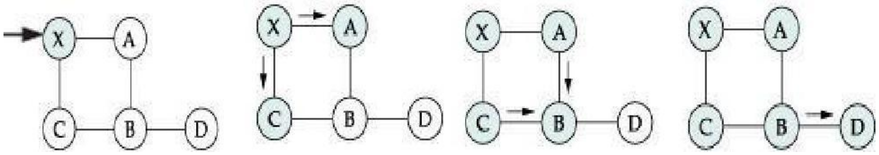
When a node receives LSP of another node, checks if it has an LSP already for that node.

If not, it stores and forwards the LSP on all other links except the incoming one.

Else if the received LSP has a bigger sequence number, then it is stored and forwarded. Older LSP for that node is discarded.

Otherwise discard the received LSP, since it is not latest for that node.

Thus recent LSP of a node eventually reaches all nodes, i.e., reliable flooding.



Flooding of LSP in a small network is as follows:

- When node *X* receives *Y*'s LSP (*fig a*), it floods onto its neighbors *A* and

Nodes *A* and *C* forward it to *B*, but does not sends it back to *X* (*fig c*).

- Node *B* receives two copies of LSP with same sequence number.
- Accepts one LSP and forwards it to *D* (*fig d*). Flooding is complete.

LSP is generated either periodically or when there is a change in the topology.

Route Calculation

Each node knows the entire topology, once it has LSP from every other node.

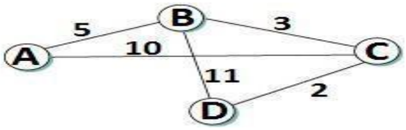
Forward search algorithm is used to compute routing table from the received LSPs.

Each node maintains two lists, namely Tentative and Confirmed with entries of the form (Destination, Cost, NextHop).

Forward Search algorithm (Djkstra's Shortest Path)

1. Initialize the Confirmed list with an entry for the Node (Cost = 0).
2. Node just added to Confirmed list is called Next. Its LSP is examined.
3. For each neighbor of Next, calculate cost to reach each neighbor as Cost (Node to Next) + Cost (Next to Neighbor).
   a. If Neighbor is neither in Confirmed nor in Tentative list, then add (Neighbor, Cost, NextHop) to Tentative list.
   b. If Neighbor is in Tentative list, and Cost is less than existing cost, then replace the entry with (Neighbor, Cost, NextHop).

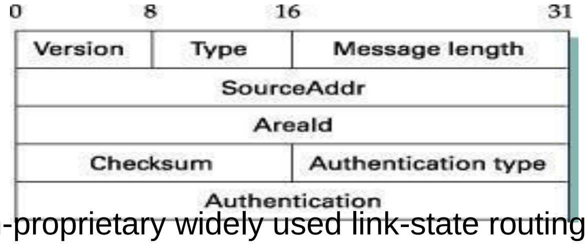
4. If Tentative list is empty then *Stop*, otherwise move *least* cost entry from Tentative list to Confirmed list. Go to *Step 2*.



- For the given network, the process of building routing table for node *D* is tabulated

Step	Confirme	Tentative	Comment
1	(D, 0, –)		*D* is moved to Confirmed list initially
Step	Confirmed	Tentative	*Comment*
2	(D, 0, –)	(B, 11, B)	*Based on D's LSP, its immediate neighbors B and C are*
3	(D, 0, –)	(B, 11, B)	*Lowest cost entry C in Tentative list is moved to Confirmed*
4	(D, 0, –)	(B, 5, C)	*Cost to reach B through C is 5, so the entry (B, 11, B) is*
5	(D, 0, –)	(A, 12, C)	*Lowest cost entry B is moved to Confirmed list. B's LSP is*
6	(D, 0, –)	(A, 10, C)	*Since A could be reached through B at a lower cost than the*
7	(D, 0, –)		*Only member A is moved to Confirmed list. Process*

Open Shortest Path First Protocol (OSPF)



OSPF is a non-proprietary widely used link-state routing protocol. Features added are:

Authentication—Malicious host can collapse a network by advertising to reach every host with cost 0. Such disasters are averted by authenticating routing updates.

Additional hierarchy—Domain is partitioned into areas, i.e., OSPF is more scalable.

Load balancing—Multiple routes to the same place are assigned same cost. Thus traffic is distributed evenly.

Version—represents the current version, i.e., 2.
Type—represents the type (1–5) of OSPF message.
SourceAddr—identifies the sender
AreaId—32-bit identifier of the area in which the node is located
Checksum—16-bit internet checksum
Authentication type—1 (simple password), 2 (cryptographic authentication).
Authentication—contains password or cryptographic checksum

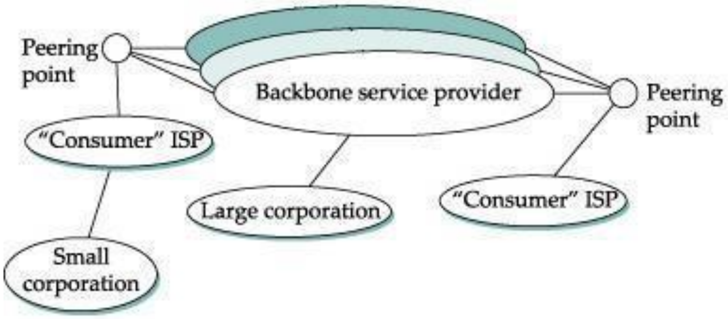
2. DISCUSS INTERDOMAIN ROUTING (OR) BORDER GATEWAY PROTOCOL. [CO4 – H1]

Internet is organized as autonomous systems (AS) to aggregate routing information.

Interdomain routing shares reachability information between autonomous systems.

Border Gateway Protocol has replaced *EGP* as major interdomain routing protocol.

Internet Structure



Internet has *backbone* networks and *sites*. Providers connect at a peering point.

Traffic on the internet is of two types:

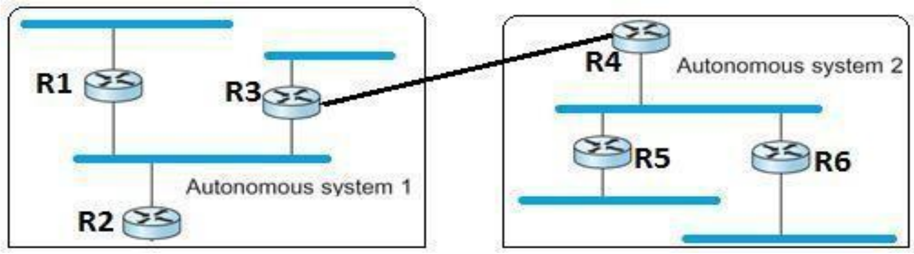
- traffic within an autonomous system is called local.
- traffic that passes through an autonomous system is called transit.

Autonomous Systems (AS) are classified as:

- Stub AS is connected to only one another autonomous system and carries local traffic only (e.g. Small corporation).
- Multihomed AS has connections to multiple autonomous systems but refuses to carry transit traffic (e.g. Large corporation).
- Transit AS has connections to multiple autonomous systems and is designed to carry transit traffic (e.g. Backbone service provider).

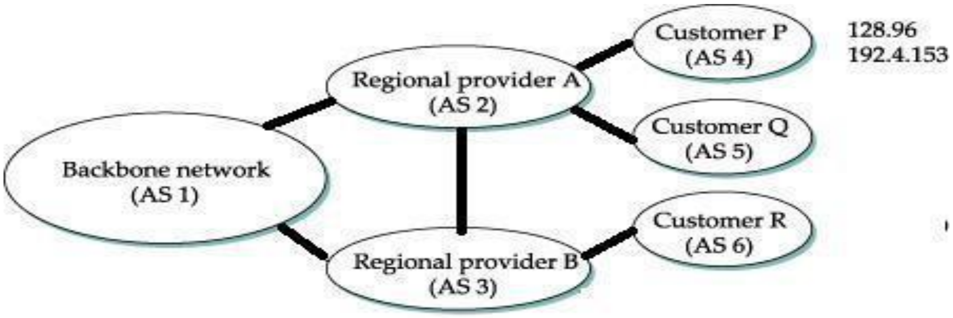
Border Gateway Protocol (BGP-4)

BGP views internet as a set of autonomous systems interconnected arbitrarily.

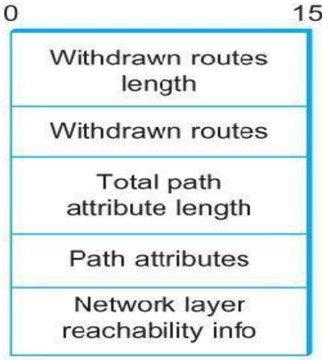


- Each AS have a border router (gateway), by which packets enter and leave that AS. In above figure, R3 and R4 are border routers.

- One of the router in each autonomous system is designated as BGP speaker.
- BGP Speaker exchange reachability information with other BGP speakers.
- BGP advertises complete path as enumerated list of AS (path vector) to reach a particular network. Paths must be without any loop, i.e., AS list is unique.



- For example, backbone network advertises that networks 128.96 and 192.4.153 can be reached along the path <AS1, AS2, AS4>.
- If there are multiple routes to a destination, BGP speaker chooses one based on policy.
- Speakers need not advertise any route to a destination, even if one exists.
- Advertised paths can be cancelled, if a link/node on the path goes down. This negative advertisement is known as withdrawn route.
- BGP is designed for classless addressing.
- Routes are not repeatedly sent. If there is no change, keep alive messages are sent.



BGP update packet format

4. DISCUSS INTERNET PROTOCOL VERSION 6 (IPV6). [CO4 – H1]

Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6.

IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.

Address Notation

Standard representation of IPv6 address is ***x* : *x* : *x* : *x* : *x* : *x* : *x* : *x*** where *x* is a 16-bit hexadecimal address separated by colon (:). For example,

47CD : 1234 : 4422 : ACO2 : 0022 : 1234 : A456 : 0124

IPv6 address with contiguous 0 bytes can be written compactly. For example,

47CD : 0000 : 0000 : 0000 : 0000 : 0000 : A456 : 0124 47CD : : A456 : 0124

IPv4 address is mapped to a IPv6 address by prefixing the 32-bit IPv4 address with 2 bytes of 1s and then zero-extending the result to 128 bits. For example,

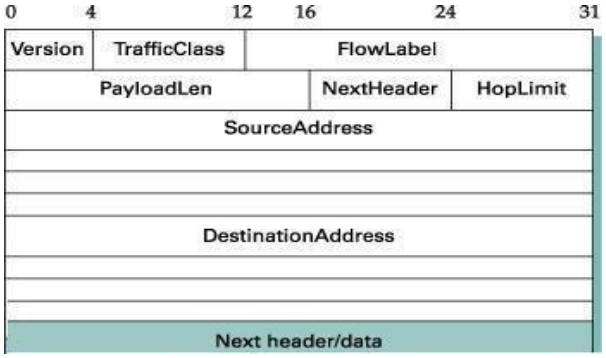
127.96.33.81 -> : : FFFF : 128.96.33.81

At present, there are few networks which are running on IPv6. There are some transition mechanisms available for IPv6 enabled networks to speak and roam around different networks easily on IPv4. These are:

- Dual stack implementation
- Tunnelling
- NAT-PT

Packet Format

IPv6 base header is 40 bytes long.



Version—specifies the IP version, i.e., 6.

TrafficClass—defines priority of the packet with respect to traffic congestion. It is either congestion-controlled or non-congestion controlled

FlowLabel—provides special handling for a particular flow of data. Router handles different flows with the help of a flow table.

PayloadLen—gives length of the packet, excluding IPv6 header.

NextHeader—Options are specified as a header following IP header. NextHeader contains a pointer to optional headers.

HopLimit—It serves the same purpose as TTL field in IPv4.

SourceAddress / DestinationAddress—16-byte addresses of source and destination host

Extension Headers

Extension header provides greater functionality to IPv6.

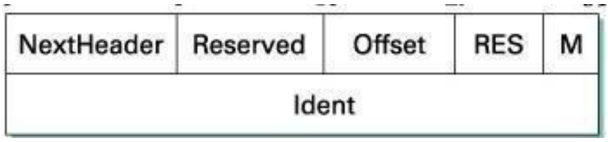
Base header may be followed by six extension headers.

Each extension header contains a NextHeader field to identify the header following it.

Hop-by-Hop—source host passes information to all routers visited by the packet

Source Routing—routing information (strict/loose) provided by the source host.

Fragmentation—In IPv6, only the source host can fragment. Source uses a path MTU discovery technique to find smallest MTU on the path.



NextHeader	Reserved	Offset	RES	M
Ident				

Authentication—used to validate the sender and ensures data integrity.

Encrypted Security Payload—provides confidentiality against eavesdropping.

Destination—source host information is passed to the destination only.

Advanced Capabilities

Auto configuration—Auto or stateless configuration of IP address to hosts without the need for a DHCP server, i.e., plug and play.

Advanced Routing—Enhanced routing support for mobile hosts is provided.

Additional Functions—Enhanced routing functionality with support for mobile hosts.

Security—Encryption and authentication options provide confidentiality and integrity.

Resource allocation—Flow label enables the source to request special handling of real- time audio and video packets

5. EXPLAIN DISTANCE VECTOR MULTICAST ROUTING PROTOCOL. [CO4 – L2]

Distance vector routing for Unicast is extended to support multicast routing.

Each router maintains (Destination, Cost, NextHop) for all destination through exchange of distance vectors.

Multicasting is added to distance-vector routing in two stages.

- o Reverse Path Broadcast *floods* packets to all networks
- o Reverse Path Multicasting *prunes* end networks that do not have hosts belonging to a multicast group.
- o DVMRP is also known as *flood-and-prune* protocol.

Reverse-Path Broadcasting

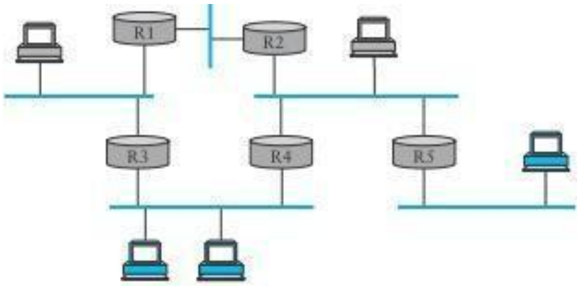
- Router on receiving a multicast packet from source S to a Destination from NextHop, forwards the packet on all out-going links, since it comes from shortest path.
- Packet is flooded but not looped back to S. The drawbacks are:
  - o It floods a network, even if it has no members for that group.

  - Packets are forwarded by each router connected to a LAN, i.e., duplicate flooding
- Duplicate flooding is avoided by
  - Router that has the shortest path to source S, is selected as parent router.
  - Only parent router forwards multicast packets from source S to that LAN.

Thus shortest path to source (reverse) is considered for forwarding decisions.

Reverse-Path Multicasting

- Multicasting is achieved by pruning networks that do not have members for a group G.
- Step 1: Identify a leaf network which has only one router (parent).
  - Leaf network is monitored to determine if it has any members for group G, by having hosts periodically announce to which group it belongs to.
  - Router thus decides whether or not to forward group G packets over that LAN.
- Step 2: Propagate "no members of G here" up the shortest path tree.
  - Routers augments (Destination, Cost) pairs with set of groups for which the leaf network is interested in receiving multicast packets.
  - Information is propagated amongst routers so that a router knows for what groups it should forward on each of its links.
- Including all this information in a routing update is expensive.



6. EXPLAIN PROTOCOL INDEPENDENT MULTICAST (PIM) USING AN EXAMPLE. [CO4 – L2]

PIM divides multicast routing problem into sparse and dense mode.PIM sparse mode (PIM-SM) is widely used. PIM does not rely on any type of Unicast routing protocol, hence protocol independent. Routers explicitly join and leave multicast group using Join and Prune messages.

One of the router is designated as rendezvous point (RP) for each group in a domain to receive PIM messages. Multicast forwarding tree is built as a result of routers sending Join messages to RP. Initially the tree is shared by multiple senders and depending on traffic it may be source- specific to a sender.

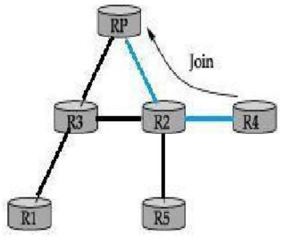
Shared Tree

When a router sends Join message for group G to RP, it goes through a set of routers.

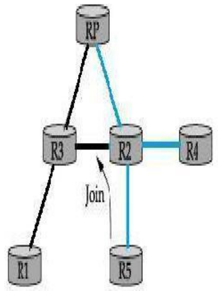
o Join message is wildcarded (*), i.e., it is applicable to all senders.
o Routers create an entry (*, G) in its forwarding table for the shared tree. o Interface on which the Join arrived is marked to forward packets for that
group.
o Forwards Join towards rendezvous router RP.

Eventually, the message arrives at RP. Thus a shared tree with RP as root is formed.

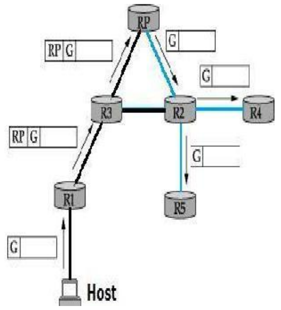
Example
Router R4 sends Join message for group G to rendezvous router RP.
Join message is received by router R2. It makes an entry (*, G) in its table and forwards the message to RP.
When R5 sends Join message for group G, R2 does not forwards the Join. It adds an outgoing interface to the forwarding table created for that group.



Join from R4



Join from R5



Multicas t

message to group G

As routers send Join message for a group, branches are added to the tree, i.e., shared.
Multicast packets sent from hosts are forwarded to designated router RP.
Suppose router R1, receives a message to group G.

o R1 has no state for group G.
o Encapsulates the multicast packet in a Register message.
o Multicast packet is tunneled along the way to RP.

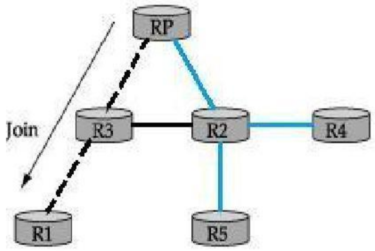
RP decapsulates the packet and sends multicast packet onto the shared tree, towards R2.
R2 forwards the multicast packet to routers R4 and R5 that have members for group G.

Source-specific tree.
RP can force routers to know about group G, by sending Join message to the sending host, so that tunneling can be avoided.

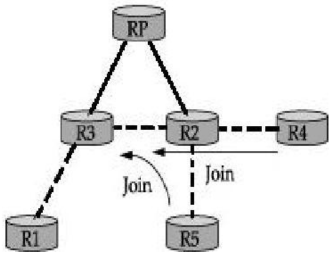
Intermediary routers create sender-specific entry (S, G) in their tables. Thus a source- specific route from R1 to RP is formed.

If there is high rate of packets sent from a sender to a group G, then shared-tree is replaced by source-specific tree with sender as root.

Example



Source-specific Join from RP



Routers switch to Source tree

Rendezvous router RP sends a Join message to the host router R1.
Router R3 learns about group G through the message sent by RP.
Router R4 send a source-specific Join due to high rate of packets from sender.
Router R2 learns about group G through the message sent by R4.

UNIT IV
TRANSPORT LAYER

PART-A

1. What is the main idea of UDP? [CO3 – L1]

The basic idea for a source process is to send a message to a port and for the destination process is to receive the message from a port.

2. What are the different fields in pseudo header? [CO3 – L1]

- Protocol number
- Source IP address
- Destination IP addresses.

3. Define TCP. [CO3 – L1]

TCP guarantees the reliable, in order delivery of a stream of bytes. It is a full-duplex protocol, meaning that each TCP connection supports a pair of byte streams, one flowing in each direction.

4. Define Congestion Control. [CO3 – L1]

It involves preventing too much data from being injected into the network, thereby causing switches or links to become overloaded. Thus flow control is an end to an end issue, while congestion control is concerned with how hosts and networks interact.

5. State the two kinds of events trigger a state transition. [CO3 – L3]

- A segment arrives from the peer.
- The local application process invokes an operation on TCP.

6. What is meant by segment? [CO3 – L1]

At the sending and receiving end of the transmission, TCP divides long transmissions into smaller data units and packages each into a frame called a segment.

7. What is meant by segmentation? [CO3 – L1]

When the size of the data unit received from the upper layer is too long for the network layer datagram or data link layer frame to handle, the transport protocol divides it into smaller usable blocks. The dividing process is called segmentation.

8. What is meant by Concatenation? [CO3 – L1]

The size of the data unit belonging to single sessions are so small that several can fit together into a single datagram or frame, the transport protocol combines them into a single data unit. The combining process is called concatenation.

9. What is rate based design? [CO3 – L1]

Rate- based design, in which the receiver tells the sender the rate-expressed in either bytes or packets per second – at which it is willing to accept incoming data.

10. Deine Gateway. [CO3 – L1]

A device used to connect two separate networks that use different communication protocols.

11. What is meant by quality of service? [CO3 – L1]

The quality of service defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute each service class is associated with a set of attributes.

12. What are the two categories of QoS attributes? [CO3 – L1]

The two main categories are,

- User Oriented
- Network Oriented

13. List out the user related attributes? [CO3 – L1]

- SCR – Sustainable Cell Rate
- PCR – Peak Cell Rate
- MCR- Minimum Cell Rate
- CVDT – Cell Variation Delay Tolerance.

14. What are the networks related attributes? [CO3 – L1]

The network related attributes are,

- Cell loss ratio (CLR)
- Cell transfer delay (CTD)
- Cell delay variation (CDV)
- Cell error ratio (CER).

15. What is RED? [CO3 – L1]

Random Early Detection in each router is programmed to monitor its own queue length and when it detects that congestion is imminent, to notify the source to adjust its congestion window.

16. What are the three events involved in the connection? [CO3 – L1]

For security, the transport layer may create a connection between the two end ports. A connection is a single logical path between the source and destination that is associated with all packets in a message. Creating a connection involves three steps:

- Connection establishment
- Data transfer
- Connection release

17. What is Silly Window Syndrome? [CO3 – L1 NOV/DEC 2015]

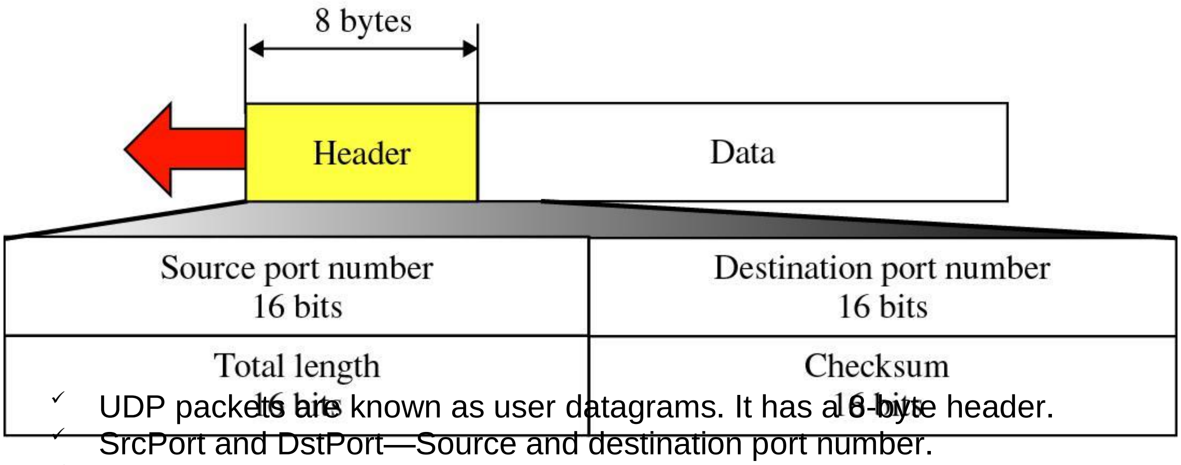
If the sender or the receiver application program processes slowly and can send only 1 byte of data at a time, then the overhead is high. This is because to send one byte of data, 20 bytes of TCP header and 20 bytes of IP header are sent. This is called as silly window syndrome.

PART-B

1. WRITE SHORT NOTES ON UDP. [CO3 – L1 MAY/JUNE 2016]

- ✓ User Datagram Protocol (UDP) is a connectionless, unreliable transport protocol.
- ✓ Adds process-to-process communication to best-effort service provided by IP.
- ✓ Simple demultiplexer allows multiple processes on each host to communicate.
- ✓ Does not provide flow control / reliable / ordered delivery UDP is suitable for a process that requires simple request-response communication with little concern for flow control/error control.

UDP Datagram

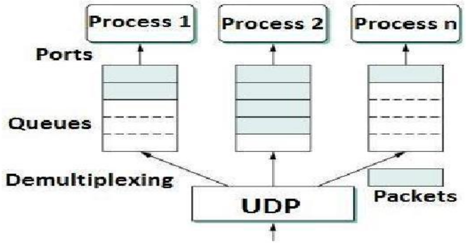


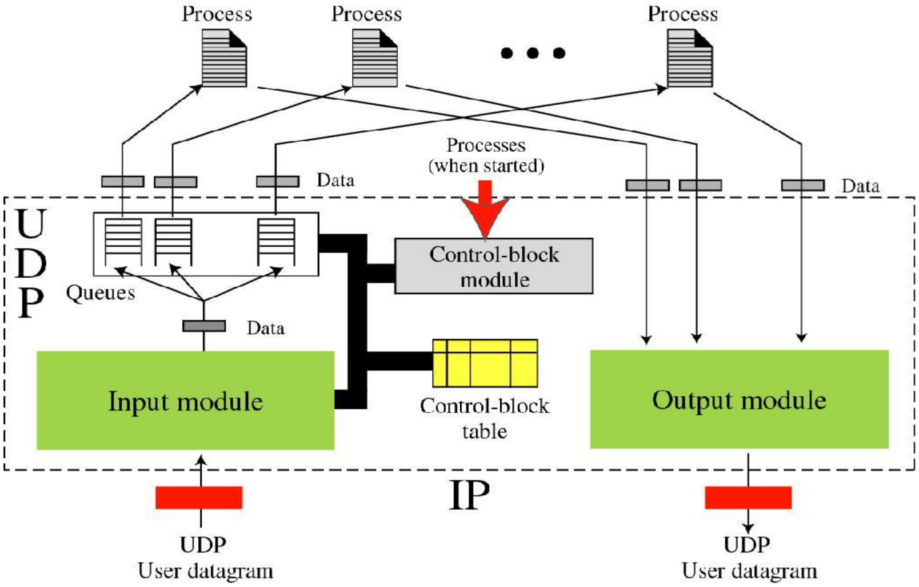
- ✓ UDP packets are known as user datagrams. It has a 8-byte header.
- ✓ SrcPort and DstPort—Source and destination port number.
- ✓ Length—total length of the user datagram, i.e., header plus data.
- ✓ Checksum—computed over UDP header, data and pseudo header.
- ✓ Pseudo header consists of IP fields (Protocol, SourceAddr, DestinationAddr) and UDP Length field. UDP delivers message to the correct recipient process using checksum.

Ports

- ✓ Processes (server/client) are identified by an abstract locator known as port.
- ✓ Server accepts message at well known port. Some well-known UDP ports are 7–Echo, 53–DNS, 111–RPC, 161–SNMP, etc.
- ✓ < port, host > pair is used as key for demultiplexing.
- ✓ Ports are implemented as a message queue.
- ✓ When a message arrives, UDP appends it to end of the queue.

When queue is full, the message is discarded. When a message is read, it is removed from the queue.





Applications

- Used for management processes such as SNMP.
- Used for route updating protocols such as RIP.
- It is a suitable transport protocol for multicasting.
- UDP is suitable for a process with internal flow and error control mechanisms such as Trivial File Transfer Protocol (TFTP).

2. List the features of TCP. Draw TCP segment format and explain its fields. [CO3 – L1]

Transmission Control Protocol (TCP) offers connection-oriented, byte-stream service.

Guarantees reliable, in-order delivery of message.

TCP is a full-duplex protocol.

Like UDP, TCP provides process-to-process communication.

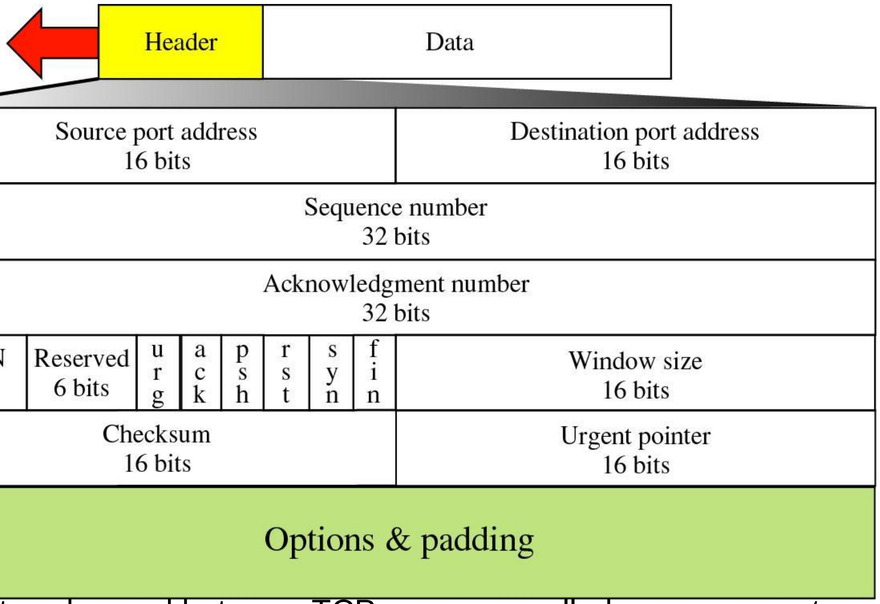
Has built-in congestion-control mechanism.

Ensures flow control, as sliding window forms heart of TCP operation.

Some well-known TCP ports are 21–FTP, 23– TELNET, 25–SMTP, 80–HTTP, etc.

Sending TCP buffers bytes in send buffer and transmits data unit as segments.
Segments are stored in receive buffer at the other end for application to read.

Segment Format



- Data unit exchanged between TCP peers are called *segments*.
- SrcPort and DstPort—*port number* of source and destination process.
- SequenceNum—contains sequence number, i.e. *first* byte of data segment.
- Acknowledgment— byte number of segment, the receiver expects *next*.
- HdrLen— length of TCP header as 4-byte *words*.
- Flags—contains *six* control bits known as flags.
  - o *URG*—segment contains *urgent* data.
  - o *ACK*—value of *acknowledgment* field is valid. o *PUSH*—sender has invoked the *push* operation. o *RESET*—receiver wants to *abort* the connection.
  - o *SYN*—synchronize sequence numbers during connection *establishment*. o *FIN*—terminates the TCP *connection.*
- AdvertisedWindow—defines receiver's window size and acts as *flow control*.
- Checksum—It is computed over TCP *header*, *Data*, and *pseudo header* containing IP fields (Length, SourceAddr & DestinationAddr).
- UrgPtr—specifies first byte of *normal* data contained in the segment, if URG bit is set.

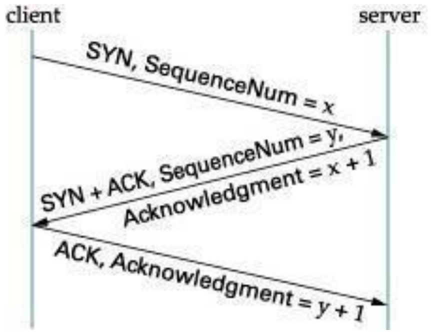
3. EXPLAIN TCP CONNECTION MANAGEMENT (OR) TCP ARCHITECTURE (OR) STATE TRANSITION DIAGRAM. [CO3 – L2 MAY/JUNE 2015]

TCP is connection-oriented.

Client performs an *active* connection to establish connection with a *passive* open server, prior to data communication
Eventually connection is terminated after data transmission.

Connection Establishment
Connection establishment in TCP is a *three-way handshaking*.

1. Client sends a SYN segment to the server containing its initial sequence number (Flags = SYN, SequenceNum = *x*)
2. Server responds with a segment that acknowledges client's segment and specifies its initial sequence number (Flags = SYN+ ACK, Ack = *x* + 1 SequenceNum = *y*).
3. Finally, client responds with a segment that acknowledges server's sequence number (Flags = ACK, Ack = *y* + 1).



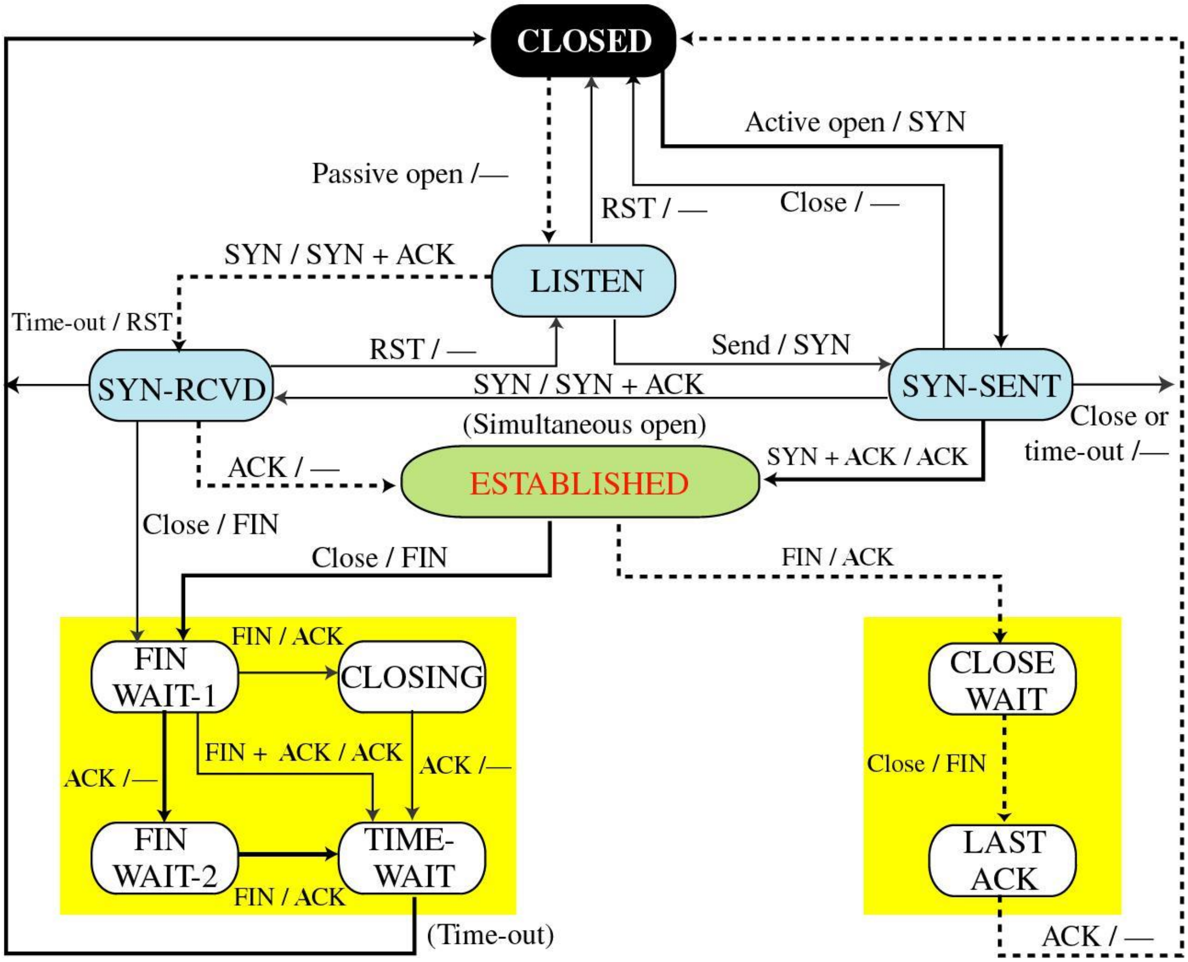
Connection Termination

- Connection termination or teardown can be done in two ways
- *Three-way close*—Both client and server close *simultaneously.*
    - o Client sends a FIN segment. The FIN segment can include last chunk of data.
    - o Server responds with FIN + ACK segment to inform itsclosing.
    - o Finally, client sends an ACK segment.
- *Half-Close*—Client stops sending but receives data. This is known as *half-close*.
    - o Client half-closes the connection by sending a FIN segment.
    - o Server sends an ACK segment. Data transfer from client to the server *stops*.
    - o After sending all data, server sends FIN segment to client, which is acknowledged by the client.

State Transition Diagram

- States involved in opening and closing a connection is shown above and below

- Events that trigger a state transition is:
  - o Segments that *arrive* from its peer.
  - o Application process invokes an *operation* on TCP
- Operation of sliding window is hidden in the ESTABLISHED state



Opening

1. Server invokes a passive open on TCP, which causes TCP to move to LISTEN state
2. Client does an active open, which causes its TCP to send a SYN segment to the server and move to SYN_SENT state.
3. When SYN segment arrives at the server, it moves to SYN_RCVD state and responds with a SYN + ACK segment.
4. Arrival of SYN + ACK segment causes the client to move to ESTABLISHED state and sends an ACK to the server.
5. When ACK arrives, the server finally moves to ESTABLISHED state.

Closing

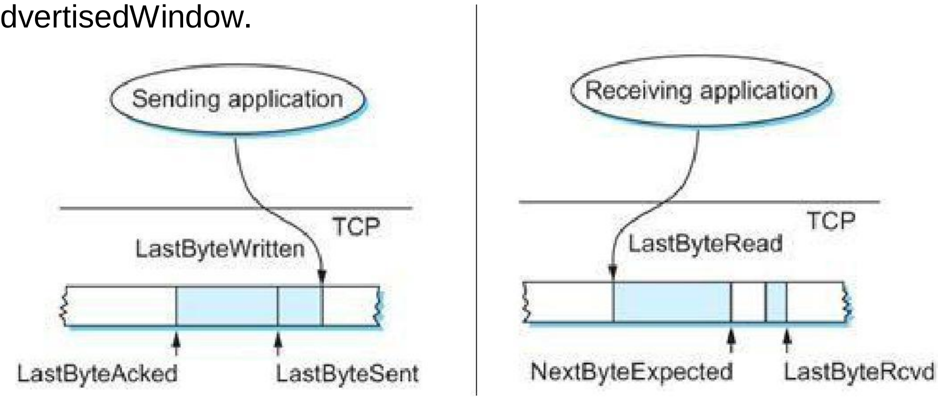
1. Client / Server can independently close its half of the connection or simultaneously. Transitions from ESTABLISHED to CLOSED state are:

2. One side closes ESTABLISHED→FIN_WAIT_1→FIN_WAIT_2→TIME_WAIT→CLOSED
3. Other side closes: ESTABLISHED → CLOSE_WAIT → LAST_ACK → CLOSED

Simultaneous close: ESTABLISHED→FIN_WAIT_1→CLOSING→TIME_WAIT→ CLOSED

4. EXPLAIN TCP FLOW CONTROL (OR) ADAPTIVE FLOW CONTROL (OR) TCP SLIDING WINDOW IN DETAIL. [CO3 – L2]

- TCP uses a variant of sliding window known as adaptive flow control that:
  - o guarantees *reliable* delivery of data
  - o ensures *ordered* delivery of data
  - o enforces *flow control* at the sender
- Receiver advertises its window size to the sender using AdvertisedWindow field.
- Sender thus cannot have *unacknowledged* data greater than AdvertisedWindow.



Send Buffer *Receive Buffer*

Send Buffer

- Sending TCP maintains *send buffer* which contains 3 segments, acknowledged data, unacknowledged data and data to be transmitted.
- Send buffer maintains three *pointers* LastByteAcked, LastByteSent, and LastByteWritten such that:

  LastByteAcked ≤ LastByteSent ≤ LastByteWritten
- A byte can be sent only *after* being written and only a sent byte *can be* acknowledged.
- Bytes to the *left* of LastByteAcked are not kept as it had been acknowledged.

Receive Buffer

- Receiving TCP maintains *receive* buffer to hold data even if it arrives out-of-order.
- Receive buffer maintains three *pointers* namely LastByteRead, NextByteExpected, and LastByteRcvd such that:

  LastByteRead< NextByteExpected ≤ LastByteRcvd + 1

- A byte *cannot* be read until that byte and all preceding bytes have been received.
- If data is received *in order*, then NextByteExpected = LastByteRcvd + 1
- Bytes to the *left* of LastByteRead are not buffered, since it is read by the application.

Flow Control

Size of *send* and *receive* buffer is MaxSendBuffer and MaxRcvBuffer respectively.

- ➢ Sending TCP prevents *overflowing* of send buffer by maintaining LastByteWritten − LastByteAcked ≤ MaxSendBuffer
- ➢ Receiving TCP avoids *overflowing* its receive buffer by maintaining LastByteRcvd − LastByteRead ≤ MaxRcvBuffer
- ➢ Receiver *throttles* the sender by having AdvertisedWindow based on *free* space available for buffering.
- ➢ Sending TCP *adheres* to AdvertisedWindow by computing EffectiveWindow that *limits* how much data it should send.
- ➢ When data arrives, LastByteRcvd moves to its right and AdvertisedWindow shrinks.
- ➢ Receiver acknowledges only, if preceding bytes have arrived.
- ➢ AdvertisedWindow *expands* when data is *read* by the application.
    - o If data is read as *fast* as it arrives then AdvertisedWindow = MaxRcvBuffer
    - o If data is read *slowly*, it eventually leads to a AdvertisedWindow of size 0.
- AdvertisedWindow field is designed to allow sender to keep the pipe *full*.

Fast Sender vs Slow Receiver

- If sender transmits at a *higher* rate, receiver's buffer gets *filled* up. Hence, dvertised Window shrinks, eventually to 0.
- Receiver advertises a window of size 0, thus sender cannot transmit as it gets *blocked*.
- When receiving process reads some data, those bytes are acknowledged and AdvertisedWindow expands.
- When an acknowledgement arrives for *x* bytes, LastByteAcked is incremented by *x* and send buffer space is freed accordingly to send further data.

5. EXPLAIN ADAPTIVE RETRANSMISSION ALGORITHMS. (OR) HOW IS TIMEOUT ESTIMATED IN TCP? [CO3 – L2]

- TCP guarantees reliability through *retransmission* when ACK arrives after timeout.
- Timeout is based on RTT, but it is highly *variable* for any two hosts on the internet.
- Appropriate timeout is chosen using *adaptive* retransmission.

Original Algorithm

- SampleRTT is the *duration* between sending a segment and arrival of its ACK.
- EstimatedRTT is *weighted average* of previous estimate and current sample.

$\text{EstimatedRTT} = \alpha \times \text{EstimatedRTT} + (1 - \alpha) \times \text{SampleRTT}$

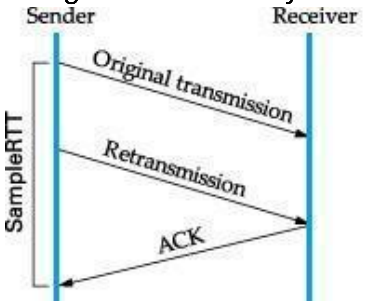
(where α is known as smoothening factor with value in the range 0.8–0.9)

- *Timeout* is determined as twice the value of EstimatedRTT .

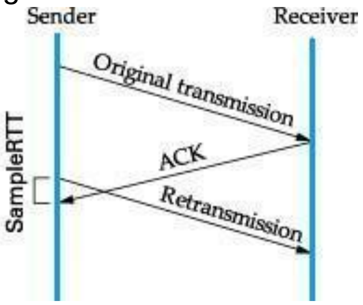
  $\text{TimeOut} = 2 \times \text{EstimatedRTT}$
- In original TCP, timeout is thus computed as function of *running average* of RTT.

Karn/Partridge Algorithm

- Flaw discovered in TCP original algorithm was that an ACK segment, acknowledges *receipt* of data, not a transmission.
- When an ACK arrives after retransmission, it is impossible to decide, whether to pair it with original or retransmitted segment for SampleRTT estimation.
  - o If ACK is associated with original one, then SampleRTT becomes too large
  - o If ACK is associated with retransmission, then SampleRTT becomes too small
- Karn and Partridge proposed that
  - o SampleRTT should be taken for segments that are sent *only once*, i.e, for segments that are not retransmitted.
  - o Each time TCP retransmits, timeout is *doubled*, since loss of segments is mostly due to congestion.



Large SampleRTT



Small SampleRTT

Jacobson/Karels Algorithm

- Jacobson and Karel discovered that problem with original algorithm was *variance* in
- Mean RTT and variation in mean is calculated

  as: $\text{Difference} = \text{SampleRTT} - \text{EstimatedRT}$

  $\text{EstimatedRTT} = \text{EstimatedRTT} + (\delta \times \text{difference})$

  $\text{Deviation} = \text{Deviation} + \delta\,(|\text{Difference}| - \text{Deviatio}$ (*where δ is a fraction between 0 and 1*)
- TimeOut is computed as a function of both EstimatedRTT and Deviation as:

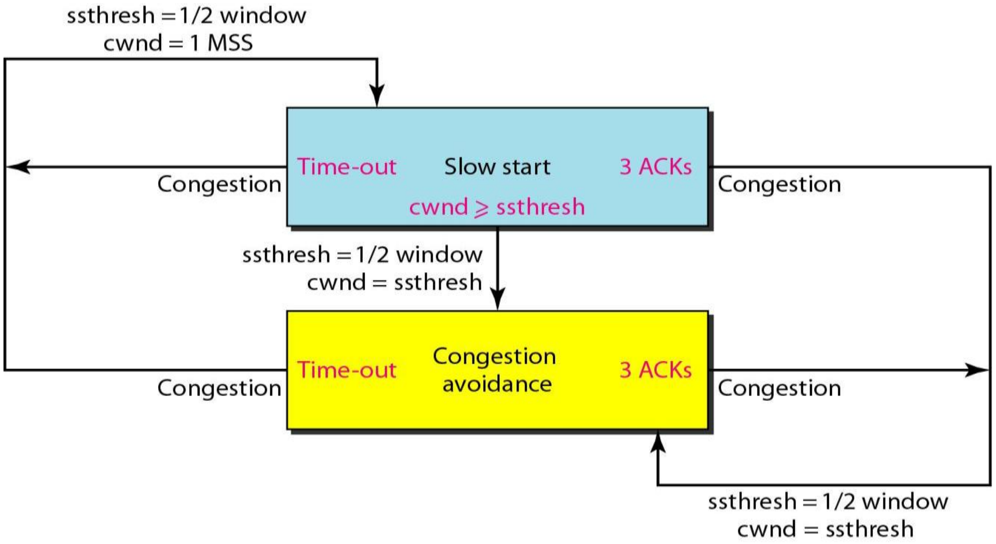
  $\text{TimeOut} = \mu \times \text{EstimatedRTT} + \varphi \times \text{Deviation}$

  (*where μ = 1 and φ = 4*)

When *variance* is small, TimeOut is close to EstimatedRTT. If variation among samples is *small,* then EstimatedRTT can be trusted.

6. EXPLAIN TCP CONGESTION CONTROL MECHANISMS IN DETAIL. [CO3 – L2]

- Each source determines *capacity* of the network, so as to send packets without loss.
- TCP uses ACKs for further transmission of packets, i.e., *self-clocking*.
- TCP maintains a state variable CongestionWindow for each *connection*.
  - A source is *not allowed* to send faster than network or destination host. MaxWindow = MIN(CongestionWindow, AdvertisedWindow)
- Congestion control mechanisms are:
  1. Additive Increase / Multiplicative Decrease (AIMD)
  2. Slow Start
  3. Fast Retransmit and Fast Recovery



Additive Increase/Multiplicative Decrease (AIMD)

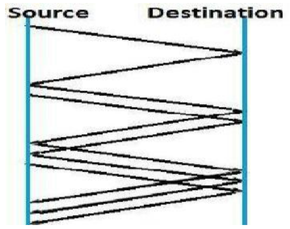
- TCP source *initializes* CongestionWindow based on congestion level in the network.
- Source *increases* CongestionWindow when level of congestion goes down and *decreases* the same when level of congestion goes up.
- TCP interprets *timeouts* as a sign of congestion and reduces the rate of transmission.
- On timeout, source reduces its CongestionWindow by half, i.e., *multiplicative decrease*. For example, if CongestionWindow = *16* packets, after timeout it is *8*.
- Value of CongestionWindow is never less than maximum segment size (MSS).
- When ACK arrives CongestionWindow is *incremented* marginally, i.e., *additive increase.*

  Increment = MSS × (MSS /
  CongestionWindow) CongestionWindow +=
  Increment

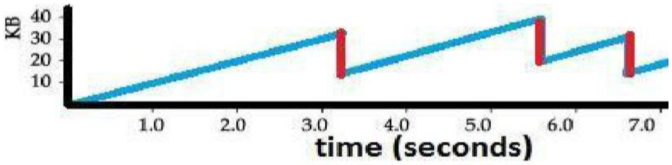
For *example*, when ACK arrives for 1 packet, 2 packets are sent. When ACK for both packets arrive, 3 packets are sent and so on.

- CongestionWindow increases and decreases throughout *lifetime* of the connection.

- When CongestionWindow is plotted as a function of time, a *saw-tooth* pattern results.



Additive Increase Analysis



CongestionWindow Trace

- AIMD decreases its CongestionWindow aggressively but increases *conservatively*.
- Small CongestionWindow results in *less probability* of packets being dropped..

AIMD is appropriate when source is operating close to capacity of the network.

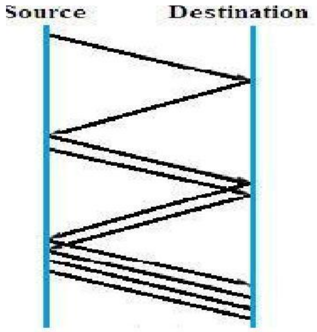
Slow Start

- Slow start is used to increase CongestionWindow *exponentially* from a cold start.
- Source TCP *initializes* CongestionWindow to one packet.
- TCP *doubles* the number of packets sent every RTT on successful transmission.
  - o When ACK arrives for first packet TCP adds 1 packet to CongestionWindow and sends two packets.
  - o When two ACKs arrive, TCP increments CongestionWindow by 2 packets and sends four packets and so on.
- Instead of sending entire permissible packets at once (bursty traffic), packets are sent in a phased manner, i.e., *slow start*.
- Initially TCP has no idea about congestion, henceforth it increases CongestionWindow rapidly until there is a timeout.

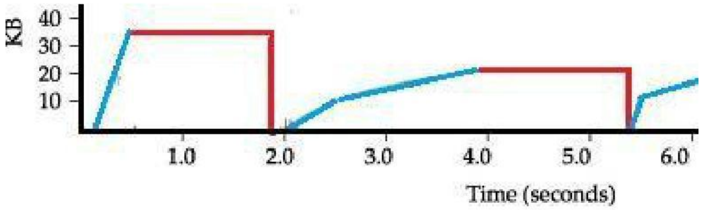
  On timeout: CongestionThreshold = CongestionWindow / 2 CongestionWindow = 1
- Slow start is repeated until CongestionWindow reaches CongestionThreshold and thereafter 1 packet per RTT.

Example

- Initial slow start causes increase in CongestionWindow up to 34KB,
- Congestion occurs at 0.4 seconds and packets are lost.
- ACK does not arrive and therefore trace of CongestionWindow becomes flat.
- Timeout occurs at 2sec. CongestionThreshold=17KB,CongestionWindow=1PK
- Slow start is done till 17KB and additive increase thereafter till congestion occurs.



Exponential Increase



Congestion Window Trace Analysis

- Slow start provides exponential growth and is designed to avoid *bursty* nature of TCP.
- TCP loses more packets initially, because it attempts to learn the available *bandwidth* quickly through exponential increase.
- If connection goes *dead* while waiting for timer to expire, slow start phase is used only up to current value of CongestionWindow.

Fast Retransmit and Fast Recovery

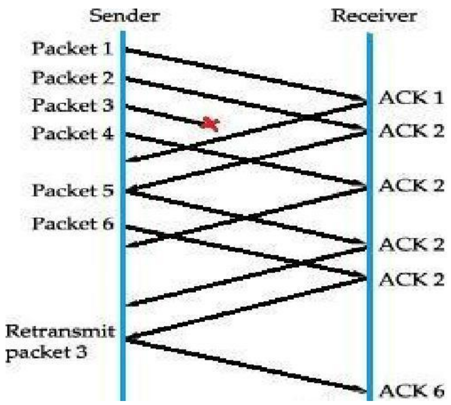
- TCP timeouts led to long periods of time during which the connection went dead while waiting for a timer to expire.
- Fast retransmit is a heuristic approach that *triggers* retransmission of a dropped packet sooner than the regular timeout mechanism. It *does not* replace regular timeouts.
- When a packet arrives out of order, receiving TCP resends the same acknowledgment (*duplicate ACK*) it sent last time.
- When *three duplicate* ACK arrives at the sender, it infers that corresponding packet may be lost due to congestion and retransmits that packet. This is called *fast retransmit* before regular timeout.
- When packet loss is detected using fast retransmit, the slow start phase is replaced by additive increase, multiplicative decrease method. This is known as *fast recovery*.
- Instead of setting CongestionWindow to one packet, this method uses the ACKs that are still in pipe to clock the sending of packets.
- Slow start is only used at the beginning of a connection and after *regular* timeout. At other times, it follows a pure AIMD pattern.

Example

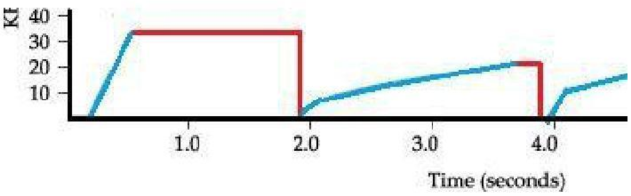
- In *example*, packets 1 and 2 are received whereas packet 3 gets lost.
  - o Receiver sends a duplicate ACK for packet 2 when packet 4 arrives.
  - o Sender receives 3 duplicate ACKs after sending packet 6 retransmits packet 3.
  - o When packet 3 is received, receiver sends cumulative ACK up to packet 6.

In *example* trace, slow start is used at beginning and during timeout at 2 secs.

- o Fast recovery avoids slow start from 3.8 to 4 sec.
- o CongestionWindow is reduced by half from 22 KB to 11 KB.
- o Additive increase is resumed thereafter.



Duplicate ACK



CongestionWindow Trace Analysis

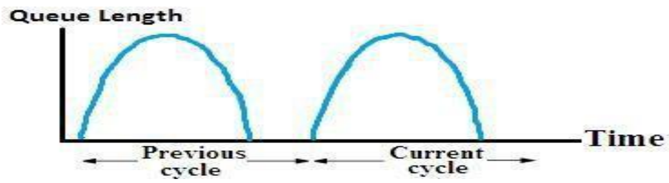
- Long periods with flat congestion window and no packets sent are *eliminated*.
- TCP's fast retransmit can detect up to three dropped packets per window.
- Fast retransmit/recovery increases throughput by 20%.

7. EXPLAIN IN DETAIL ABOUT TCP CONGESTION AVOIDANCE ALGORITHMS. [CO3 – L2]

- Congestion avoidance mechanisms *prevent* congestion before it actually occurs.
- TCP *creates* loss of packets in order to determine bandwidth of the connection.
- Routers *help* the end nodes by intimating when congestion is likely to occur.
- Congestion-avoidance mechanisms are: o DECbit
  - o Random Early Detection (RED)
  - o Source-based congestion avoidance

DECbit

- Each router monitors its load and *explicitly* notifies the end node when congestion is likely to occur. Source *reduces* its transmission rate and congestion is avoided. A binary congestion bit called *DECbit* is *added* to the packet header.
- Router *sets* this bit in packets that flow through, if its average queue length is >= 1.
  - o Average queue length is measured over a time interval that includes the *last busy* + *last idle* cycle + *current busy* cycle.
  - o Calculates average queue length by *dividing* the curve area with time interval.



- Destination host *copies* the DECbit onto ACK and sends it back to the source.

- Source checks *how many* ACK has DECbit set for previous window packets.
- If less than 50% of ACK have DECbit set, then source *increases* its congestion window by 1 packet, otherwise *decreases* the congestion window by 87.5%.
- *Increase by 1, decrease by 0.875* rule was based on AIMD for stabilization.

Random Early Detection (RED)

- Router notifies the source that congestion is likely to occur by *dropping packets* before its buffer space exhausts (*early drop*), rather than later due to congestion.
- Source is *implicitly* notified by timeout or duplicate ACK.
- Each incoming packet is dropped with a probability known as *drop probability* when the queue length exceeds *drop level*. This is called early random drop.
- Average queue length is computed as a weighted running average: AvgLen = (1 − Weight) × AvgLen + Weight × SampleLen
- Queue length *thresholds* defined by RED are MinThreshold and MaxThreshold.
- When a packet arrives, gateway *compares* current AvgLen with these thresholds and decides whether to queue or drop the packet as follows:

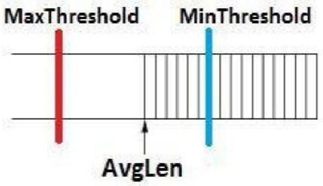
```
if AvgLen ≤ MinThreshold
        Queue the packet
if MinThreshold < AvgLen < MaxThreshold
        Calculate probability P
        Drop the arriving packet with probability P
if AvgLen ≥ MaxThreshold
        Drop the arriving packet
```

- When AvgLen exceeds MinThreshold, a small percentage of packets are dropped. It forces TCP to reduce CongestionWindow, which in turn reduces the rate at which packets arrive at the router. Thus, AvgLen decreases and congestion is *avoided*.
- Drop probability P is computed as a function of AvgLen.

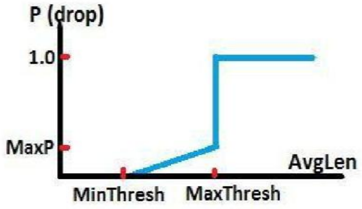
  P = MaxP × (AvgLen − MinThreshold) / (MaxThreshold − MinThreshold)

- Drop probability increases slowly when AvgLen is between two thresholds. On reaching MaxP at the upper threshold, it jumps to unity.
- MaxThreshold value is twice of MinThreshold due to bursty Internet traffic.

RED drops packets *randomly.* The probability that a flow’s packet being dropped is proportional to its share of the bandwidth.



RED thresholds



Drop probability function

Source-Based Congestion Avoidance

- Source looks for signs of congestion in the network. For instance, increase in RTT indicates queuing at a router.

Some mechanisms

1. TCP checks to see if current RTT is greater than mean RTT. If so, congestion window is decreased by one-eighth, else normal increase.
2. TCP increases window size by one packet and compares the throughput achieved when the window was one packet smaller.

TCP Vegas

- *Throughput* increases as congestion window increases. Increase in window size beyond available bandwidth, results in packets queuing at the bottleneck router.
- TCP Vegas goal is to measure and control the right amount of *extra data* in transit.
- Extra data refers to amount of data that source would have refrained from sending so as to not *exceed* the available bandwidth.

➢ A flow's BaseRTT is set to RTT of a packet when the flow is not congested. BaseRTT = MIN (RTTs)

- Expected throughput without overflowing is:
  ExpectedRate = CongestionWindow / BaseRTT
- ActualRate, i.e., current sending rate for a packet is calculated by recording bytes transmitted during a RTT.
  ActualRate = ByteTransmitted / SampleRTT
- ExpectedRate and ActualRate are compared.
- Thresholds α and β are defined and corresponds to less data and too much extra data in the network, such that α < β.
- TCP uses difference in rates and adjusts CongestionWindow accordingly.
  - If Diff < α, CongestionWindow is linearly increased during the next RTT
  - If Diff > β, CongestionWindow is linearly decreased during the next RTT
  - If α < Diff < β, CongestionWindow is unchanged
- When actual and expected rates *vary* significantly, it indicates congestion in the network. The β threshold triggers *decrease* in sending rate.
- When actual and expected rate is almost the *same*, there is available bandwidth that goes wasted. The α threshold triggers *increase* in sending rate.
- Overall goal of TCP Vegas is to keep *between* α and β extra bytes in the network.

8. DEFINE QOS. MENTION THE APPROACHES TO IMPROVE QOS. [CO3 – L1]

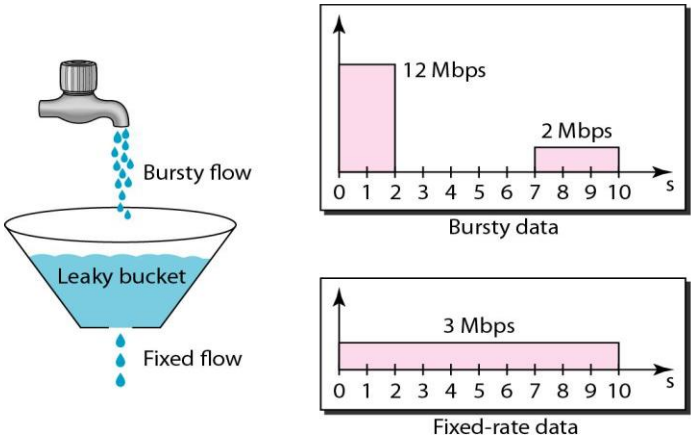
- Best-effort service offered by the network is insufficient for applications. They require assurances from network. For example:
  - o Multimedia applications require minimum bandwidth.
  - o Real-time applications require timeliness rather than correctness.
- Network that supports different level of service based on application requirements offer Quality of Service (QoS).
- QoS is defined as a set of attributes pertaining to the performance of a connection. Attributes may be either user or network oriented.

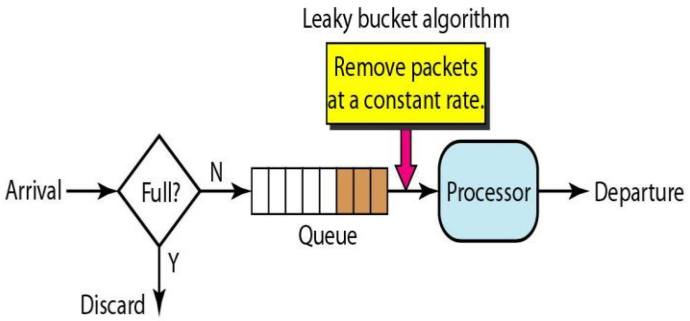
Approaches to improve QoS.

- Approaches to improve QoS are classified as either *fine-grained* or *coarse-grained*.
- Fine-grained approaches provide QoS to *individual* applications or flows. *Integrated Services*, a QoS architecture used with RSVP belongs to this category.
- Coarse-grained approaches provide QoS to *large classes* of data or aggregated traffic.

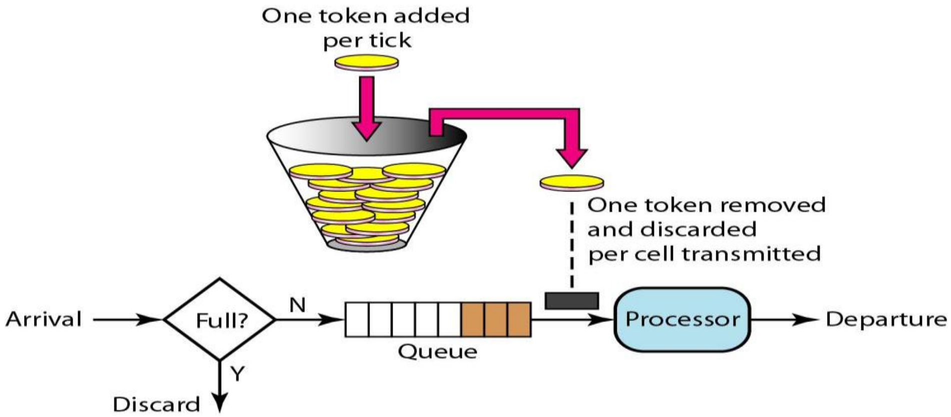
  Differentiated Services belongs to this category.

Leaky Bucket implementation





Token Bucket implementation



UNIT V
APPLICATION LAYER

PART-A

1. What is the function of SMTP? [CO2 – L1]

The TCP/IP protocol supports electronic mail on the Internet is called Simple Mail Transfer (SMTP). It is a system for sending messages to other computer users based on e-mail addresses. SMTP provides mail exchange between users on the same or different computers.

2. What is the difference between a user agent (UA) and a mail transfer agent (MTA)? [CO2 – L1]

The UA prepares the message, creates the envelope, and puts the message in the envelope. The MTA transfers the mail across the Internet.

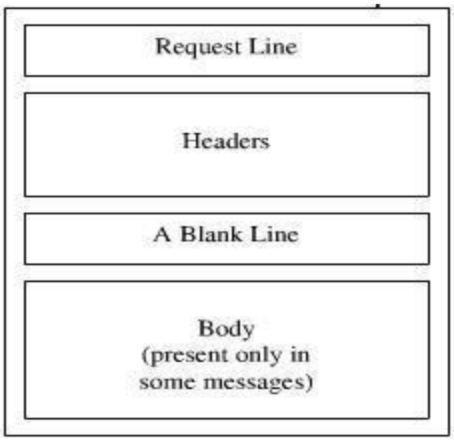
3. How does MIME enhance SMTP? [CO2 – L2]

MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP. MIME transforms non-ASCII data at the sender site to NVT ASCII data and deliverers it to the client SMTP to be sent through the Internet. The server SMTP at the receiving side receives the NVT ASCII data and delivers it to MIME to be transformed back to the original data.

4. **Why is an application such as POP needed for electronic messaging? [CO2 – L1]**

Workstations interact with the SMTP host, which receives the mail on behalf of every host in the organization, to retrieve messages by using a client-server protocol such as Post Office Protocol, version 3(POP3). Although POP3 is used to download messages from the server, the SMTP client still needed on the desktop to forward messages from the workstation user to its SMTP mail server.

5. Give the format of HTTP request message. [CO2 – L3 MAY/JUNE 2014]



6. What is the purpose of Domain Name System? [CO2 – L1]

Domain Name System can map a name to an address and conversely an address to name.

7. Discuss the three main division of the domain name space. [CO2 – H1]

Domain name space is divided into three different sections: generic domains, country domains & inverse domain.

Generic domain: Define registered hosts according to their generic behavior, uses generic suffixes.

Country domain: Uses two characters to identify a country as the last suffix.

Inverse domain: Finds the domain name given the IP address.

8. Discuss the TCP connections needed in FTP. [CO2 – H1]

FTP establishes two connections between the hosts. One connection is used for data transfer, the other for control information. The control connection uses very simple rules of communication. The data connection needs more complex rules due to the variety of data types transferred.

9. Discuss the basic model of FTP. [CO2 – H1]

The client has three components: the user interface, the client control process, and the client data transfer process. The server has two components: the server control process and the server data transfer process. The control connection is made between the control processes. The data connection is made between the data transfer processes.

10. Name four factors needed for a secure network. [CO2 – L1]

Privacy: The sender and the receiver expect confidentiality.

Authentication: The receiver is sure of the sender’s identity and that an imposter has not sent the message.

Integrity: The data must arrive at the receiver exactly as it was sent.

Non-Reputation: The receiver must able to prove that a received message came from a specific sender.

11. How is a secret key different from public key? [CO2 – L2]

In secret key, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. In public key, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

12. What is a digital signature? [CO2 – L1 NOV/DEC 2015]

Digital signature is a method to authenticate the sender of a message. It is similar to that of signing transactions documents when you do business with a bank. In network transactions, you can create an equivalent of an electronic or digital signature by the way you send data.

13. What are the advantages & disadvantages of public key encryption? [CO2 – L1]

Advantages:

a) Remove the restriction of a shared secret key between two entities. Here each entity can create a pair of keys, keep the private one, and publicly distribute the other one.

b) The no. of keys needed is reduced tremendously. For one million users to communicate, only two million keys are needed.

Disadvantage:

If you use large numbers the method to be effective. Calculating the cipher text using the long keys takes a lot of time. So it is not recommended for large amounts of text.

14. What are the advantages & disadvantages of secret key encryption? [CO2 – L1]

Advantage:

Secret Key algorithms are efficient: it takes less time to encrypt a message. The reason is that the key is usually smaller. So it is used to encrypt or decrypt long messages.

Disadvantages:

Each pair of users must have a secret key.

15. What are the requests messages support SNMP and explain it? [CO2 – L1]

- GET
- SET

The former is used to retrieve a piece of state from some node and the latter is used to store a new piece of state in some node.

16. Define PGP. [CO2 – L1]

Pretty Good Privacy is used to provide security for electronic mail. It provides authentication, confidentiality, data integrity, and non repudiation.

17. Define SSH. [CO2 – L1]

Secure Shell is used to provide a remote login, and used to remotely execute commands and transfer files and also provide strong client/server authentication / message integrity.

18. Discuss the basic model of FTP. [CO2 – H1]

The client has three components: the user interface, the client control process, and the client data transfer process. The server has two components: the server control process and the server data transfer process. The control connection is made between the control processes. The data connection is made between the data transfer processes.

19. What is TELNET? [CO2 – L1]

Terminal Network is a protocol used to login in to the remote host.

20. Define Cryptography. [CO2 – L1]

- Original message before being transformed is called **plaintext**.
- After the message is transformed, is called **cipher text**.
- An encryption algorithm transforms the plaintext to cipher text; a decryption algorithm transforms the cipher text back to plaintext.
- The term cipher is used to refer to encryption and decryption algorithms.

21. What are the types of DNS Message? [CO2 – L1]

Two types of messages

Query: header and question records

Response: Header, question records, answer records, authoritative records, and additional records.

22. What is TELNET PROTOCOL? [CO2 – L1]

A TELNET connection is a Transmission Control Protocol (TCP) connection used to transmit data with interspersed TELNET control information.

The TELNET Protocol is built upon three main ideas: first, the concept of a "Network Virtual Terminal"; second, the principle of negotiated options; and third, a symmetric view of terminals and processes.

23. What is POP3? [CO2 – L1]

POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP), a protocol for transferring e-mail across the Internet.

24. What is IMAP? [CO2 – L1]

IMAP (Internet Message Access Protocol) is a standard protocol for accessing e-mail from your local server. IMAP (the latest version is IMAP Version 4) is a client/server protocol in which e-mail is received and held for you by your Internet server.

IMAP can be thought of as a remote file server. POP3 can be thought of as a "store-and-forward" service.

25. What is SSH? [CO2 – L1]

(**S**ecure **Sh**ell) A security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.

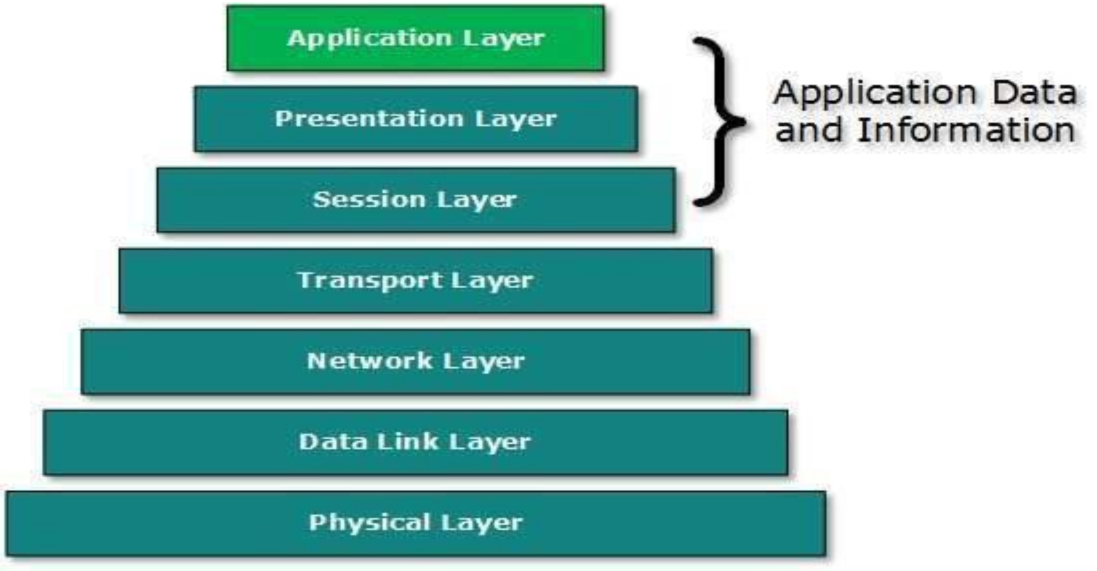
PART-B

1. EXPLAIN APPLICATION LAYER IN DETAIL. [CO2 – L2 NOV/DEC 2015]

Application layer is the top most layer in OSI and TCP/IP layered model. This layer exists in both layered Models because of its significance, of interacting with user and user applications. This layer is for applications which are involved in communication system.

A user may or may not directly interacts with the applications. Application layer is where the actual communication is initiated and reflects. Because this layer is on the top of the layer stack, it does not serve any other layers. Application layer takes the help of Transport and all layers below it to communicate or transfer its data to the remote host.

When an application layer protocol wants to communicate with its peer application layer protocol on remote host, it hands over the data or information to the Transport layer. The transport layer does the rest with the help of all the layers below it.



There is an ambiguity in understanding Application Layer and its protocol. Not every user application can be put into Application Layer. except those applications which interact with the communication system. For example, designing software or text-editor cannot be considered as application layer programs.

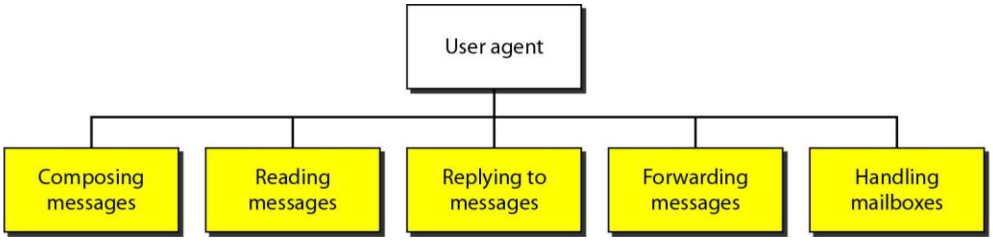
On the other hand, when we use a Web Browser, which is actually using Hyper Text Transfer Protocol (HTTP) to interact with the network. HTTP is Application Layer protocol.

Another example is File Transfer Protocol, which helps a user to transfer text based or binary files across the network. A user can use this protocol in either GUI based software like FileZilla or CuteFTP and the same user can use FTP in Command Line mode.

Hence, irrespective of which software you use, it is the protocol which is considered at Application Layer used by that software. DNS is a protocol which helps user application protocols such as HTTP to accomplish its work.

2. EXPLAIN SIMPLE MAIL TRANSFER PROTOCOL WITH NECESSARY DIAGRAMS. [CO2 – L2]

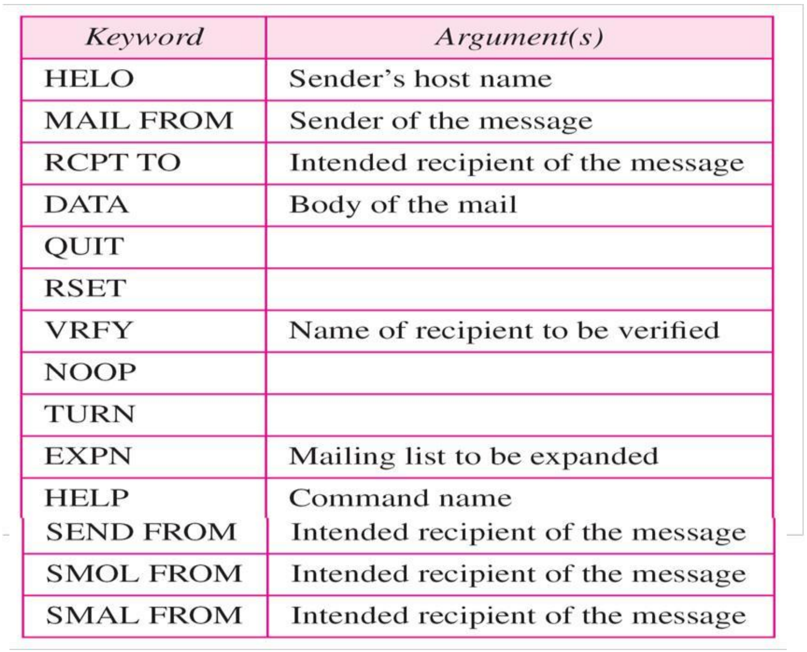
The Simple Mail Transfer Protocol (SMTP) is used to transfer electronic mail from one user to another. This task is done by means of email client software (User Agents) the user is using. User Agents help the user to type and format the email and store it until internet is available. When an email is submitted to send, the sending process is handled by Message Transfer Agent which is normally comes inbuilt in email client software.



Message Transfer Agent uses SMTP to forward the email to another Message Transfer Agent (Server side). While SMTP is used by end user to only send the emails, the Servers normally use SMTP to send as well as receive emails. SMTP uses TCP port number 25 and 587.

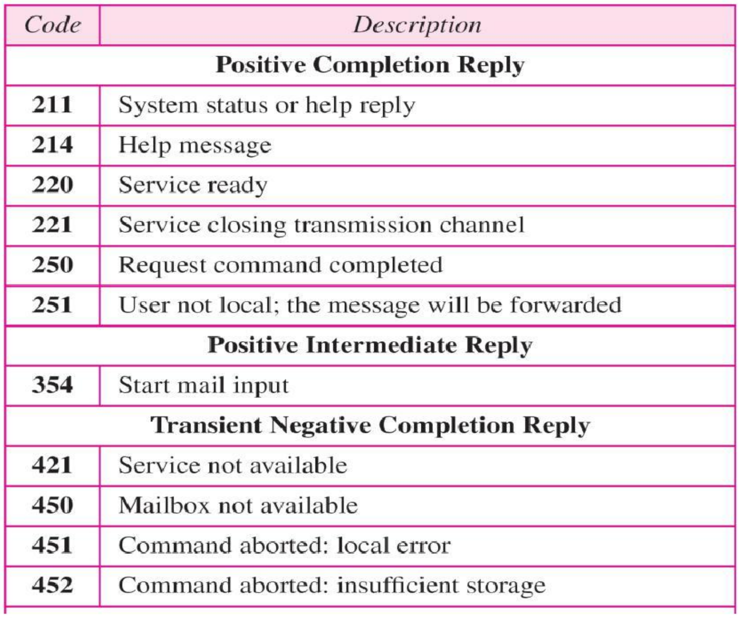
Client software uses Internet Message Access Protocol (IMAP) or POP protocols to receive emails.

Commands

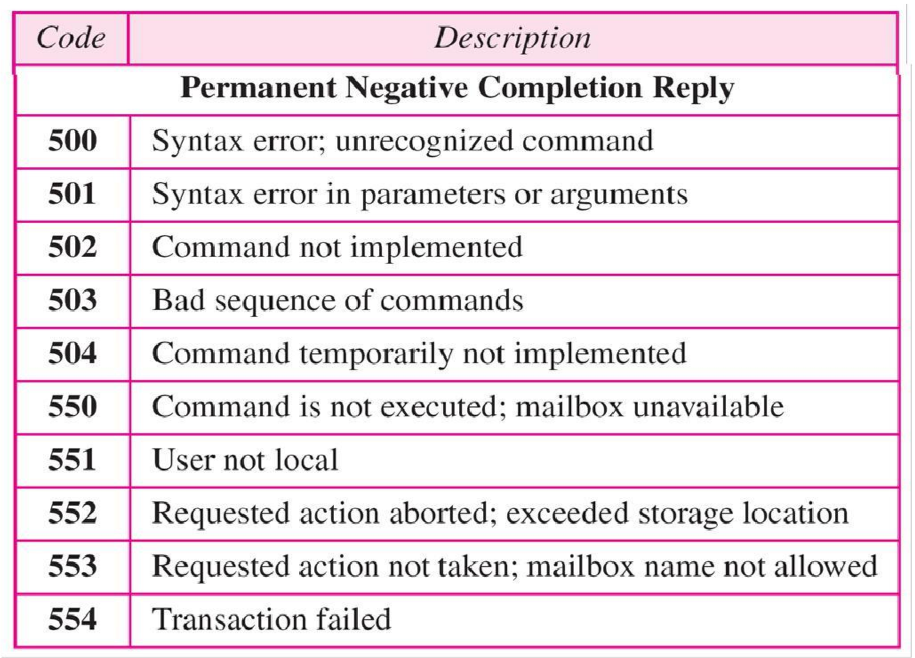


Keyword	*Argument(s)*
HELO	Sender's host name
MAIL FROM	Sender of the message
RCPT TO	Intended recipient of the message
DATA	Body of the mail
QUIT	
RSET	
VRFY	Name of recipient to be verified
NOOP	
TURN	
EXPN	Mailing list to be expanded
HELP	Command name
SEND FROM	Intended recipient of the message
SMOL FROM	Intended recipient of the message
SMAL FROM	Intended recipient of the message

Responses



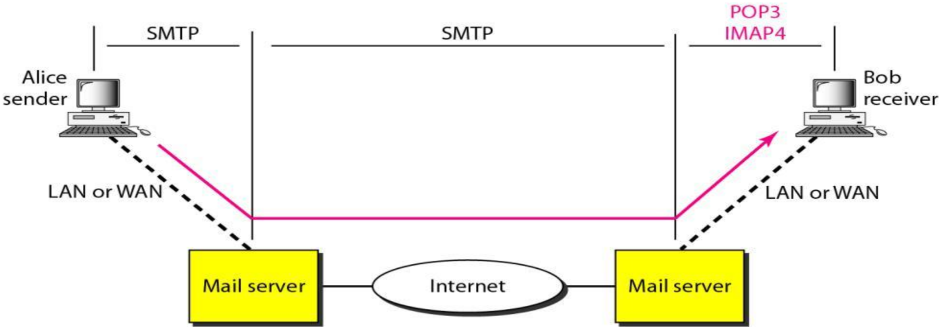
Code	Description
Positive Completion Reply	
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local; the message will be forwarded
Positive Intermediate Reply	
354	Start mail input
Transient Negative Completion Reply	
421	Service not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted: insufficient storage



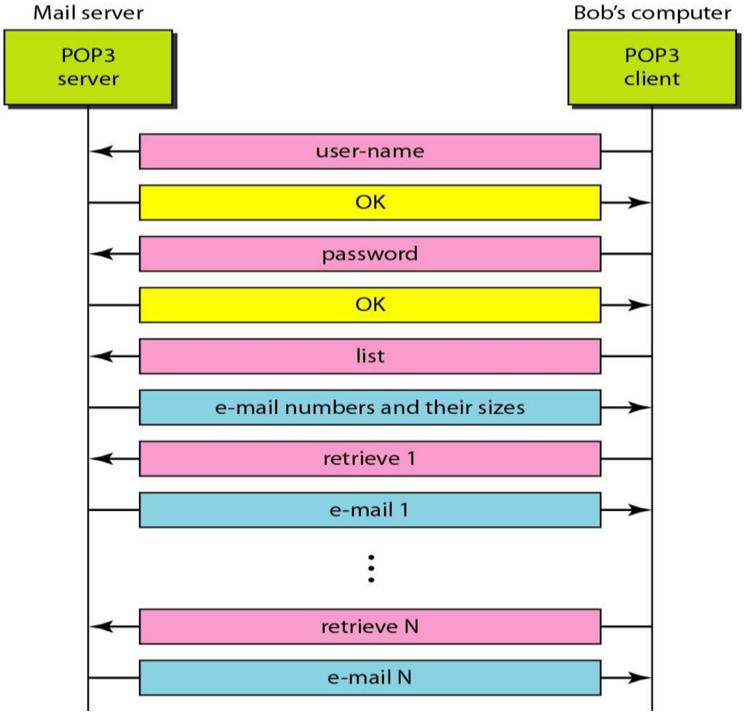
Code	Description
Permanent Negative Completion Reply	
500	Syntax error; unrecognized command
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command temporarily not implemented
550	Command is not executed; mailbox unavailable
551	User not local
552	Requested action aborted; exceeded storage location
553	Requested action not taken; mailbox name not allowed
554	Transaction failed

POST OFFICE PROTOCOL (POP)

The Post Office Protocol version 3 (POP 3) is a simple mail retrieval protocol used by User Agents (client email software) to retrieve mails from mail server.



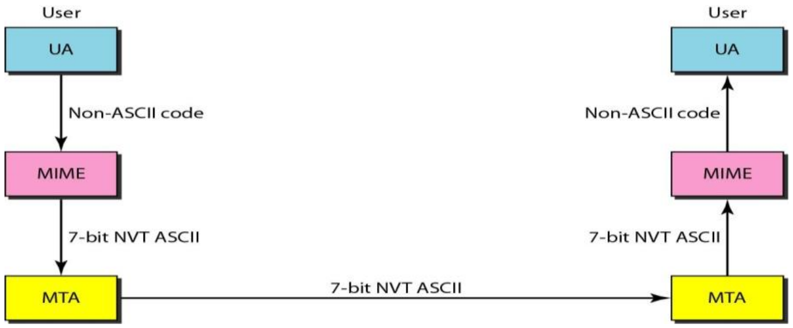
When a client needs to retrieve mails from server, it opens a connection with the server on TCP port 110. User can then access his mails and download them to the local computer. POP3 works in two modes.



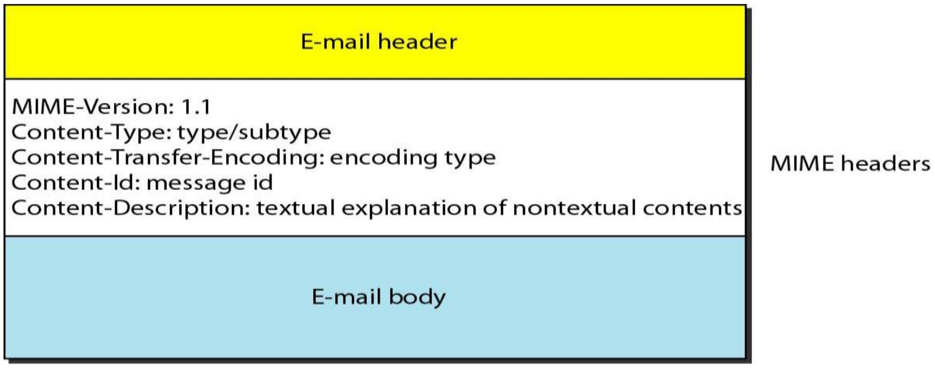
The most common mode the delete mode, is to delete the emails from remote server after they are downloaded to local machines. The second mode, the keep mode, does not delete the email from mail server and gives the user an option to access mails later on mail server.

3. EXPLAIN MIME (MULTIPURPOSE INTERNET MAIL EXTENSION). [CO2 – L2 NOV/DEC 2015]

This allows the transmission of Non ASCII data through the email, MIME allows arbitrary data to be encoded in ASCII and sent in a standard email message.



Each MIME message includes information that tells the recipient the type of data and the type of encoding used and this information along with the MIME version resides in the MIME header. Typical MIME header looks like,


E-mail header
MIME-Version: 1.1
Content-Type: type/subtype
Content-Transfer-Encoding: encoding type
Content-Id: message id
Content-Description: textual explanation of nontextual contents
MIME headers
E-mail body

Content Description: contains the file name of the file that is being sent. Content - Type: is an important field that specifies the data format ie. tells what kind of data is being sent. It contains two identifiers a content type and a subtype separated by a slash. for e.g. image/gif. There are 7 Content Types -

1. text
2. image
3. video
4. audio
5. application

The delivery protocols determine how the mail is transferred by the mail transfer agent to the user agent which provides an interface for reading mails.

4. EXPLAIN DOMAIN NAME SYSTEM. [CO2 – L1]

The Domain Name System (DNS) works on Client Server model. It uses UDP protocol for transport layer communication. DNS uses hierarchical domain based naming scheme. The DNS server is configured with Fully Qualified Domain Names (FQDN) and email addresses mapped with their respective Internet Protocol addresses.
A naming service can be developed to map user-friendly names into router-friendly addresses. Name services are sometimes called middleware because they fill a gap between applications and the underlying network.

Host names differ from host addresses in two important ways. First, they are usually of variable length and mnemonic, thereby making them easier for humans to remember. (In contrast, fixed-length numeric addresses are easier for routers to process).Second, names typically contain no information that helps the network locate (route packets toward) the host. Addresses, in contrast, sometimes have routing information embedded in them; flat addresses (those not divisible into component parts) are the exception.

A namespace defines the set of possible names. A namespace can be either flat (names are not divisible into components), or it can be hierarchical. The naming system maintains a collection of bindings of names to values. The value can be anything we want the naming system to return when presented with a name; in many cases it is an address.

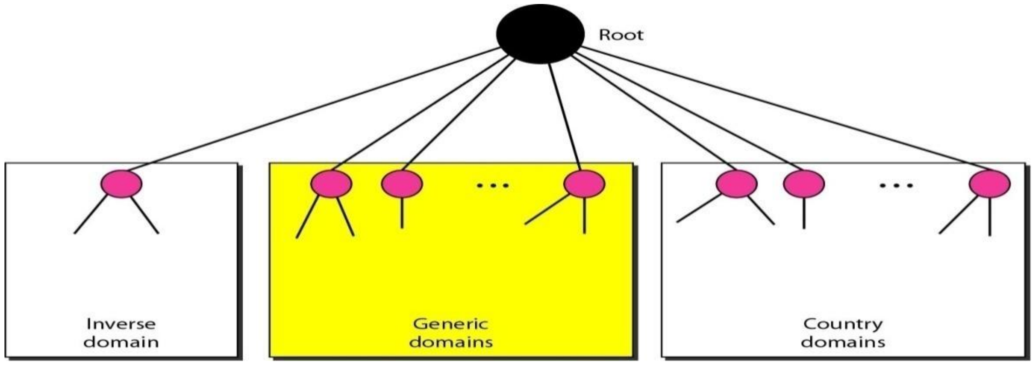
A resolution mechanism is a procedure that, when invoked with a name, returns the corresponding value. A name server is a specific implementation of a resolution mechanism that is available on a network and that can be queried by sending it a message.

DNS employs a hierarchical namespace rather than a flat namespace, and the “table” of bindings that implements this namespace is partitioned into disjoint pieces and distributed throughout the Internet. These sub tables are made available in name servers that can be queried over the network.

What happens in the Internet is that a user presents a host name to an application program, and this program encages the naming system to translate this name into a host address. The application then opens a connection to this host by presenting some transport protocol with the host s IP address.

DOMAIN HIERARCHY:

DNS names are processed from right to left and use periods as the separator. An example domain name for a host is cicada.cs.princeton.edu.There are domains for each country, plus the “big six” domains: .edu, .com,.gov, .mil, .org, and .net.



NAME SERVERS:

The first step is to partition the hierarchy into sub trees called zones. Each zone can be thought of as corresponding to some administrative authority that is responsible for that portion of the hierarchy.

Within this zone, some departments is a zone want the responsibility of managing the hierarchy (and so they remain in the university-level zone), while others, like the Department of Computer science, manage their own department-level zone. The relevance of a zone is that it corresponds to the fundamental unit of implementation in DNS-the name server. Specifically, the
information contained in each zone is implemented in two or more name servers.

Each name server, in turn, is a program that can be accessed over the Internet. Clients send queries to name servers, and name servers respond with the requested information. Sometimes the response contains the final answer that the client wants, and sometimes the response contains a pointer to another that the client should query next.

Each name server implements the zone information as a collection of resource records. In essence, a resource record is a name-to-value binding, or more specifically, a 5-tuple that contains the following fields:

< Name, Value, Type, Class, TTL >

The Name and Value fields are exactly what you would expect, while the Type field specifies how the Value should be interpreted. For example, Type=A indicates that the Value is in IP address. Thus, records implement the name-to-address mapping we have been assuming. Other record types include

NS: The Value field gives the domain name for a host is running a name server that knows how to resolve names within the specified domain.

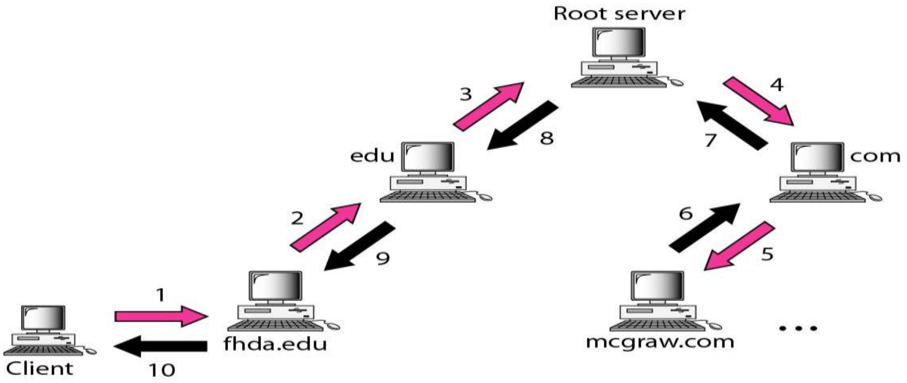
CNAME: the Value field gives the canonical name for a particular host; it is used to define aliases.

MX: The Value field gives the domain name for a host that is running a mail server that accepts the messages for the specified domain.

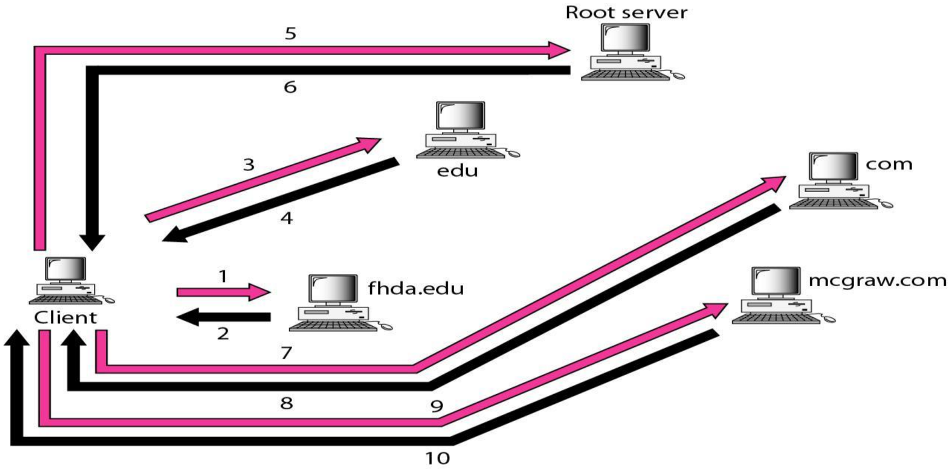
The Class field was included to allow entities other than the NIC to define useful record types.

Finally, the TTL field shows how long this resource record is valid. It is used by servers that cache resource records from other servers; when the TTL expires, the server must evict the record from its cache

Recursive resolution

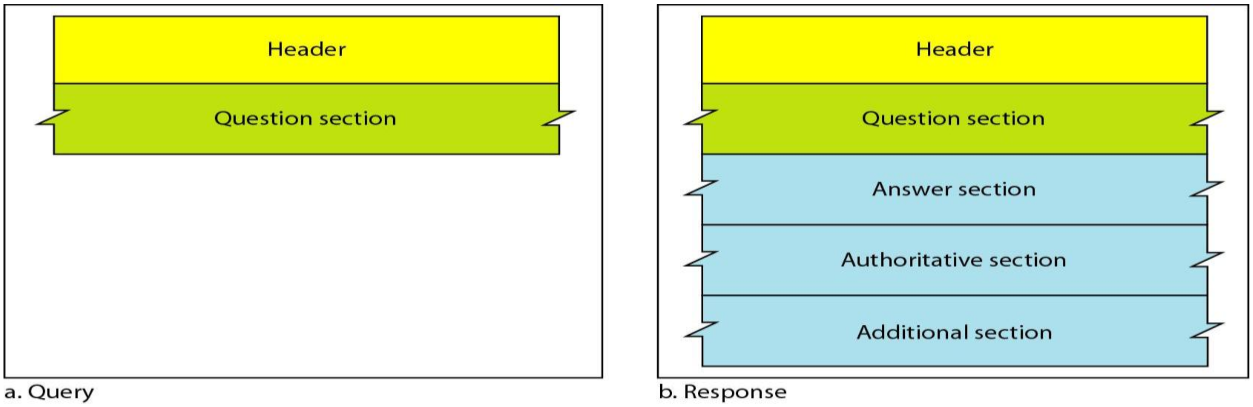


Iterative resolution



A DNS server is requested with FQDN and it responds back with the IP address mapped with it. DNS uses UDP port 53.

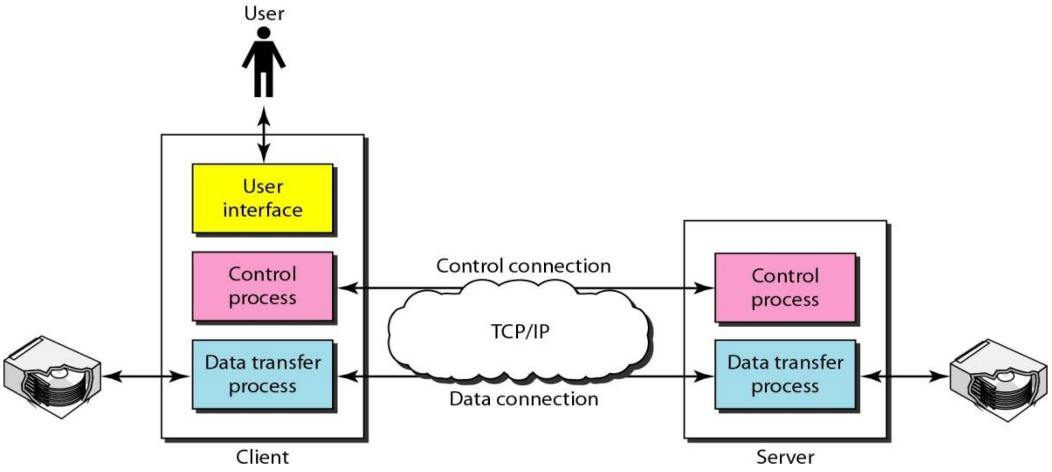
DNS Messages

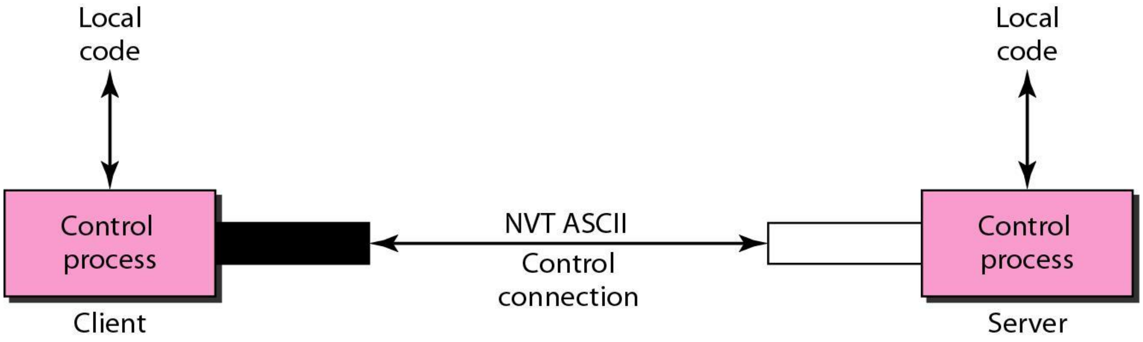


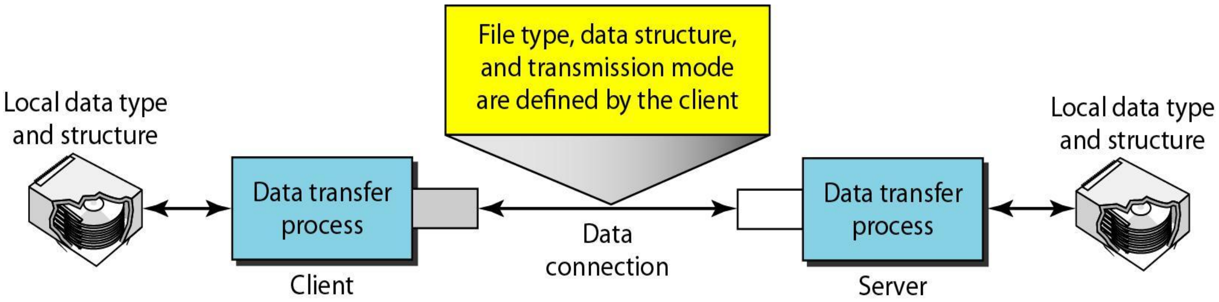
5. EXPLAIN FILE TRANSFER PROTOCOL. [CO2 – L2]

The File Transfer Protocol (FTP) is the most widely used protocol for file transfer over the network. FTP uses TCP/IP for communication and it works on TCP port 21. FTP works on Client/Server Model where a client requests file from Server and server sends requested resource back to the client.

FTP uses out-of-band controlling i.e. FTP uses TCP port 20 for exchanging controlling information and the actual data is sent over TCP port 21.






File type, data structure, and transmission mode are defined by the client
Local data type and structure
Local data type and structure
Data transfer process
Data connection
Data transfer process
Client
Server

The client requests the server for a file. When the server receives a request for a file, it opens a TCP connection for the client and transfers the file. After the transfer is complete, the server closes the connection. For a second file, client requests again and the server reopens a new TCP connection.

6. EXPLAIN HYPER TEXT TRANSFER PROTOCOL (HTTP). [CO2 – L2]

The Hyper Text Transfer Protocol (HTTP) is the foundation of World Wide Web. Hypertext is well organized documentation system which uses hyperlinks to link the pages in the text documents. HTTP works on client server model. When a user wants to access any HTTP page on the internet, the client machine at user end initiates a TCP connection to server on port 80. When the server accepts the client request, the client is authorized to access web pages. The protocol transfer all data in the
form of plain text, hypertext, audio, video, and so on. However it is called the hypertext transfer protocol because its efficiency allows its use in a hypertext environment where there are rapid jumps from one document to another.

To access the web pages, a client normally uses web browsers, who are responsible for initiating, maintaining, and closing TCP connections. HTTP is a stateless protocol, which means the Server maintains no information about earlier requests by clients.

HTTP functions like a combination of FTP and SMTP. It is similar to FTP because it transfers files and uses the services of TCP. However, it is much simpler than FTP because it uses only data are transferred between the client and the server.

HTTP is like SMTP because the data transferred between the client and server look like SMTP messages. In addition, the format of the messages is controlled by MIME-like headers.
However, HTTP differs from SMTP in the way the messages are sent from the client to the server and from the server to the client. Unlike SMTP, the HTTP messages are not destined to be read by humans; they are read and interpreted by the HTTP server and HTTP client (browser). SMTP messages are stored and forwarded, but HTTP messages are delivered immediately.

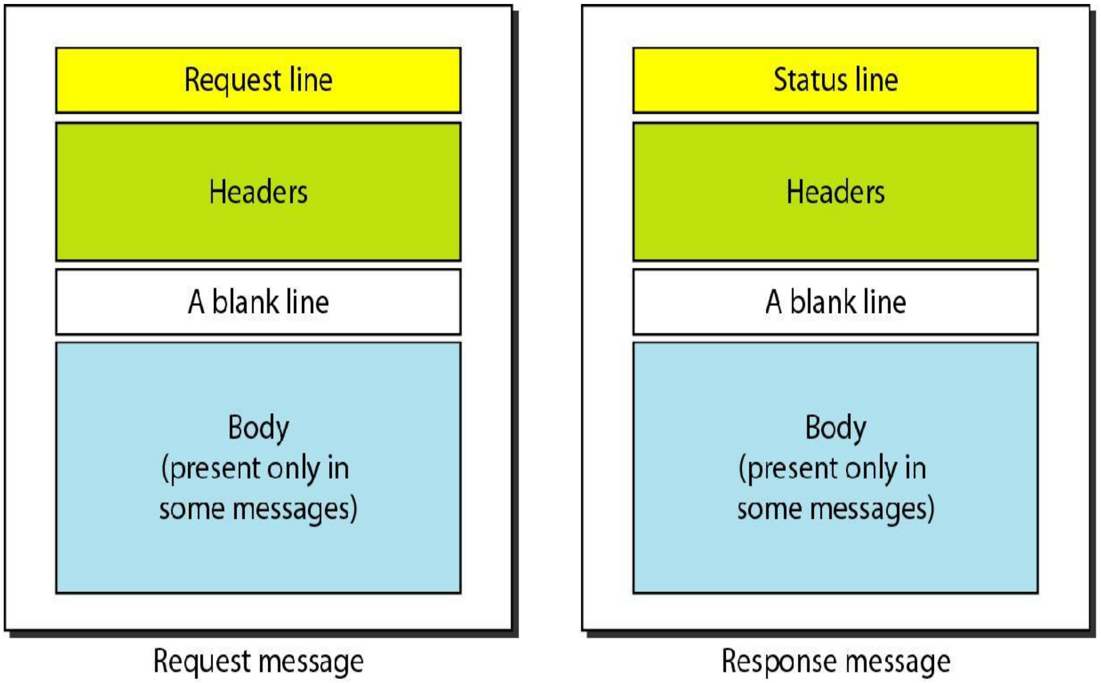
The idea of HTTP is very simple. A client sends a request, which looks like mail, to the server. The
server sends the response, which looks like a mail reply, to the client. The request and response messages carry data in the form of a letter with MIME-like format. The commands from the client to the server are embedded in a letter like request message. The contents of the requested file or other information are embedded in a letter like response message.

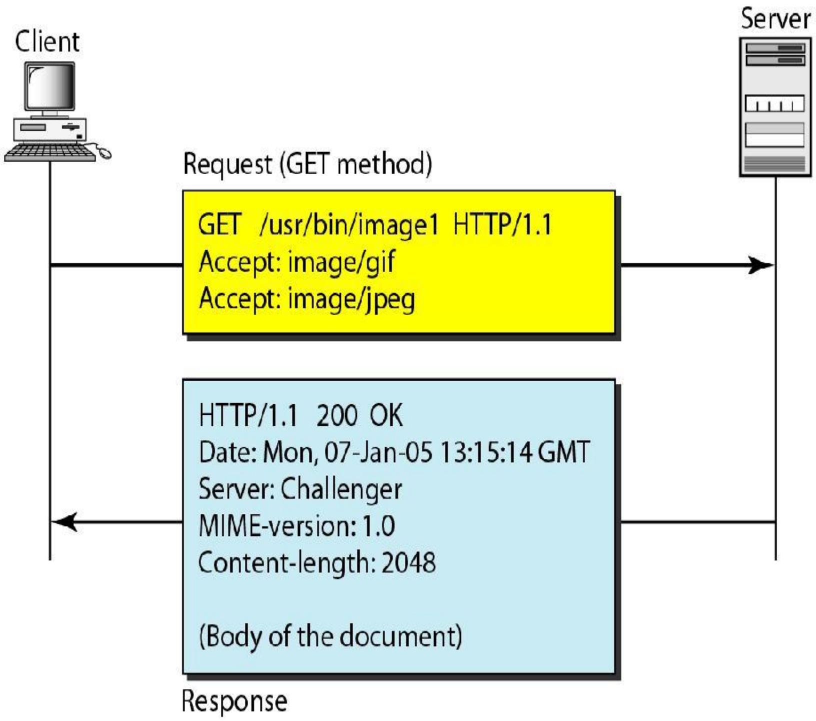
HTTP Transaction

Client initializes the transaction by sending a request message. The server replies by sending a
response.

Messages

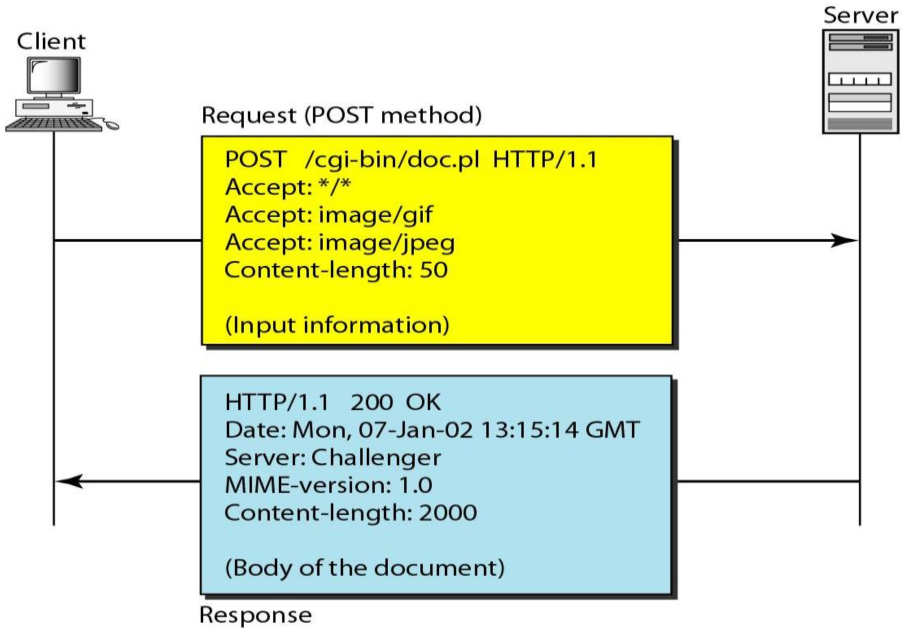
There are two general types of HTTP messages, shown in figure request and response. Both message types follow almost the same format.





```
GET  /usr/bin/image1  HTTP/1.1
Accept: image/gif
Accept: image/jpeg
```

```
HTTP/1.1  200  OK
Date: Mon, 07-Jan-05 13:15:14 GMT
Server: Challenger
MIME-version: 1.0
Content-length: 2048

(Body of the document)
```



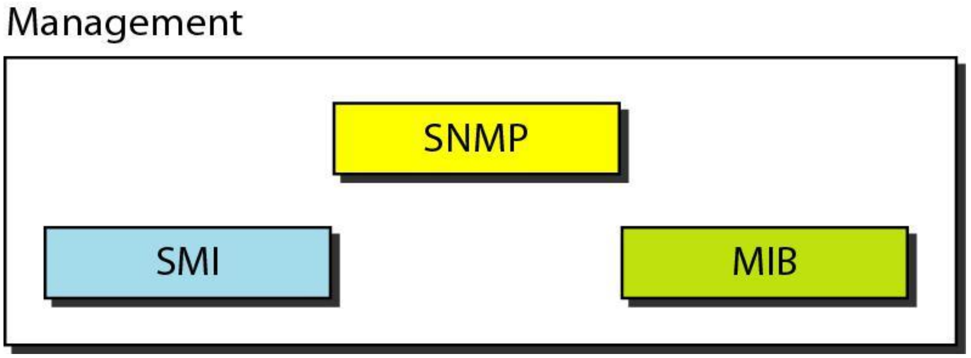
```
POST   /cgi-bin/doc.pl  HTTP/1.1
Accept: */*
Accept: image/gif
Accept: image/jpeg
Content-length: 50

(Input information)
```

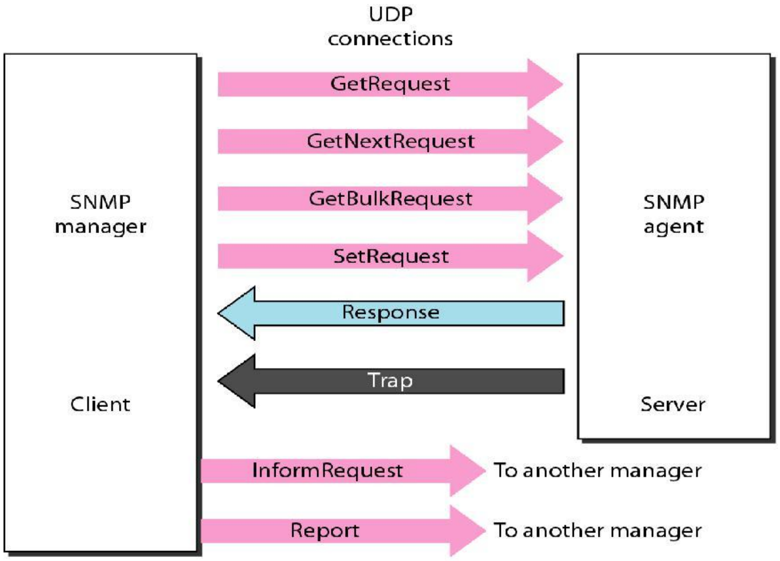
```
HTTP/1.1   200  OK
Date: Mon, 07-Jan-02 13:15:14 GMT
Server: Challenger
MIME-version: 1.0
Content-length: 2000

(Body of the document)
```

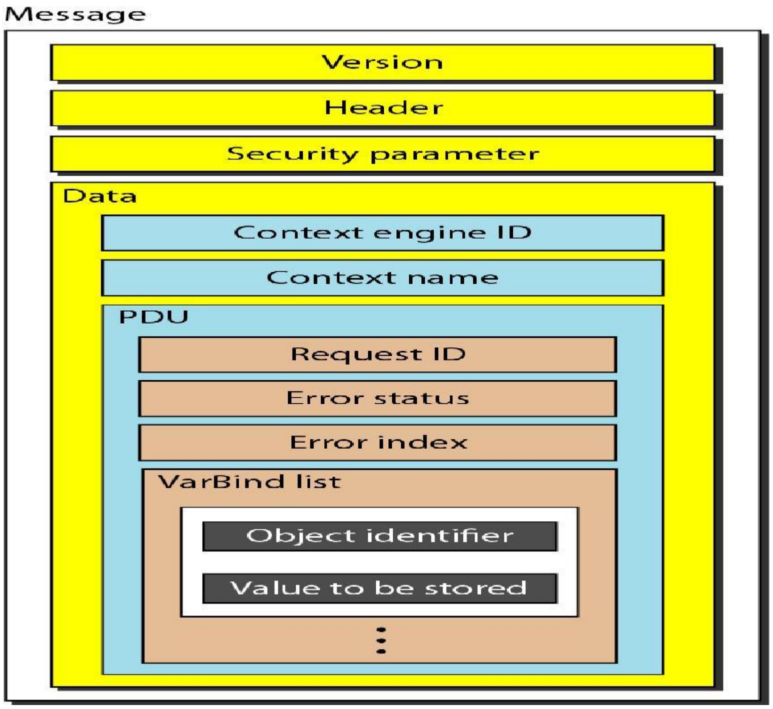
7. EXPLAIN SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL). [CO2 – L2]

A large network can often get into various kinds of trouble due to routers (dropping too many packets), hosts(going down) etc. One has to keep track of all these occurrence and adapt to such situations. A protocol has been defined. Under this scheme all entities in the network belong to 4 classes:

1. Managed Nodes
2. Management Stations
3. Management Information (called Object)
4. A management protocol







The managed nodes can be hosts, routers, bridges, printers or any other device capable of communicating status information to others. To be managed directly by SNMP, a node must be capable of running am SNMP management process, called SNMP agent. Network management is done by management stations by exchanging information with the nodes. These are basically general purpose computers running special management software. The management stations polls the stations periodically. Since SNMP uses unreliable service of UDP the polling is essential to keep in touch with the nodes. Often the nodes send a trap message indicating that it is going to go down.

The management stations then periodically checks (with an increased frequency). This type of polling is called trap directed polling. Often a group of nodes are represented by a single node which
communicates with the management stations. This type of node is called proxy agent. The proxy agent can also serve as a security arrangement. All the variables in these schemes are called Objects. Each variable can be referenced by a specific addressing scheme adopted by this system. The entire collection of all objects is called Management Information Base (MIB).

The information are exchanged in a standard and vendor-neutral way. All the data are represented in Abstract Syntax Notation 1 (ASN.1). It is similar to XDR as in RPC but it has widely different representation scheme. A part of it actually adopted in SNMP and modified to form Structure Of Information Base. The Protocol specifies various kinds of messages that can be exchanged between the managed nodes and the management station.