PART A

1. Compare LAN and WAN.

LAN	WAN
Scope of Local Area Network is restricted to a small/ single building	Scope of Wide Area Network spans over large geographical area country/ Continent
LAN is owned by some organization.	A part of n/w asserts are owned or not owned.
Data rate of LAN 10-100mbps.	Data rate of WAN is Gigabyte.

2. Define Full Duplex and simplex transmission system.

With Full duplex transmission, two stations can simultaneously send and receive data from each other. This mode is known as two-way simultaneous. The signals are transmitted in only one direction. One is the sender and another is the receiver.

3. Why sliding window flow control is considered to be more efficient than stop and wait flow control?

In sliding window flow control, the transmission link is treated as a pipeline that may be filled with frames in transit. But with stop-and-wait flow control only one frame may be in the pipe at a time.

4. Differentiate between lost frame and damaged frame? What is the difference between stop and wait and sliding window protocol? (Nov/Dec 2012)

Lost Frame	Damaged Frame
Lost frame is the frame that fails to arrive at the other side.	The damaged frame is a recognizable frame does arrive, but some of the bits are in error

Stop and Wait Protocol	Sliding Window Protocol
In stop and wait protocol, we can send one frame at a time	In sliding window protocol we can send multiple frames at a time.
Shows poor performance than Sliding Window Protocol, comparatively	As sliding window doesn't waste network bandwidth compared with stop-n-wait, both in normal and in congested condition, sliding window show better performance than stop-n-wait.

5. Define Piggybacking?

The technique of temporarily delaying outgoing acknowledgment so that they can be hooked onto the next outgoing data frame is widely known as piggybacking.

6. What is OSI?

OSI (Open Systems Interconnection) is reference model for how applications can communicate over a network. It is partitioned into seven layers. It was developed by the International Organization for Standardization (ISO).

7. What is a protocol? What are the key elements of a protocol?

Protocol is used for communications between entities in a system and must speak the same language. Protocol is the set of rules governing the exchange of data between two entities. It defines what is communicated, how it is communicated, when it is communicated. The Key elements of a Protocol are as follows,

- **Syntax** – It refers to the structure or format of data meaning the order in which they are presented.
- **Semantics** – It refers to the meaning of each section of bit. How to do interpretation.
- **Timing** – When data should be sent and how fast they can be sent.

8. What are the uses of transport layer?

- Reliable data exchange
- Independent of network being used
- Independent of application

9. What is Protocol Data Unit (PDU)?

At each layer, protocols are used to communicate and Control information is added to user data at each layer. Transport layer may fragment user data. Each fragment has a transport header added and header consists of destination SAP, sequence number and error detection code.

10. What are the uses of internet layer in TCP/IP?

- Systems may be attached to different networks
- Routing functions across multiple networks
- Implemented in end systems and routers

11. What is a layered Network Architecture?

- A layer is created when a different level of abstraction occurs at protocol. Each layer should perform a well defined function.
- Function of each layer should be chosen using internationality standardized protocols. Boundaries between should be chosen to minimize information flow across the interfaces.
- A set of layers and protocol is called network architecture. A list of protocols used by a system is called protocol stack.

12.Compare OSI and TCP.

Open System Interconnection	**Transmission Control Protocol**
It distinguishes between Service, Interface, Protocol	It does not distinguish between Service,Interface,Protocol
Protocols are well hidden	Protocols are not just hidden
Dejure standard Fit Model	Defacto standard Fit Model
In transport layer only connection oriented services are available	In Transport layer choice is for connection oriented and connectionless
Contains 7 layers	Contains 5 layers

13. How do layers of the internet model correlate to the layers of the OSI model?

OSI	**TCP/IP**
Physical Layer	Physical Layer
Data Link Layer	Network Access Layer
Network Layer	IP Layer
Transport Layer	TCP Layer
Session Layer	Application Layer
Presentation Layer	
Application layer	

14. What is the use of data link layer in OSI?

- **Frame synchronization**: Data is divided by data link layer as frames, a manageable unit.
- **Flow Control**: Sending station does not overwhelm receiving station.
- **Error Control**: Any error in bits must be detected and corrected using some mechanism.
- **Addressing**: Two stations in a multi point that involved in transmission must be specified using physical address
- **Access Control**: When two or more devices are connected to the same link, Access control mechanism is needed to determine which device has control over the link at any given time.

15. Why is flow control and error control duplicated in different layers?

Like the data link layer, the transport layer is responsible for flow and error control. Flow control and error control at data link layer is node-to-node level. But at transport layer, flow control and error control is performed end-end rather than across a single link.

16. List the key ingredients of technology that determines nature of a LAN. List the common topologies available for LAN.

Topology, Transmission medium and Medium access control technique are the technology that determines nature of a LAN. Star Topology, Ring Topology, Bus Topology and Tree Topology are the topologies available for LAN.

17. What are the functions of physical layer and presentation layer?

Functions of Physical Layer-

- Encoding/ decoding of signals
- Preamble generation/removal (for synchronization)
- Bit transmission/ reception

Functions of Presentation Layer-

- Translation, Encryption / Decryption

- Authentication and Compression

18. What do you mean by Flow Control? (Nov/Dec 2011)

Flow control is a technique for assuring that a transmitting entity does not overwhelm a receiving entity with data. It is a feedback mechanism by which the receiver is able to regulate the sender. Such a mechanism is used to keep the sender from overrunning the receiver, i.e., from transmitting more data than the receiver is able to process

19. Define error detection and correction. (Nov/Dec 2011)

Error detection: Sender transmits every data unit twice. Receiver performs bit-by-bit comparison between that two versions of data. Any mismatch would indicate an error, which needs error correction. Error Correction is the process or analyzing and rectifying the errors and the code.

20. What are the functions of Application Layer? (Apr/May 2011)

It enables the user (human/software) to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management and other types of distributed information services. Services provided by the application layer are Network Virtual terminal, File transfer, access and management. Mail services, Directory services.

21. Define bit stuffing. (Apr/May 2011)

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.

22. What are the two types of line configuration? (Nov/Dec 2010)

The two types of line configuration are Point to point line configuration and multipoint line configuration.

Point to point line configuration

- It provides a dedicated link between 2 devices.
- Entire capacity of the link is reserved for transmission between 3 devices only

Eg: connection between remote control and TV's control system

Multipoint line configuration

- Also called as multi drop connection
- Here the channel capacity is shared
- If many devices share the link simultaneously it is called spatially shared connection

23. What do you mean by error control? (Nov/Dec 2010)

Error control refers to mechanism to detect and correct errors that occur in the transmission of frames.

24. What are the major duties of Network Layer? (May/June 2012)

It is used to send the data from source to destination with help of logical address.

25. What are the two types of errors occurred during data transmission? (May/June 2012)

Single bit error and burst error

26. Define networks.(Nov/Dec 2012)

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Networks are commonly categorized based on their characteristics.

27. Compare error detection and correction. (Nov/Dec 2012)

Error Detection	Error Correction
Only the occurrence of an error is checked	The exact number of bit that are corrupted and location of error in the message are known.

28.What do you meant by framing? (Nov/Dec2013 and Nov/Dec 2014)

The data link layer divides the stream of bits received from the network layer into manageable data units called frames. The ways to address the framing problem are

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

29.Define a layer. (Nov/Dec 2013)

- A layer is created when a different level of abstraction occurs at protocol. Each layer should perform a well defined function.
- Function of each layer should be chosen using internationality standardized protocols. Boundaries between should be chosen to minimize information flow across the interfaces.
- A set of layers and protocol is called network architecture. A list of protocols used by a system is called protocol stack.

30. **What is the purpose of layering? (May 2013)**

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

PART-B

1. **Explain in detail the error detection. (Nov/Dec 2010, Apr/May 2012, Nov/Dec 2012,Nov/Dec 2014)**

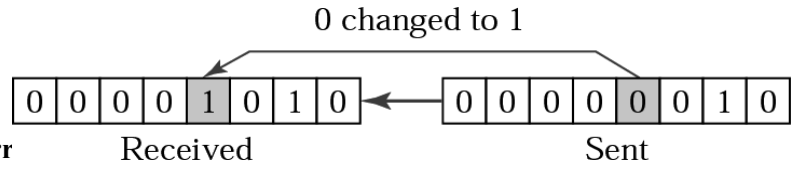
Error Detection

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

Types of Errors

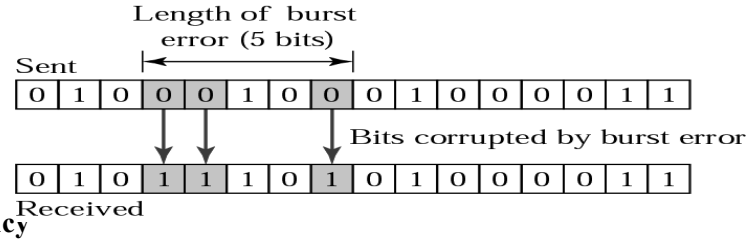
Single-bit error

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 Err

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.

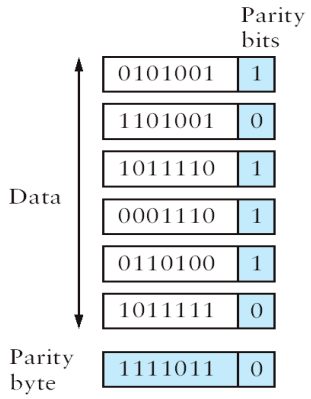


Fig: Two-dimensional parity

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.

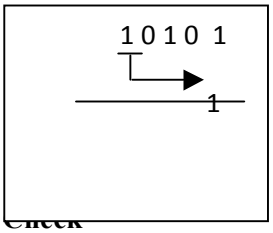
In this case, 14 bits of redundant information are added with original information.

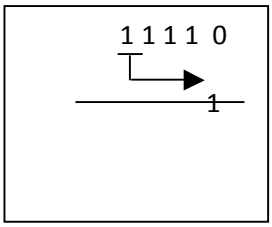
Check sum algorithm

- 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.

Sender Receiver

7	7





Cyclic Redundancy Check

- It uses small number of redundant bits to detect errors.
- Divisor is calculated by the polynomial functions under two conditions

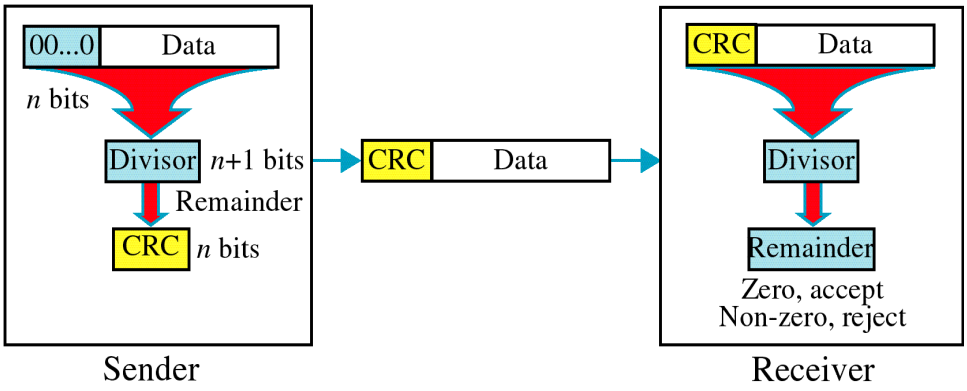
  a. It should not be divisible by x

  b. It should be divisible by x+1

  Consider the original message as M(x) – n+1 bits

  Divisor C(x) – K bits

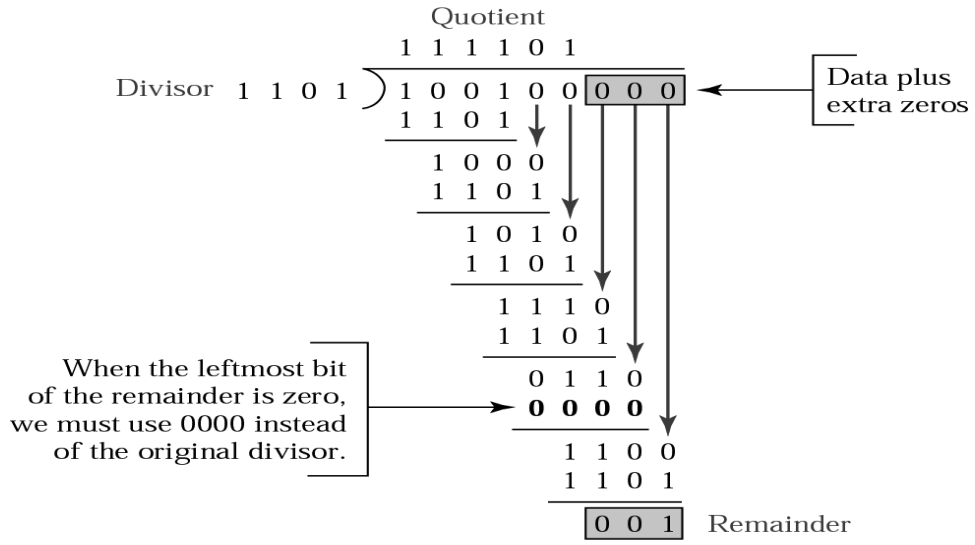
  Original sent message = M(x) + k-1 bits



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



2. **Explain about internet architecture.**

The Internet architecture, also called the TCP/IP architecture after its two main protocols, is depicted in Fig.1. An alternative representation is given in Fig.2.

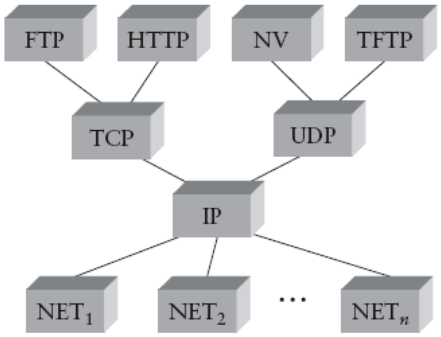


Fig.1 Internet protocol graph.

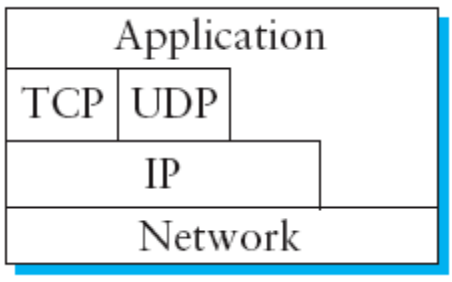


Fig2. Alternative view of the Internet architecture.

At the lowest level are a wide variety of network protocols, denoted NET1, NET2, and so on.

The *Internet Protocol* (IP) supports the interconnection of multiple networking technologies into a single, logical internetwork

The third layer contains two main protocols: the *Transmission Control Protocol* (TCP) and the *User Datagram Protocol* (UDP).

TCP and UDP provide alternative logical channels to application programs: TCP provides a reliable byte-stream channel, and UDP provides an unreliable datagram delivery channel.

The Internet architecture has three features:

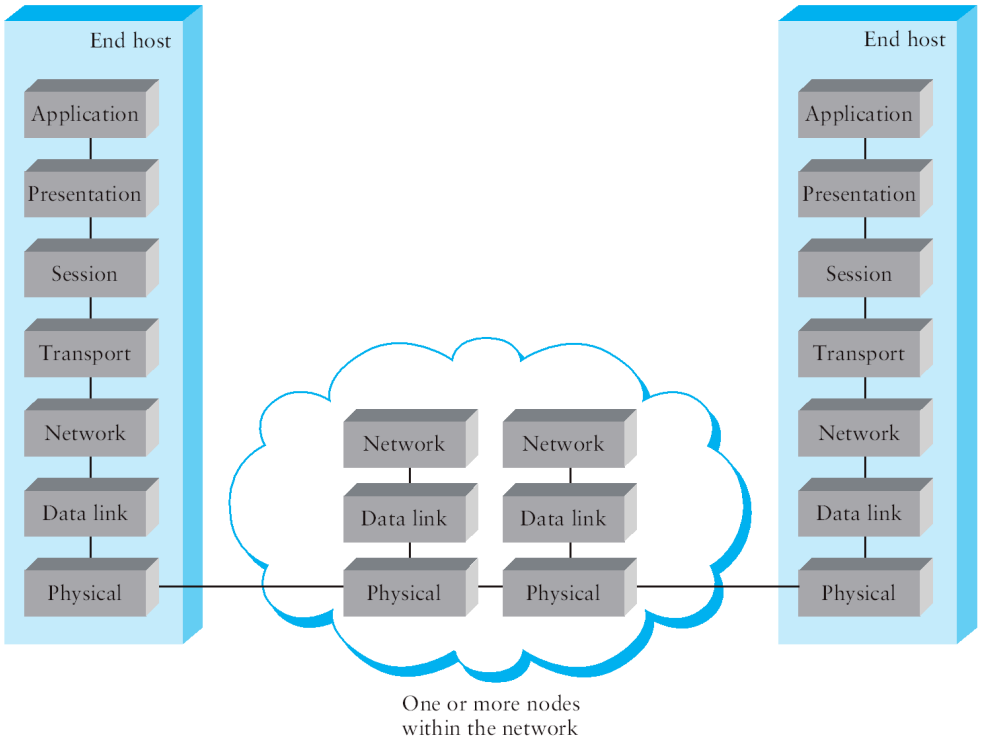
1. The application is free to bypass the defined transport layers and to directly use IP or one of the underlying networks.
   2. IP serves as the focal point for the architecture—it defines a common method for exchanging packets among a wide collection of networks. Above IP can be arbitrarily many transport protocols, each offering a different channel abstraction to application programs.
   Below IP, the architecture allows for arbitrarily many different network technologies, ranging from Ethernet to FDDI to ATM to single point-to-point links.
2. The existence of working implementations is required for standards to be adopted by the IETF.

3.**Discuss in detail about the layers in OSI model. (Nov/Dec2010, Nov/Dec2011, Apr/May2012, Nov/Dec 2012)**

OSI Architecture

ISO defines a common way to connect computer by the architecture called Open System Interconnection (OSI) architecture.

Network functionality is divided into seven layers.

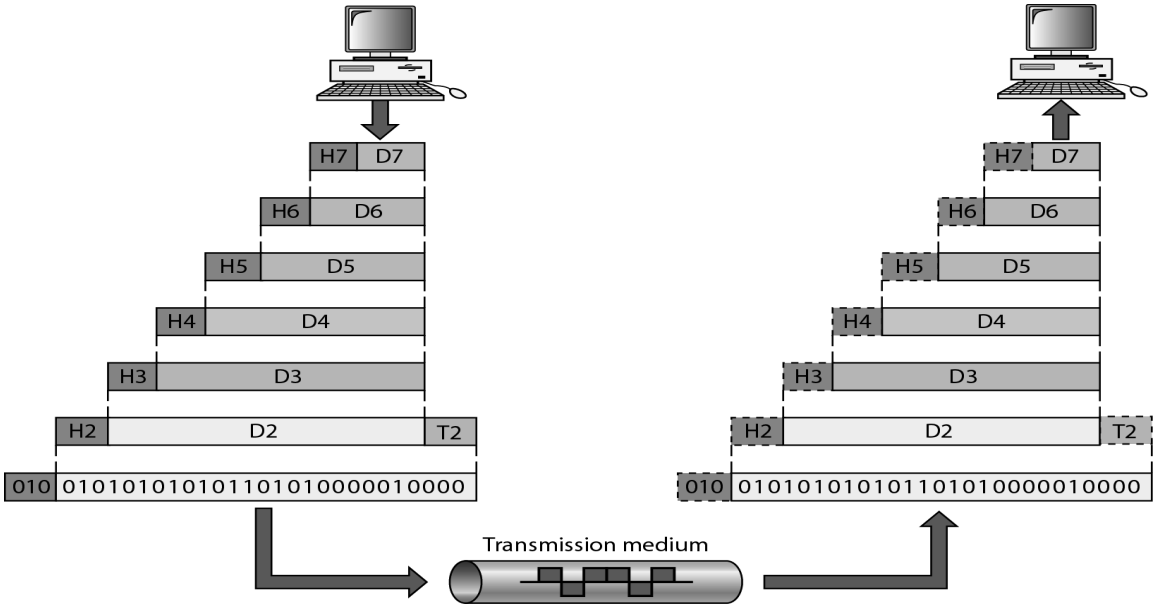


Organization of the layers

The 7 layers can be grouped into 3 subgroups

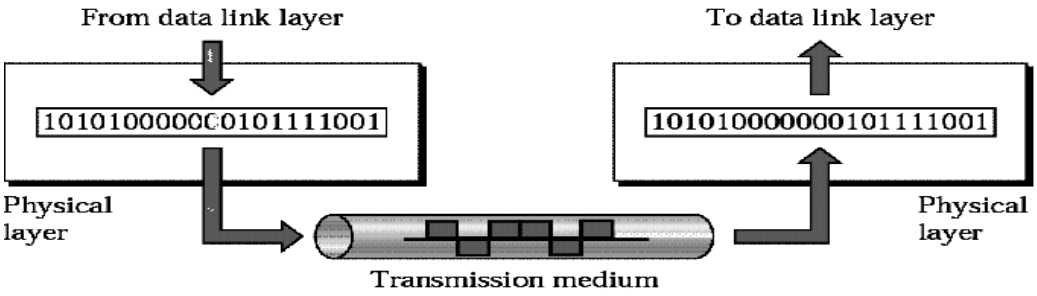
1. **Network Support Layers**
   Layers 1,2,3 - Physical, Data link and Network are the network support layers. They deal with the physical aspects of moving data from one device to another such as electrical specifications, physical addressing, transport timing and reliability.
2. **Transport Layer**
   Layer4, transport layer, ensures end-to-end reliable data transmission on a single link.
3. **User Support Layers**
   Layers 5,6,7 – Session, presentation and application are the user support layers. They allow interoperability among unrelated software systems

An Data exchange using the OSI model



1. Physical Layer

The physical layer coordinates the functions required to transmit a bit stream over a physical medium.



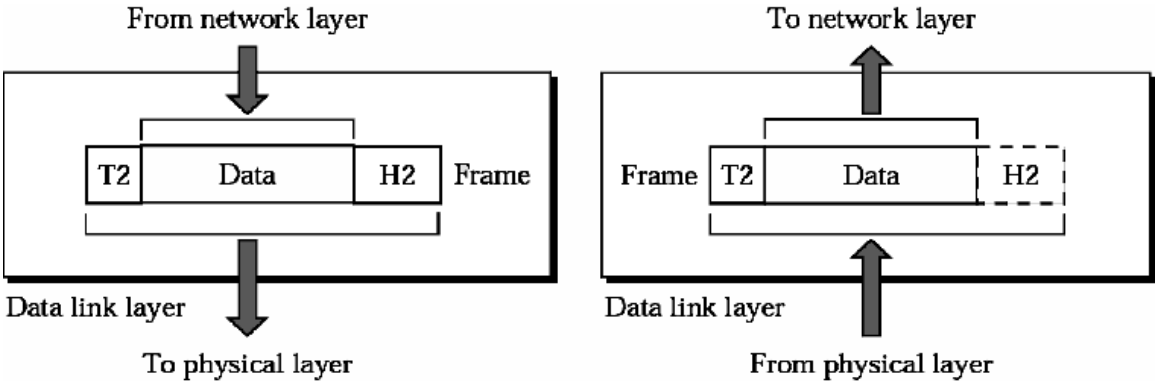
The physical layer is concerned with the following:

- **Physical characteristics of interfaces and media -** The physical layer defines the characteristics of the interface between the devices and the transmission medium.
- **Representation of bits -** To transmit the stream of bits, it must be encoded to signals. The physical layer defines the type of encoding.
- **Data Rate or Transmission rate -** The number of bits sent each second – is also defined by the physical layer.
- **Synchronization of bits -** The sender and receiver must be synchronized at the bit level. Their clocks must be synchronized.
- **Line Configuration -** In a point-to-point configuration, two devices are connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.
- **Physical Topology -** The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh, bus, star or ring topology.

- **Transmission Mode -** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex or full-duplex.

2. Data Link Layer

It is responsible for transmitting frames from one node to next node.

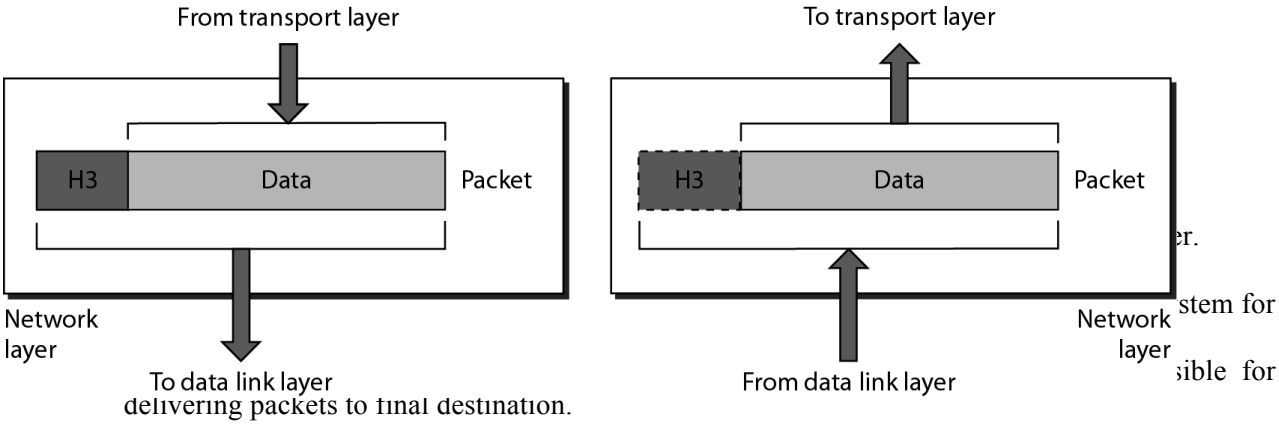


The other responsibilities of this layer are

- **Framing -** Divides the stream of bits received into data units called frames.
- **Physical addressing** – If frames are to be distributed to different systems on the n/w , data link layer adds a header to the frame to define the sender and receiver.
- **Flow control**- If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the Data link layer imposes a flow ctrl mechanism.
- **Error control**- Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
- **Access control** -Used to determine which device has control over the link at any given time.

3. NETWORK LAYER

This layer is responsible for the delivery of packets from source to destination.



er.

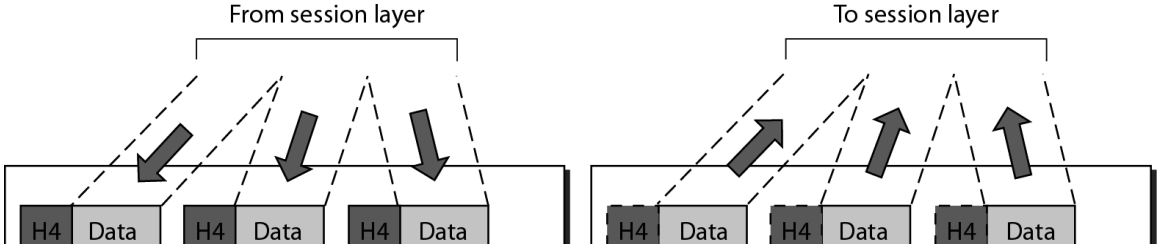
stem for

sible for

delivering packets to final destination.

4. TRANSPORT LAYER

- It is responsible for **Process to Process** delivery.
- It also ensures whether the message arrives in order or not.

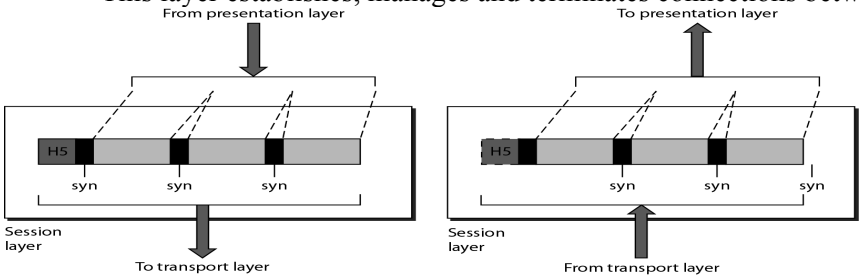


The other responsibilities of this layer are

- **Port addressing** - The header in this must therefore include a address called port address. This layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly** - The message is divided into segments and each segment is assigned a sequence number. These numbers are arranged correctly on the arrival side by this layer.
- **Connection control** - This can either be **connectionless or connection-oriented.** The connectionless treats each segment as a individual packet and delivers to the destination. The connection-oriented makes connection on the destination side before the delivery. After the delivery the termination will be terminated.
- **Flow and error control** - Similar to data link layer, but process to process take place.

5. SESSION LAYER

This layer establishes, manages and terminates connections between applications.

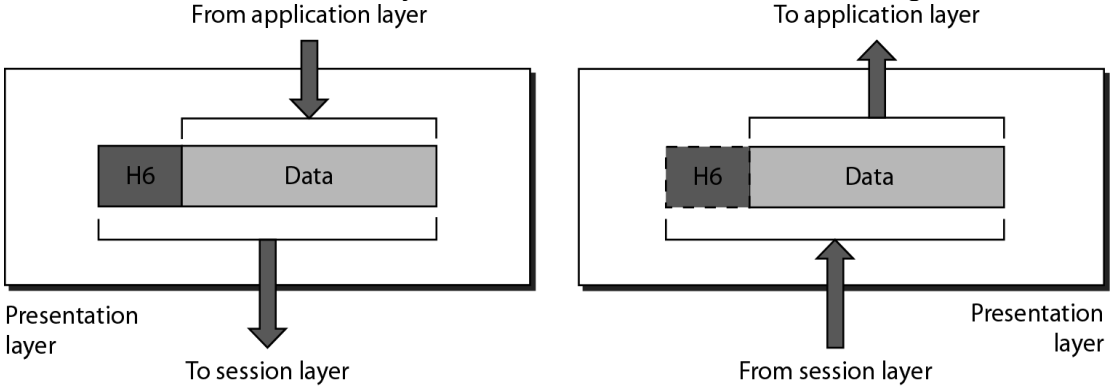


The other responsibilities of this layer are

- **Dialog control** - This session allows two systems to enter into a dialog either in half duplex or full duplex.
- **Synchronization**-This allows to add checkpoints into a stream of data.

6. PRESENTATION LAYER

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

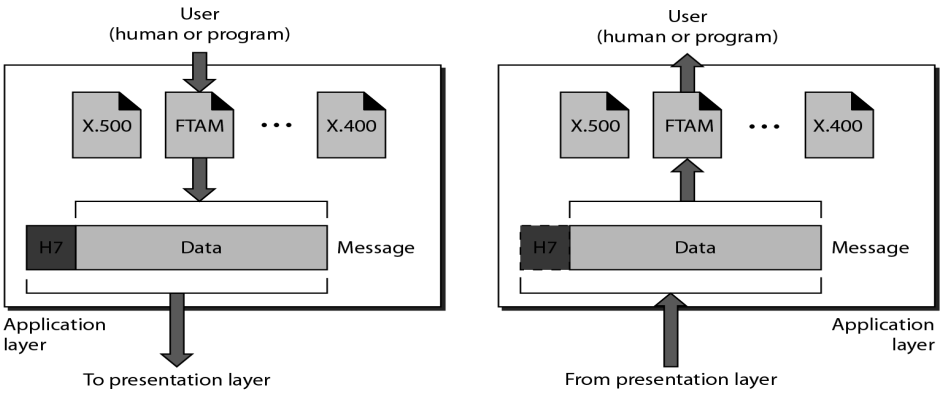


The other responsibilities of this layer are

- **Translation** – Different computers use different encoding system, this layer is responsible for interoperability between these different encoding methods. It will change the message into some common format.
- **Encryption and decryption**-It means that sender transforms the original information to another form and sends the resulting message over the n/w. and vice versa.
- **Compression and expansion**-Compression reduces the number of bits contained in the information particularly in text, audio and video.

7. APPLICATION LAYER

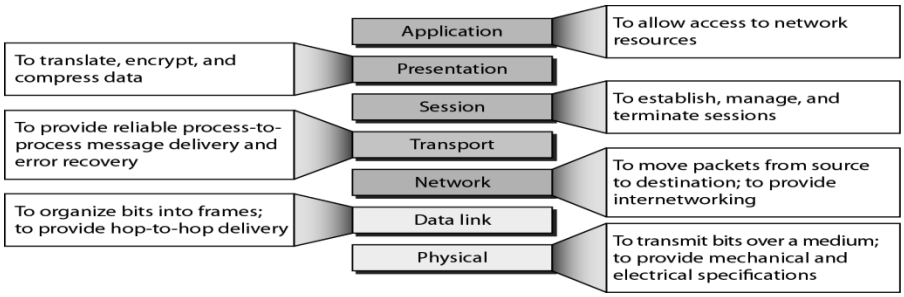
This layer enables the user to access the n/w. This allows the user to log on to remote user.



The other responsibilities of this layer are

- **FTAM(file transfer,access,mgmt)** - Allows user to access files in a remote host.
- **Mail services** - Provides email forwarding and storage.
- **Directory services** - Provides database sources to access information about various sources and objects.

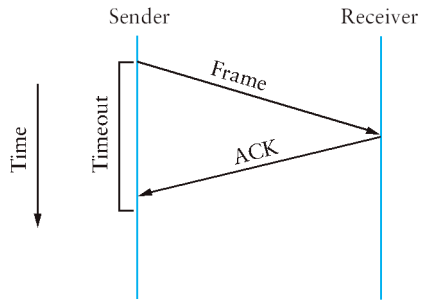
Summary of layers



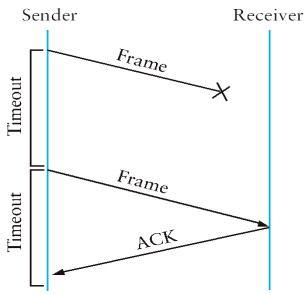
4. **Explain sliding window flow control and stop and wait flow control in detail.**

STOP AND WAIT ALGORITHM

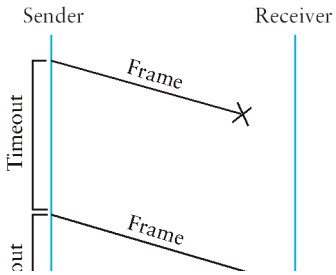
- After transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame.
- If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmit the original frame.

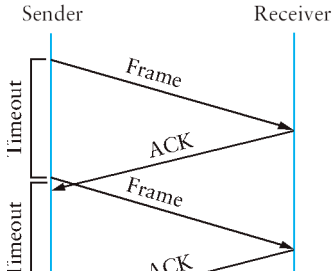


a) The ACK is received before the timer expires



b) The original frame is lost

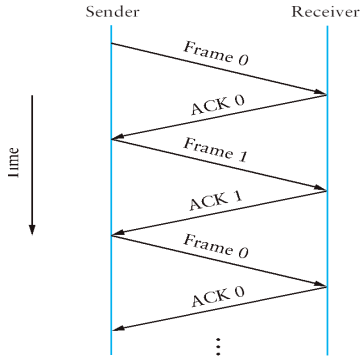




c) The ACK is lost d) The timeout fires too soon

Fig: illustrates four different scenarios that result from this basic algorithm. The sending side is represented on the left, the receiving side is depicted on the right, and time flows from top to bottom.

- In Fig (a) ACK is received before the timer expires, (b) and (c) show the situation in which the original frame and the ACK, respectively, are lost, and (d) shows the situation in which the timeout fires too soon..
- Suppose the sender sends a frame and the receiver acknowledges it, but the acknowledgment is either lost or delayed in arriving. This situation is in (c) and (d). In both cases, the sender times out and retransmit the original frame, but the receiver will think that it is the next frame, since it correctly received and acknowledged the first frame.



- This makes the receiver to receive the duplicate copies. To avoid this two sequence numbers (0 and 1) must be used alternatively.
- The main drawback of the stop-and-wait algorithm is that it allows the sender have only one outstanding frame on the link at a time.

SLIDING WINDOW ALGORITHM

- 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.

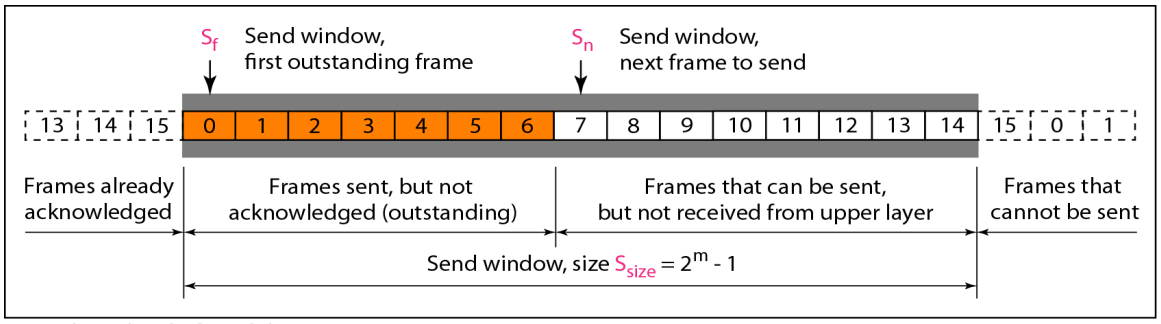
  There are two methods to retransmit the lost frames
  - GO-Back N
  - Selective Repeat

Go – Back N Method

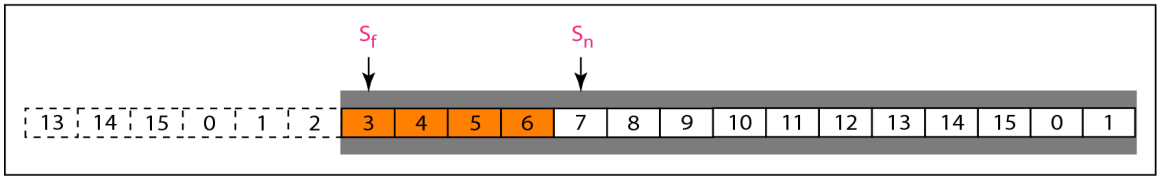
Sender Window

- 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.



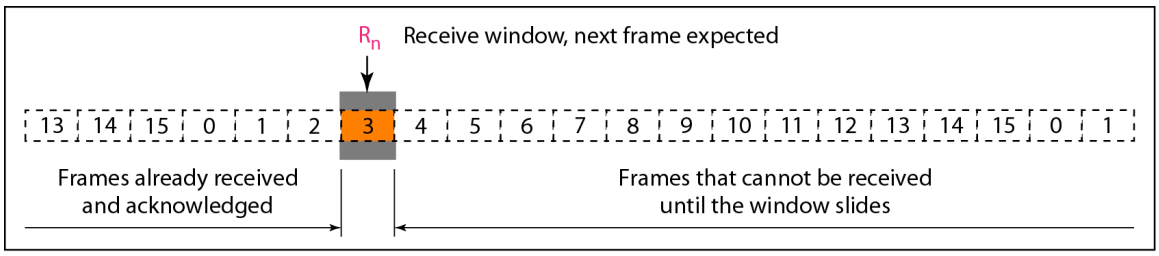
a. Send window before sliding



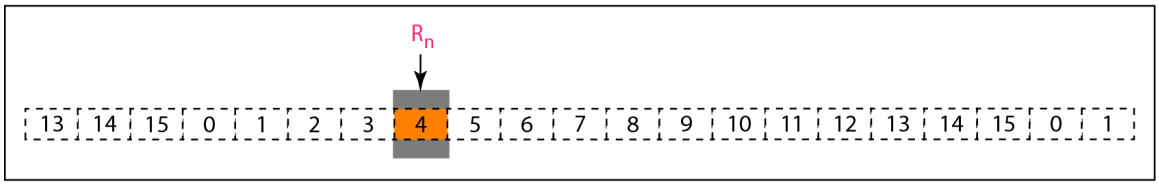
b. Send window after sliding

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.



a. Receive window

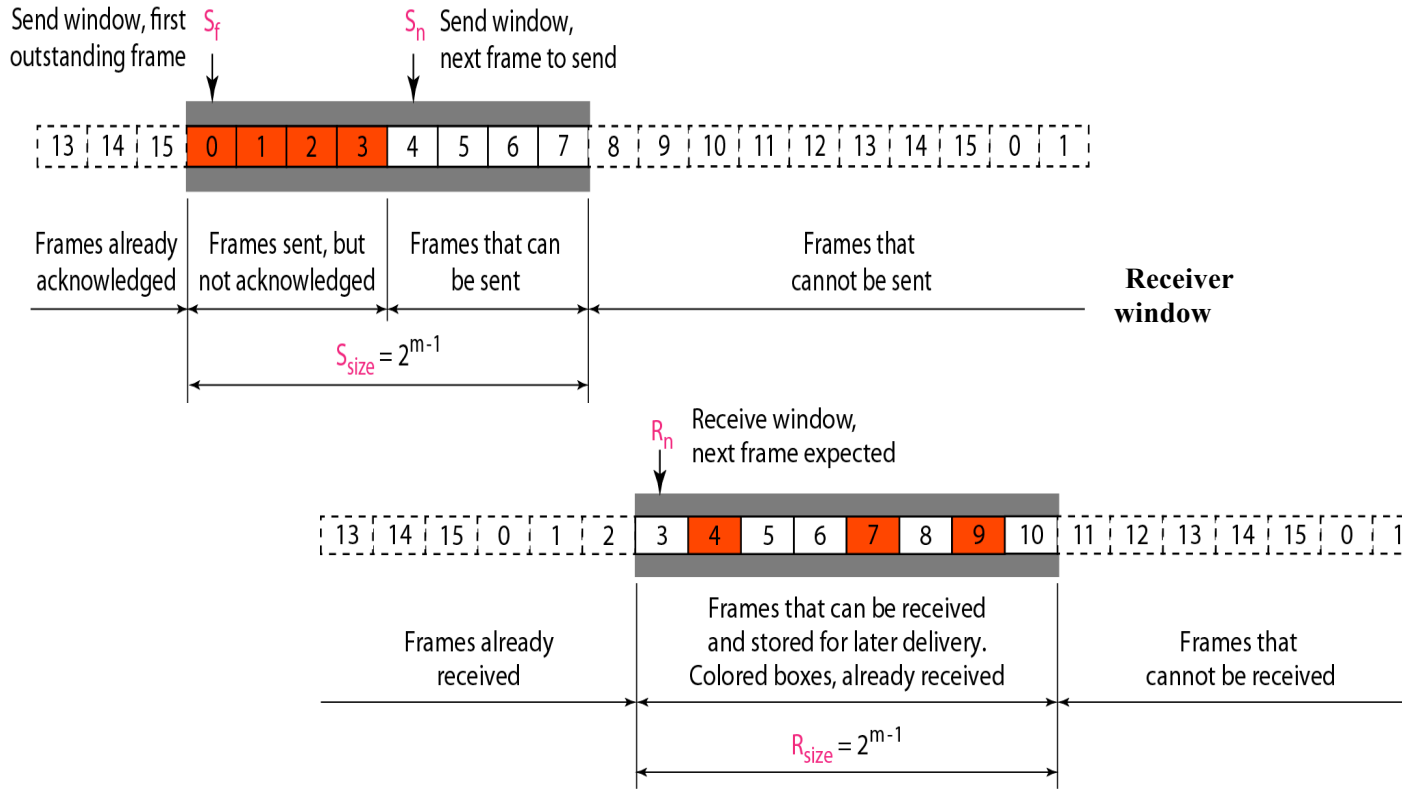


b. Window after sliding

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



- 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.

5. **Discuss in detail about the Byte- oriented Protocols (PPP), Bit-oriented Protocols (HDLC) and SONET.**

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

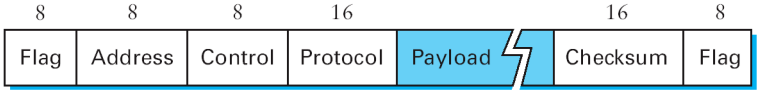
The BISYNC protocol illustrates the sentinel approach to framing; its frame format is

- 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



- 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

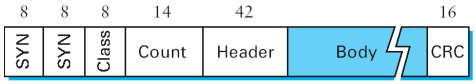


Fig: DDCMP frame format

- 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

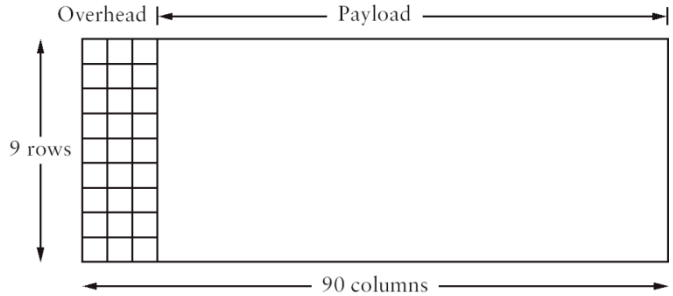
Fig: HDLC Frame Format

- 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.

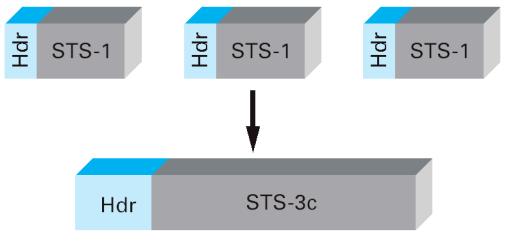
If it sees a 1 (i.e., the last eight bits it has looked at are 01111111), then there must have been an error and the whole frame is discarded.

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 fram frames, where the bytes from these frames are inter transmitted, then a byte from the second frame is
- 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 bit in overhead is used for this purpose.

6. **Discuss about Error Correction. (Nov/Dec 2012)**

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.

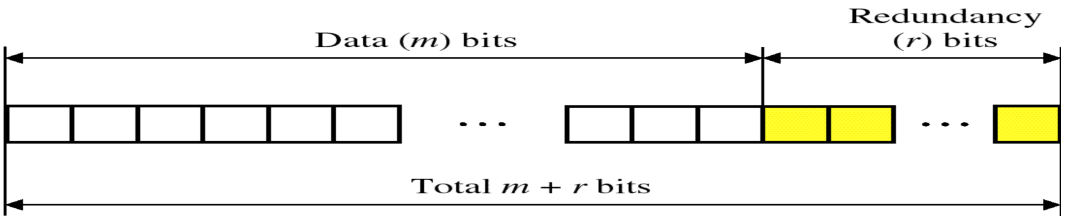
1) error
2) no error

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

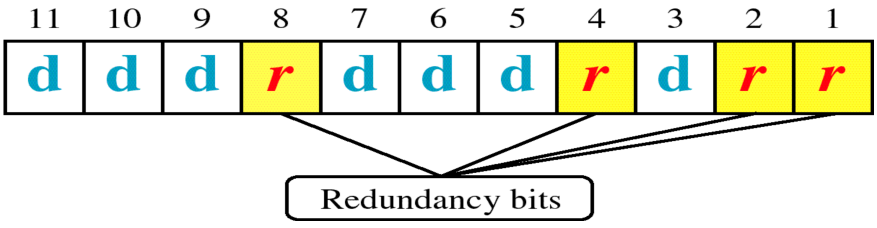
Hamming Code

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

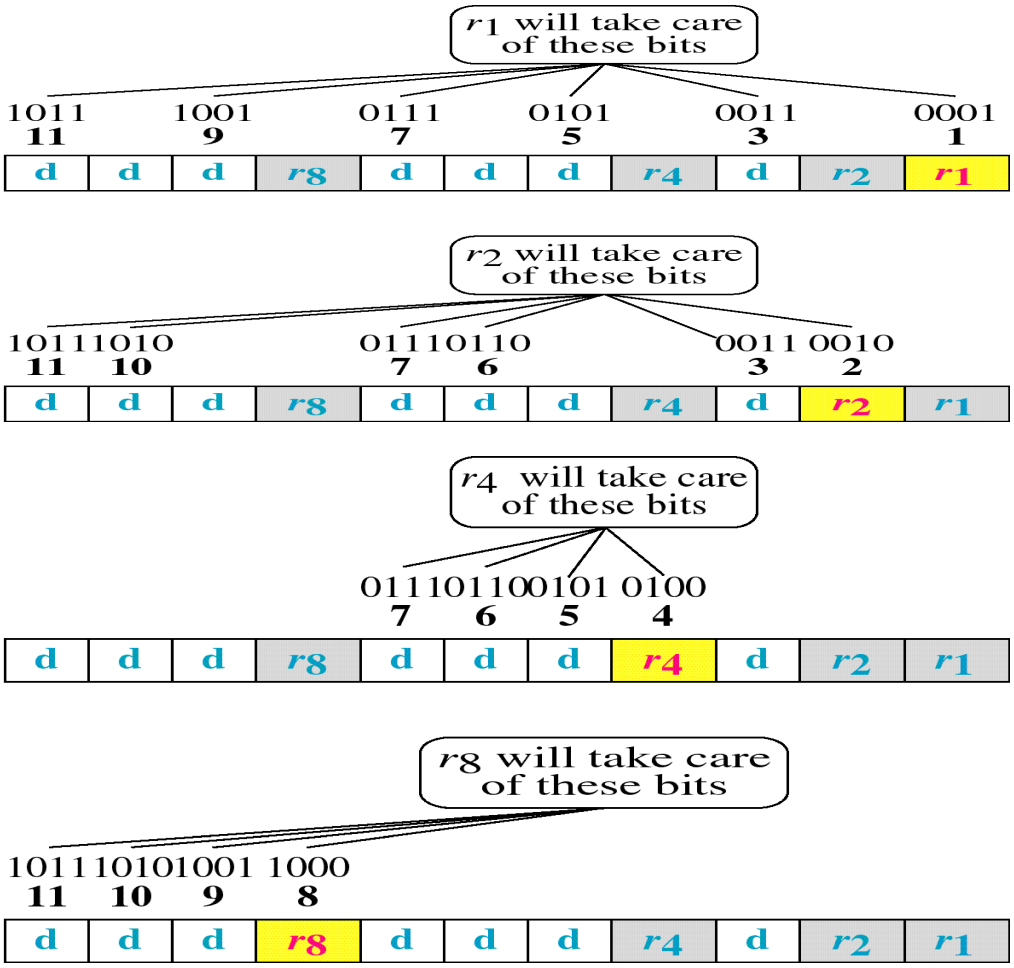


The combination used to calculate each of the four r values for a seven-bit data sequence are as follows

- 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

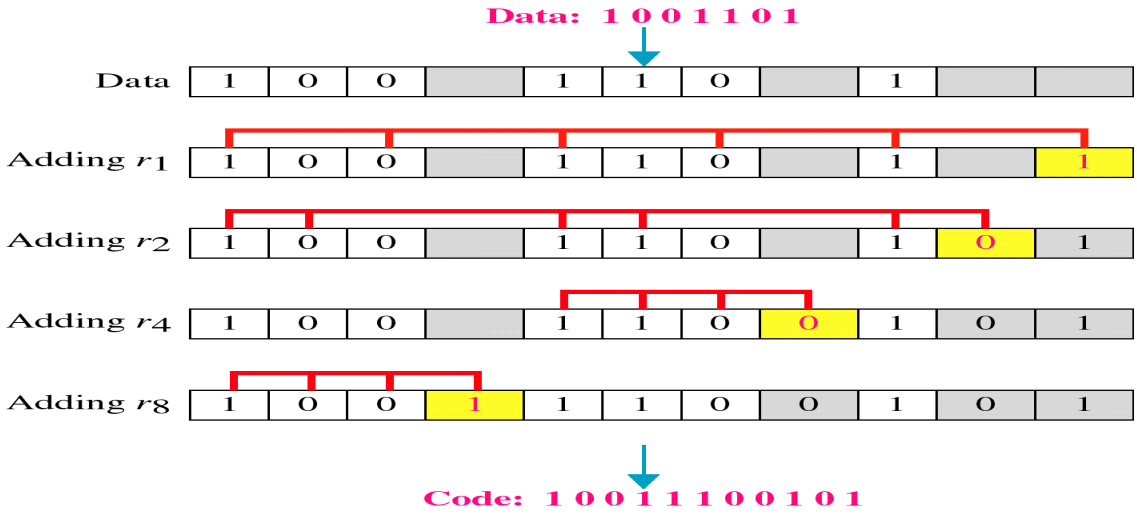


Calculating the r values

- 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.



7. **The message 11001001 is to be transmitted, using CRC error detection algorithm. Assuming the CRC polynomial to be x^3+1, determine the message that should be transmitted. If the second left most bit is corrupted, show that it is detected by the receiver. (May/June 2013)**
Suppose we want to transmit the message 11001001 and protect it from errors using the CRC polynomial $x^3 + 1$.

a) Use polynomial long division to determine the message that should be transmitted.
M(x) = 11001001
Because the CRC polynomial is of degree 3, adding 3-zeros at the end of M(x), we get T(x) = 11001001000
Let, $C(x) = x^3 + 1 = 1001$, which is the CRC polynomial. Then the polynomial long division is as follows:

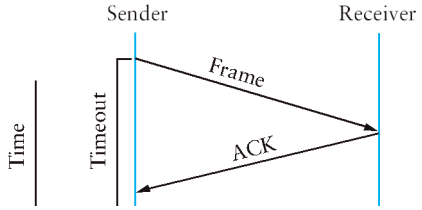
```
          1 1 0 1 0 0 1 1
      ----------------------------
1001) 1 1 0 0 1 0 0 1 0 0 0
        1 0 0 1
      -----------
          1 0 1 1
          1 0 0 1
        ----------
              1 0 0 0
              1 0 0 1
            ----------
                  1 1 0 0
                  1 0 0 1
                ----------
                      1 0 1 0
                      1 0 0 1
                    ----------
                      0 1 1
```

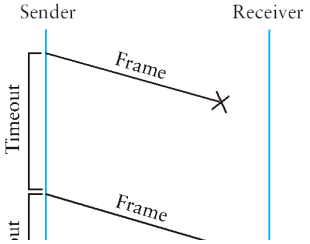
Message transmitted = 11001001**011**

b) Suppose the leftmost bit of the message is inverted due to noise on the transmission link. What is the result of the receiver's CRC calculation? How does the receiver that an error has occurred?
If the leftmost bit is inverted, the message will be
01001001011
Upon CRC calculation using the long division, the result will be **010.** Because **010**
000, the receiver knows that an error has occurred.

8. **Discuss the principle of stop and wait flow control algorithm. Draw time line diagrams and explain how loss of a frame and loss of an ACK are handled. What is the effect of delay-bandwidth product on link utilization? (May/June 2013)**
Stop and Wait Algorithm

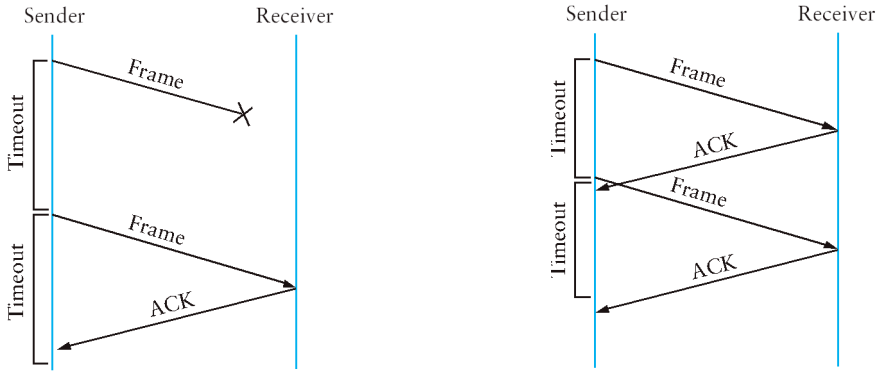
- After transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame.
- If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmit the original frame.





a) The ACK is received before the timer expires

b) The original frame is lost



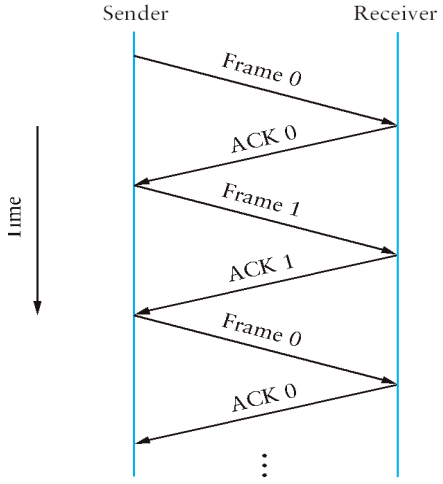
c) The ACK is lost

d) The timeout fires too soon

Fig: illustrates four different scenarios that result from this basic algorithm. The sending side is represented on the left, the receiving side is depicted on the right, and time flows from top to bottom.

- In Fig (a) ACK is received before the timer expires, (b) and (c) show the situation in which the original frame and the ACK, respectively, are lost, and (d) shows the situation in which the timeout fires too soon.

- Suppose the sender sends a frame and the receiver acknowledges it, but the acknowledgment is either lost or delayed in arriving. This situation is in (c) and (d). In both cases, the sender times out and retransmit the original frame, but the receiver will think that it is the next frame, since it correctly received and acknowledged the first frame.
- This makes the receiver to receive the duplicate copies. To avoid this two sequence numbers (0 and 1) must be used alternatively.



- The main drawback of the stop-and-wait algorithm is that it allows the sender have only one outstanding frame on the link at a time.

9. **Assume that a frame consists of 6 characters encoded in 7-bit ASCII. Attach a parity bit for every character to maintain even parity. Also attach a similar parity bit for each bit position across each**

of the bytes in the frame. Show that such a 2-dimensional parity scheme can detect all 1-bit, 2-bit and 3-bit errors and can correct a single bit error. (May/June 2013)

Error Correction

Error Correction can be handled in two ways:

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

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.

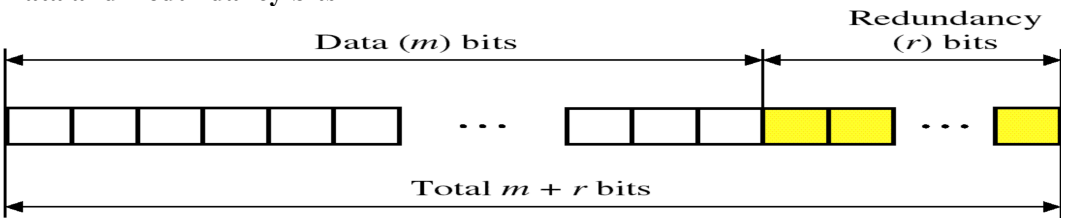
1) error
2) no error

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

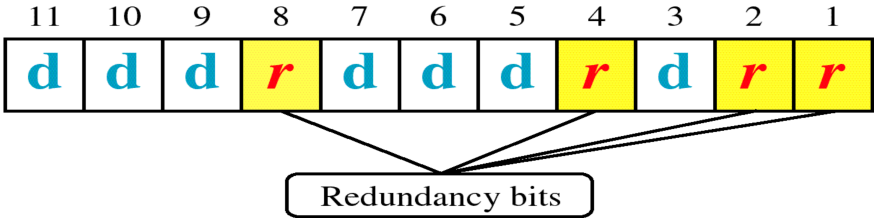
Hamming Code

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

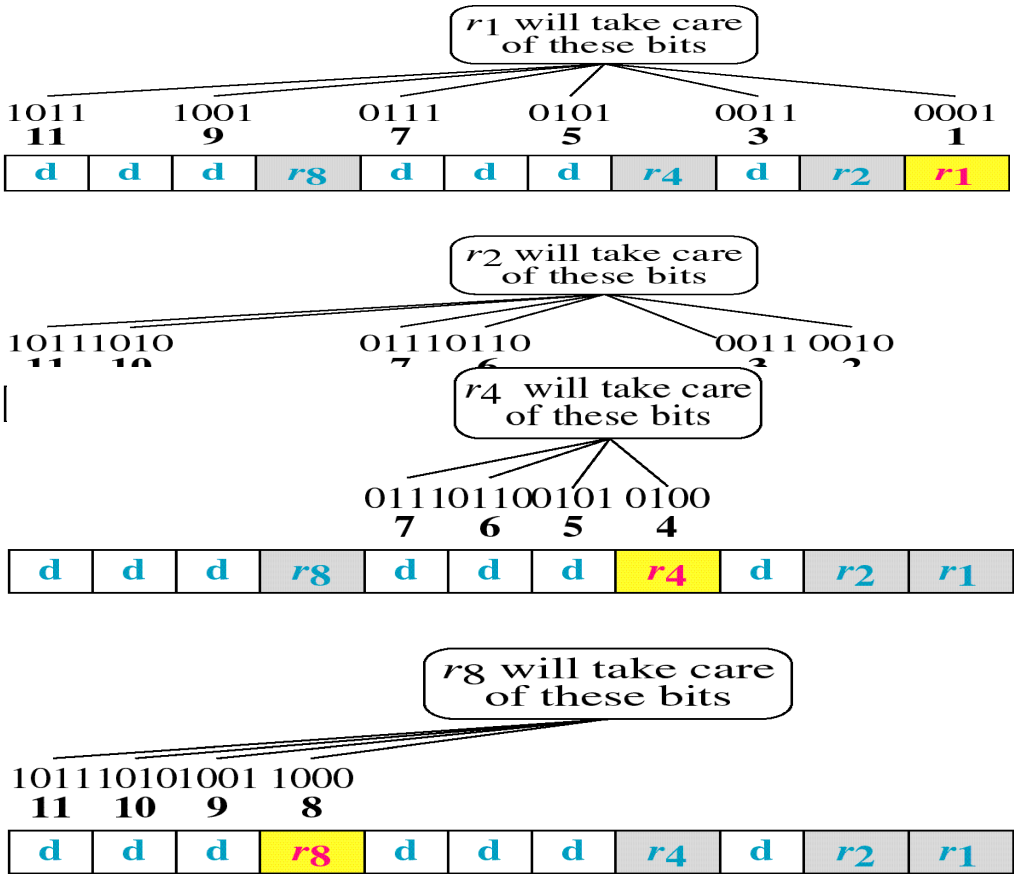


The combination used to calculate each of the four r values for a seven-bit data sequence are as follows

- 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

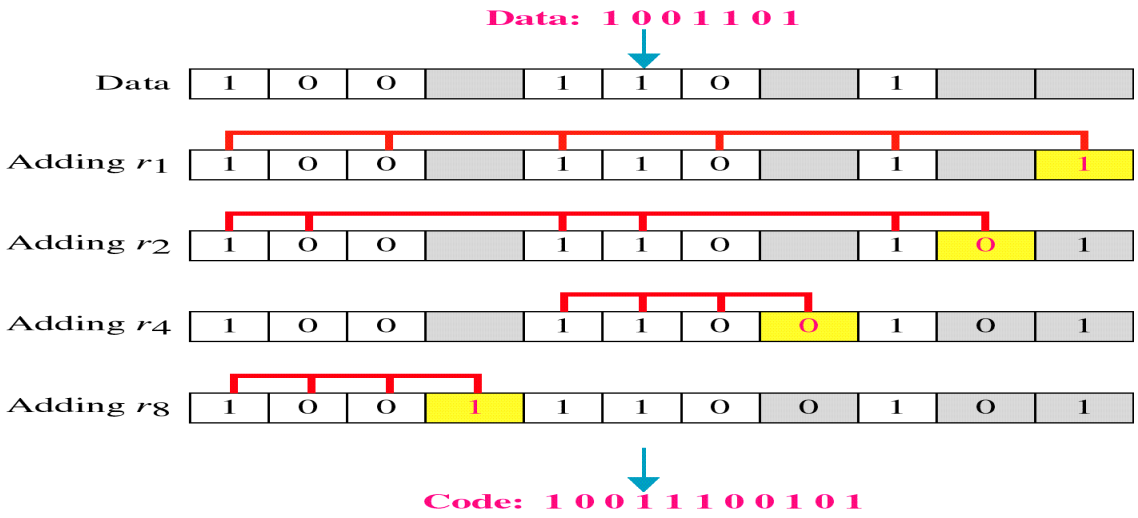


Calculating the r values

- 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.



10. **Suppose we want to transmit the message 11001001 and protect it from errors using the CRC polynomial x^3+1. Use polynomial long division to determine the message that should be transmitted. (Nov/Dec 2013)**

Use polynomial long division to determine the message that should be transmitted.

M(x) = 11001001

Because the CRC polynomial is of degree 3, adding 3-zeros at the end of M(x), we get T(x) = 11001001000

Let, $C(x) = x^3 + 1 = 1001$, which is the CRC polynomial. Then the polynomial long division is as follows:

```
          1 1 0 1 0 0 1 1
        ---------------------------
1001) 1 1 0 0 1 0 0 1 0 0 0
        1 0 0 1
        -----------
          1 0 1 1
          1 0 0 1
          ----------
            1 0 0 0
            1 0 0 1
            ----------
              1 1 0 0
              1 0 0 1
              ----------
                1 0 1 0
                1 0 0 1
                ----------
                  0 1 1
```

Message transmitted = 11001001**011**

11. **Given a remainder of 111, a data unit of 10110011 and a divisor of 1001, is there an error in the data unit. Justify your answer with necessary principles. (May/June 2014)**

If there are no errors, the receiver received T intact. The received frame is divided by P :

```
          1000000110
     ------------------
1011 ) 10110011111
       1011
       ----
        0000
        0000
        ----
         0000
         0000
         ----
          0001
          0000
          ----
           0011
           0000
           ----
            0111
            0000
            ----
             1111
             1011
             ----
              1001
              1011
              ----
               0101
               0000
               ----
                101
                ---
```

There is remainder, it is assumed that there have been errors.

12. **How frame order and flow control is achieved using the data link layer? (May/June 2014)**

Flow control is a technique that a transmitting entity does not conquer a receiving entity with data. Two fundamental mechanisms are acknowledgement and timeouts.

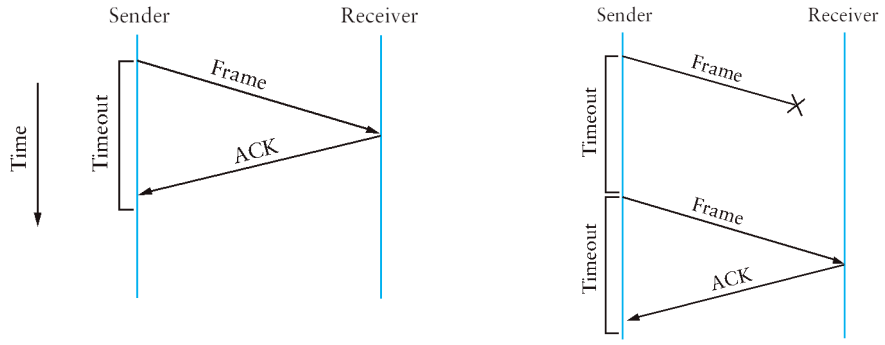
- After getting each frame the receiver will send ACK to sender.
- If the sender does not receive ACK up to reasonable amount of time then it retransmit the original frame waiting for reasonable amount of time is called timeout.

The two flow control mechanisms are

- Stop and wait Flow Control
- Sliding Window Flow Control

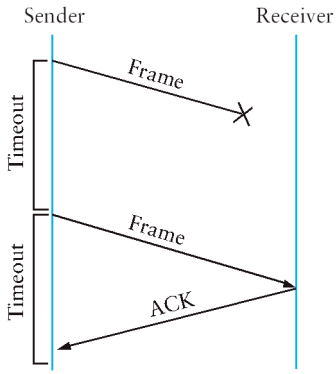
Stop and Wait Algorithm

- After transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame.
- If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmit the original frame.

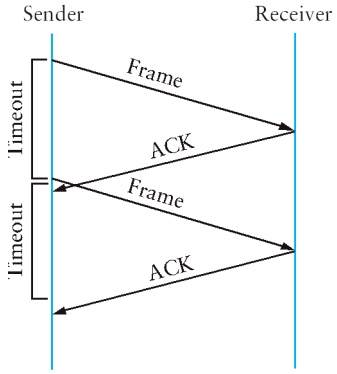


a) The ACK is received before the timer expires

b) The original frame is lost



c) The ACK is lost

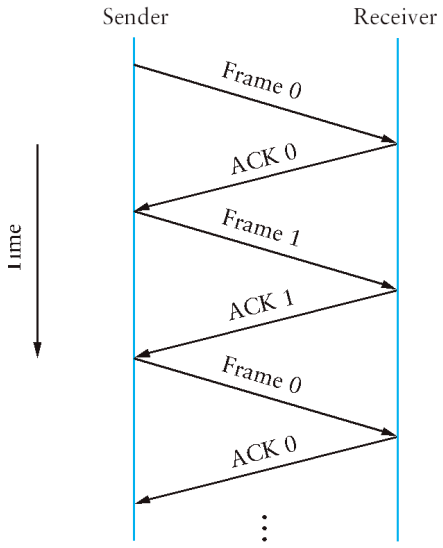


d) The timeout fires too soon

Fig: illustrates four different scenarios that result from this basic algorithm. The sending side is represented on the left, the receiving side is depicted on the right, and time flows from top to bottom.

- In Fig (a) ACK is received before the timer expires, (b) and (c) show the situation in which the original frame and the ACK, respectively, are lost, and (d) shows the situation in which the timeout fires too soon..
- Suppose the sender sends a frame and the receiver acknowledges it, but the acknowledgment is either lost or delayed in arriving.
- This situation is in (c) and (d). In both cases, the sender times out and retransmit the original frame, but the receiver will think that it is the next frame, since it correctly received and acknowledged the first frame.

- This makes the receiver to receive the duplicate copies. To avoid this two sequence numbers (0 and 1) must be used alternatively.



- The main drawback of the stop-and-wait algorithm is that it allows the sender have only one outstanding frame on the link at a time.

Sliding Window Algorithm

- 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.

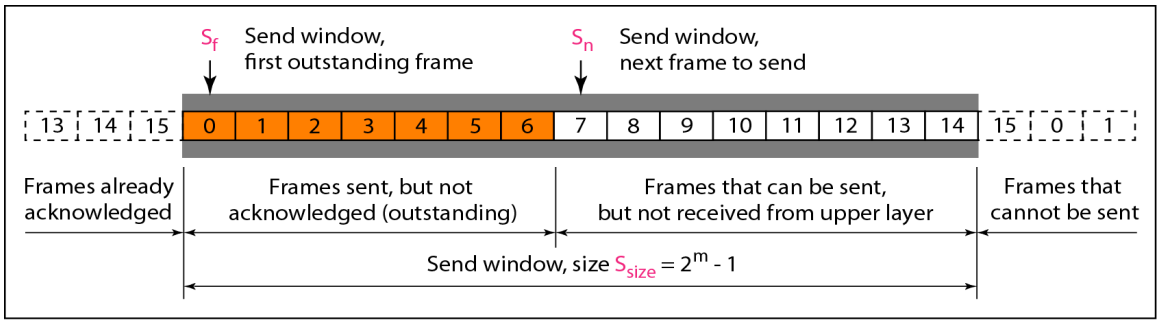
There are two methods to retransmit the lost frames

- GO-Back N
- Selective Repeat

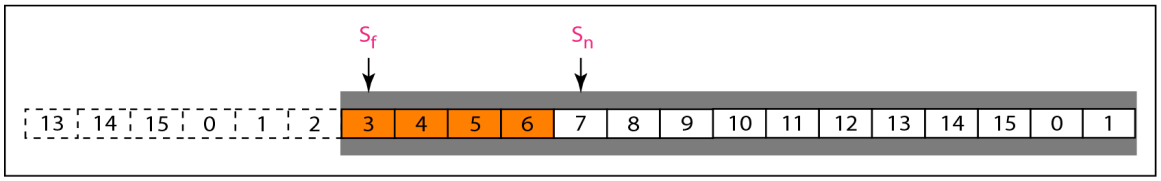
Go – Back N Method

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.



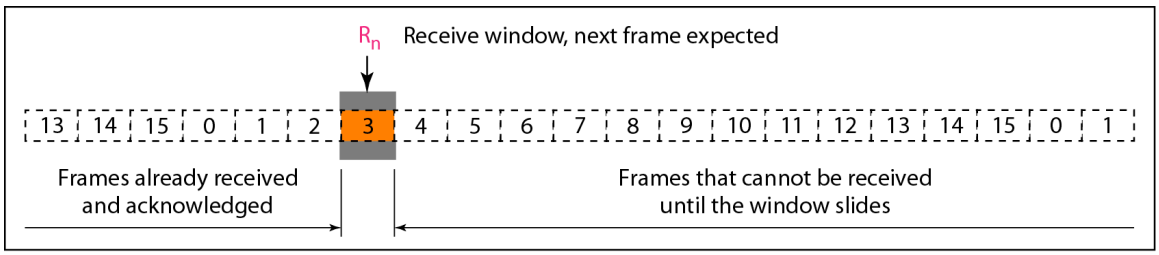
a. Send window before sliding



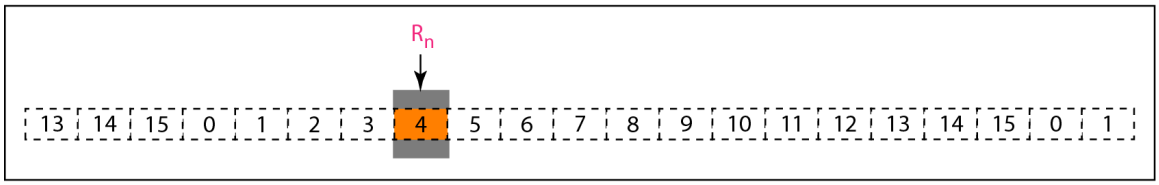
b. Send window after sliding

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.



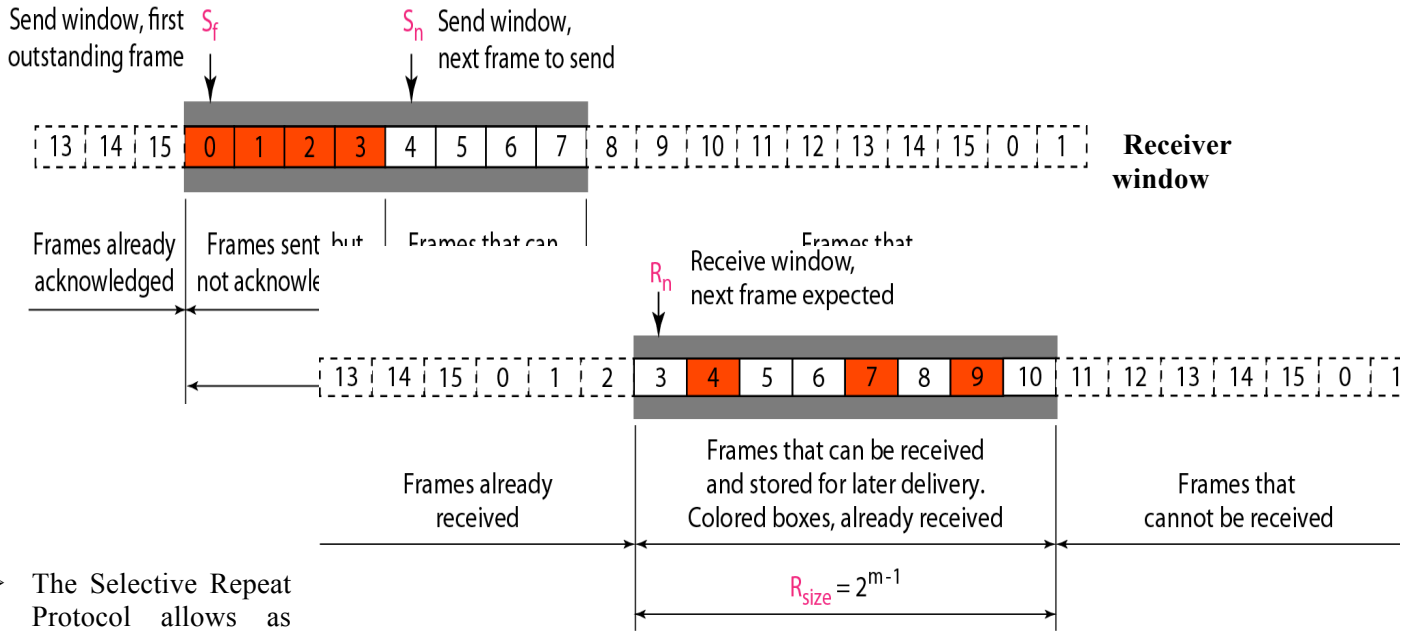
a. Receive window



b. 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



- 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.

UNIT- II

PART A

1. List the advantages of a centralized scheme.

It may afford greater control over access for priorities, overrides, and guaranteed capacity.
It enables the use of relatively simple access logic at each station.
It avoids problems of distributed coordination among peer entities.

2. Mention some of the physical properties of Ethernet. (Apr/May 2011)

The Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link. An Ethernet is like a bus that has multiple stations plugged into it.

3. What is CSMA/CD? (Nov/Dec 2011)

Carrier Sense Multiple Access with Collision Detection is one of the methods of medium access. It is used to sense whether a medium is busy before transmission. If the medium is busy, it refrains from transmitting the data or else proceeds with the transmission. Also has the ability to check whether a transmission has collided with another.

4. List the rules for CSMA/CD.

1. If the medium is idle, transmit; otherwise go to step 2.
2. If the medium is busy, continue to listen until the channel is idle, and then transmit immediately.
3. If a collision detected during transmission, transmit a brief jamming signal to all station to indicate collision has occurred and then cease transmission.
4. After transmitting a jamming signal, wait for some time, then transmit again.

5. When a transmitting station will insert a new token on the ring?

It will insert a new token when the station has completed transmission of its frame.
The leading edge of the transmitted frame has returned to the station.

6. What is Early Token Release (ETR)?

ETR allows a transmitting station to release a token as soon as it completes frame transmission, whether or not the frame header has returned to the station.

7. What is a bridge? (Nov/Dec 2011)

Bridge is a hardware networking device used to connect two LANs. A bridge operates at data link layer of the OSI layer. A bridge observes and forwards all frames that it receives. It does forwarding & filtering frames using LAN destination address. Bridges are used to connect LAN or WAN and works at data link layer level. Collision Probability is more.

8. What is the advantage of FDDI over a basic token ring? (Nov/Dec 2010)

FDDI	**Token Ring (IEEE 802.5)**
No priority and reservation bits.	It has priority scheme by using reservation bits.
No need of converting a token to start of data frame by inverting token bits because of high data rate.	It converts a token to data frame changing token frame.
A station that transmits data frames releases a new token as soon as it completes data.	A station that data transmissions after releasing back its own transmission, release the token.

9. Give the format of Ethernet address.

Preamble	Dest addr	Src addr	Type	Body	CRC
64	48	48	16		32

10. What is meant by the contention period of Ethernet? How many lines are required to connect n systems in Direct Mesh topology?

When several stations on an Ethernet have data to send, there are contention periods during which collisions happen and no data is successfully transmitted. n (n-1)/2 lines are required.

11. What does IEEE 10 Base 5 standard signify?

- 10 represents data rate 10 Mbps.
- 5 refers to segment length 5* 100 m that can run without repeaters
- Base represents Base band communication.

12. Define Repeater and Hub.

Repeaters and hubs are interconnecting devices.

Repeater: Repeaters extends the Ethernet segment and it repeats the signal. It does not amplify the signal.
Hub: A Hub has several point to point segments coming out. It is a multi way repeater. It broadcasts any signal through all outgoing lines.

13. What is meant by Exponential back of algorithm?

After first collision, each station waits either 0 or 1 slot time before trying again. If two stations collide and each one picks same random number 0/1. After second collision, each one picks 0, 1, 2 or 3 slot at random and waits. If collision occurs again, then next time the number of slots to wait is chosen at random from 0 to $[2^3 – 1]$. This algorithm is called binary exponential "back off algorithm".

14. Mention the different types of bridge. What are the limitations of bridges? (Nov/Dec 2013)

- Simple Bridge connects two LAN
- Multi port Bridge connect more than 2 LANs
- Transparent Bridge it learns on its own about connected LANs.

The limitations of bridges: Scalability and Heterogeneity.

15. What are the functions of Bridges? (Nov/Dec 2010)

- A bridge should have enough buffer space to store the frames until it is transmitted.
- It should be able to distinguish addresses of host on different LAN.
- It can contain information about other bridges.
- It should follow congestion control mechanisms to overcome congestion.
- It works at layer 1 and layer 2.

16. List out any four IEEE 802 standard with its name. (May/June 2012)

The IEEE 802 family of standards is maintained by the IEEE 802 LAN/MAN Standards Committee (LMSC). The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs. An individual Working Group provides the focus for each area.

17. Define Bridge and Switch. (May/June 2012)

Bridge: used to send the message from one LAN into another LAN.
Switch: used to send the data from one node into another node directly in the network.

18. What is packet switching? (Nov/Dec 2012)

In a packet-switched network, it's not necessary to dedicate transmission capacity along a path through the network. Rather, data are sent out in a sequence of small chunks, called packets. Packet switching is mainly used in terminal-to-computer and computer-to-computer communications.

19. Define Unicasting, Broadcasting and Multicasting. (Nov/Dec 2011)

- Unicasting: Transmitting data from a single sender to a single receiver.
- Broadcasting: Transmitting data from a single source to all the other nodes in the network
- Multicasting: Transmitting data from a single source to a group of destination nodes.

20. List the difference between Packet Switching and Circuit Switching. (Apr/May 2011, Nov/Dec 2011, May/June 2014)

Issue	**Packet switching**	**Circuit Switching**
Circuit setup	Not Required	Required
Transmission path	No Transmission path	Dedicated path
Delay	Packet transmission delay	Call setup delay
Addressing	Each packet contains the full source and destination address	Only data is sent
Bandwidth	Dynamic Bandwidth	Fixed Bandwidth
Routing	Each packet is routed independently	Entire data is sent through the same path
Congestion control	Difficult	Easy if enough buffers can be located in advance for each VC set up
Complexity	In the transport layer	In the network layer
Suited for	Connection-oriented and connectionless service	Connection-oriented service

21. What is IP address?

An Internet Address is made of four bytes (32 bits) that define a host's connection to a network. There are currently 5 different field lengths patterns, each define a class of addresses. These are designed to cover the needs of different types of organizations, class A, B, C, D, E.

Class	Netid	Hostid

22. How many network addresses and host addresses are supported by class A, class B networks?

- Class A: Number of networks = 127
  Number of hosts = 2^{24} -1
- Class B: Number of networks = 2^{14} -1
  Number of hosts = $2^{16} - 1 = 65,535$

23. Differentiate Physical Address and Logical Address.

Physical Address	**Logical Address**
It is implemented by data link layer	It is implemented by n/w layer
It contains 48 bits	It contains 32 bits
It is a local addressing system	It is an universal address system
Another name is MAC address	Another name is IP address
It is flat in nature	Hierarchical in nature
Does not give any clue for routing	Its structure gives clue for routing

24. What does a router do when it receives a packet with a destination address that it does not have an entry for, in its routing table?

Default Router: If IP Software is not able to find the destination, from routing table then it sends the datagram to default router. It is useful when a site has small set of local address connected to it and connected to the rest of the Internet.

25. Define ARP.

Associates an IP address with physical address. It is used to find the physical address of the node when its Internet address is known. Any time a host/router needs to find the physical address of another host on its network, it formats an ARP query packet that includes the IP address and broadcasts it. All hosts in the network process the ARP packet but only the required station sends back physical address.

26. Define RARP.

Allows a host to discover its internet address when it knows only its physical address (a diskless computer). The host wishing to retrieve its internet address broadcasts an RARP query packet that contains its physical address to every host on its physical network. A server on the network recognizes the RARP packet and returns the host's internet address.

27. What do you mean by ICMP?

ICMP is an error reporting mechanism. It does not specify the action to be taken for each possible error. The source must relate the error to an individual application program and take other actions to correct the problem.

28. List out the functions of IP.

IP services are unreliable, best-effort, connectionless packet delivery system.

- Unreliable – delivery is not guaranteed, Connectionless – each pocket is treated independent from others, Best-effort delivery – it makes an earnest attempt to deliver packets. It defines basic unit of data transfer through TCP/IP.
- IP s/w performs routing function and finds a path from source to destination.
- IP includes a set of rules that embody the idea of unreliable packet delivery.

29. To whom ICMP reports error message?

ICMP allows routers to send error messages to other router or hosts. ICMP is an error reporting mechanism. It does not specify the action to be taken for each possible error. It is informing the source that the error has occurred and the source has to take actions to rectify the errors.

30. What is subnetting? (Nov/Dec 2011)

The whole network can't be managed by single server, so that the entire network divided into small network in order to manage the network easily.

31. What is the access method used by wireless LAN? (May/June 2014)

The access method used by wireless LAN is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

32. What is the network address in a class A subnet with the IP address of one of the hosts as 25.34.12.56 and mask 255.255.0.0? (May/June 2014)

IP Address	-	25.34.12.56
Mask	-	255.255.0.0
Network Address	-	25.34.0.0

PART-B

1. Explain how bridges run a distributed spanning tree algorithm. (April/May 2011)

***Spanning tree* algorithm:**

- developed by Radia Perlman at Digital Equipment Corporation
- It is a protocol used by a set of bridges to agree upon a spanning tree for a particular extended LAN.
- It is a dynamic algorithm which bridges are always prepared to reconfigure themselves into a new spanning tree should some bridge fail.

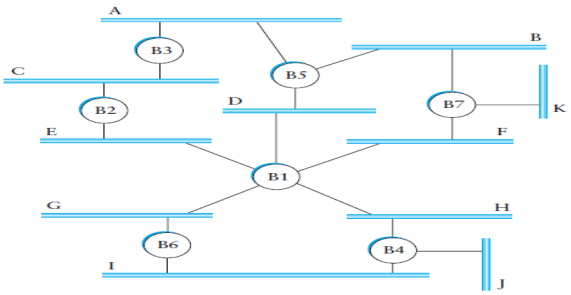


Fig. Extended LAN with loops

Problem:

1. The network is managed by more than one administrator

- It is possible that no single person knows the entire configuration of the network, meaning that a bridge that closes a loop might be added without anyone knowing.

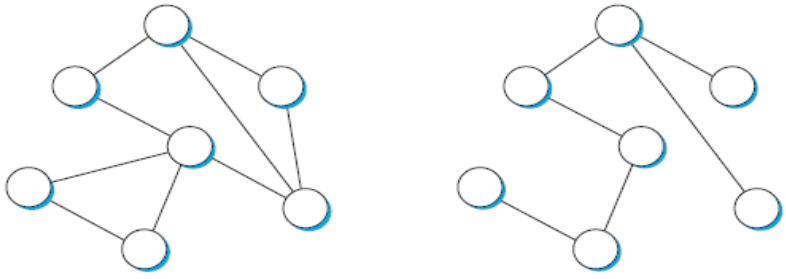
2. Loops are built into the network on purpose - to provide redundancy in case of failure.

Bridges must be able to correctly handle loops. This problem is addressed by having the bridges run a distributed *spanning tree* algorithm.

Extended LAN as being represented by a graph that possibly has loops (cycles), then a spanning tree is sub graph of this graph that covers (spans) all the vertices, but contains no cycles.

That is, a spanning tree keeps all of the vertices of the original graph, but throws out some of the edges.

Example of (a) a cyclic graph; (b) a spanning tree.



(a) (b)

- Each bridge has a unique identifier; ie B1, B2, B3, and so on.
- First elects the bridge with the smallest id as the root of the spanning tree;

Procedure:

- The root bridge always forwards frames out over all of its ports.
- Each bridge computes the shortest path to the root and notes which of its ports is on this path. This port is also selected as the bridge's preferred path to the root.

- Finally, all the bridges connected to a given LAN elect a single *designated* bridge that will be responsible for forwarding frames toward the root bridge.
- If two or more bridges are equally close to the root, then the bridges' identifiers are used to break ties; the smallest id wins.

Information of new configuration messages

- The bridges have to exchange configuration messages with each other and then decide whether or not they are the root or a designated bridge based on these messages.
- It identifies a root with a smaller id or
- It identifies a root with an equal id but with a shorter distance or
- The root id and distance are equal, but the sending bridge has a smaller id.
- If the new message is better than the currently recorded information, the bridge discards the old information and saves the new information
- It first adds 1 to the distance-to-root field since the bridge is one hop farther away from the root than the bridge that sent the message.

2. Discuss in detail about the Ethernet. (April/May 2012)

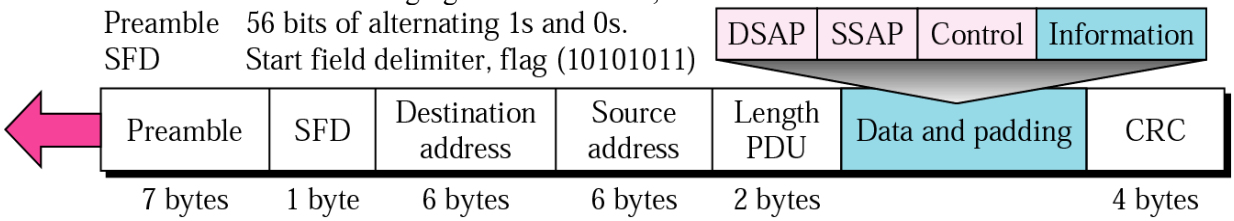
The Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link. An Ethernet is like a bus that has multiple stations plugged into it. The "carrier sense" in CSMA/CD means that all the nodes can distinguish between an idle and a busy link, and "collision 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.

Ethernet and a 1000-Mbps version called Gigabit Ethernet. The rest of this section focuses on10-Mbps Ethernet, since it is typically used in multiple-access mode and we are interested in how multiple hosts share a single link. Both 100-Mbps and 1000-Mbps Ethernets are designed to be used in full-duplex and point-to-point configurations.

Ethernet Frame Format

- Consists of seven fields
- No mechanism for acknowledging received frames; considered an unreliable medium

Preamble 56 bits of alternating 1s and 0s.
SFD Start field delimiter, flag (10101011)



- Preamble – seven bytes of alternating 0s and 1s to notify receiver of incoming frame and to provide synchronization
- Start frame delimiter (SFD) – one byte signaling the beginning of the frame
- Destination address (DA) – six bytes containing the physical address of the next destination; if packet must reach another LAN, this field contains the physical address of the router; upon reaching the target network, field then contains the physical address of the destination device
- Source address (SA) – six byte field containing physical address of last station to forward packet, sending station or most recent router
- Length/type – two bytes indicating number of bytes in coming PDU; if fixed length, can indicate type
- Data – 46 to 1500 bytes
- CRC – CRC-32 error detection information

Ethernet Addressing

- Each station on the network must have a unique physical address
- Provided by a six-byte physical address encoded on the network interface card (NIC)
- Normally written in hexadecimal notation

06-01-02-01-2C-4B

Categories of traditional Ethernet

- Baseband – digital signals using Manchester encoding
  - 10Base5, 10Base2, 10-Base-T, 10Base-FL
  - First number indicates data rate in Mbps.
  - Last number indicates maximum cable length or type

- Broadband – analog signals using digital/analog conversion (differential PSK)
  - Only specification: 10Broad36

3. Explain the functioning of wireless LAN in detail. (Nov2010/Dec 2012, Nov/Dec 2014)

A **wireless local area network** (**WLAN**) is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and still be connected to the network, and can provide a connection to the wider Internet. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name.

i. Stations

ii. All components that can connect into a wireless medium in a network are referred to as stations. All stations are equipped with wireless network interface controllers (WNICs). Wireless stations fall into one of two categories: wireless access points, and clients. Access points (APs), normally wireless routers, are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with. Wireless clients can be mobile devices such as laptops, personal digital assistants, IP phones and other smartphones, or fixed devices such as desktops and workstations that are equipped with a wireless network interface.

iii. Basic service set

iv. The basic service set (BSS) is a set of all stations that can communicate with each other. Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.

v. There are two types of BSS: Independent BSS (also referred to as IBSS), and infrastructure BSS. An independent BSS (IBSS) is an ad hoc network that contains no access points, which means they cannot connect to any other basic service set.

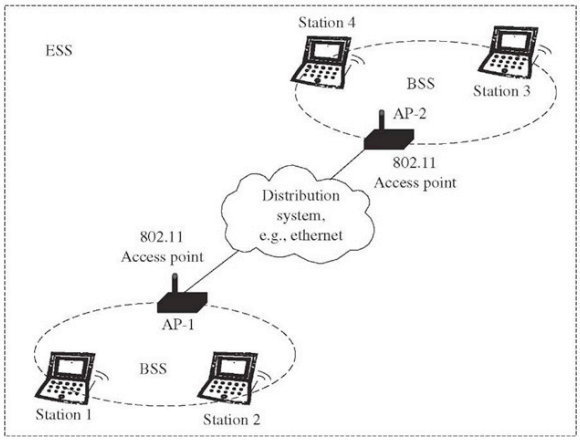
vi. Extended service set

vii. An extended service set (ESS) is a set of connected BSSs. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string.

viii. Distribution system

ix. A distribution system (DS) connects access points in an extended service set. The concept of a DS can be used to increase network coverage through roaming between cells.

x. DS can be wired or wireless. Current wireless distribution systems are mostly based on WDS or MESH protocols, though other systems are in use.



4.Explain CSMA in detail. (April/May 2011)

CSMA: listen before transmit.

- A network station wishing to transmit will first check the cable plant to ensure that no other station is currently transmitting (*CARRIER SENSE*).
- The communications medium is one cable, therefore, it does allow multiple stations access to it with all being able to transmit and receive on the same cable (*MULTIPLE ACCESS*).
- Error detection is implemented throughout the use of a station "listening" while it is transmitting its data.
  - A jam signal is transmitted to network by the transmitting stations that detected the collision, to ensure that all stations know of the collision. All stations will "back off" for a random time.
  - Detection and retransmission is accomplished in microseconds.
  - Two or more stations transmitting causes a collision (*COLLISION DETECTION*)

If channel sensed idle: transmit entire frame

If channel sensed busy, defer transmission collisions *can* still occur.

Propagation delay means two nodes may not hear each other's transmission.

Before transmit sense the medium whether the medium is busy or idle. Whether the medium is idle, the sender ready to transmit the data , medium is busy the sender waits for certain time then sense the medium always. Suppose multiple user sense the medium is idle, all are trying to send the data, in this case collision is happened. To avoid this we are using relay and also using some the control frames like RTS and CTS.

5.Explain in detail about IP v4 addressing.

A very important concept in IP addressing is the network address. When an organization is given a block of addresses, the organization is free to allocate the addresses to the devices that need to be connected to the Internet. The first address in the class, however, is normally (not always) treated as a special address. The first address is called the network address and defines the organization network. It defines the organization itself to the rest of the world. The first address is the one that is used by routers to direct the message sent to the organization from the outside.

- There are 5 classes. Class A,B,C are unicast addressing. Class D is a multicast addressing. Class E is reserved for future use. Class A: 0.0.0.1 to 127.255.255.255, Class B: 128.0.0.0 to 191.255.255.255, Class C: 192.0.0.0 to 223.255.255.255,
- Class D: 224.0.0.0 to 239.0.0.0 and Class E: 240.0.0.0 to 255. 255.255.255.
- Class A. eg: 127.9.19.89,Class B eg: 120.19.17.15,class C eg: 198.16.12.34,Class D eg:230.16.12.54
- Special IP address is constructed by replacing the normal network ID or host ID (or both) in an IP address with one or two special patterns. The two patterns are:
- **Class A**

0 Netid	Host ID

- **Class B**

10 Net id	Host ID

- **Class C**

110	net id	Host id

- **Class D**

1110	Multicast address

- **Class E**

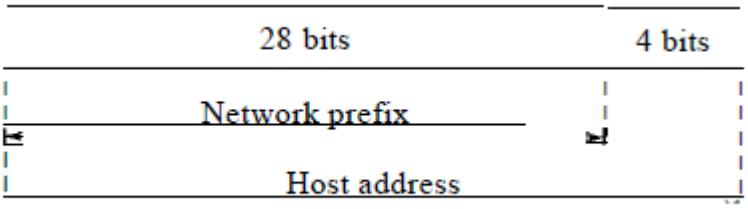
1111	reserved for future use

Hierarchy

IP addresses, like other addresses or identifiers we encounter these days, have levels of hierarchy.

Two-Level Hierarchy: No Subnetting

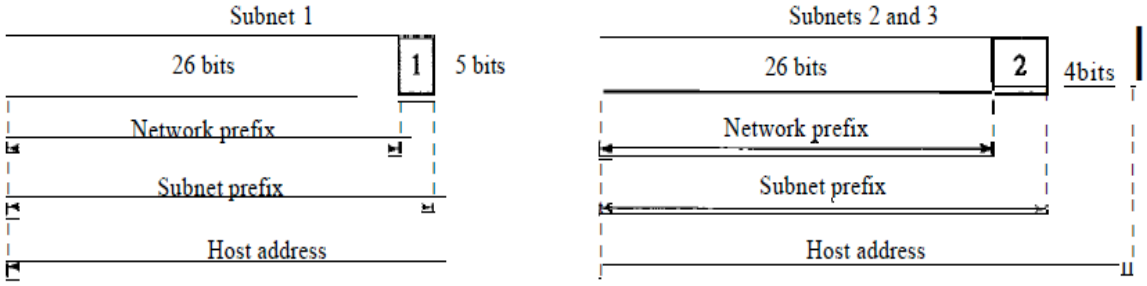
An IP address can define only two levels of hierarchy when not subnetted. The *n* leftmost bits of the address *x.y.z.tJn* define the network (organization network); the 32 – *n* rightmost bits define the particular host (computer or router) to the network. The two common terms are prefix and suffix. The part of the address that defines the network is called the prefix; the part that defines the host is called the suffix. Figure shows the hierarchical structure of an IPv4 address.



Each address in the block can be considered as a two-level hierarchical structure: the leftmost *n* bits (prefix) define the network; the rightmost 32 - *n* bits define the host.

Three-Levels ofHierarchy: Subnetting

An organization that is granted a large block of addresses may want to create clusters of networks (called subnets) and divide the addresses between the different subnets. The rest of the world still sees the organization as one entity; however, internally there are several subnets. All messages are sent to the router address that connects the organization to the rest of the Internet; the router routes the message to the appropriate subnets. The organization, however, needs to create small subblocks of addresses, each assigned to specific subnets. The organization has its own mask; each subnet must also have its own.



6. Explain in detail about DHCP.

Automated configuration methods use a protocol known as the Dynamic Host Configuration Protocol (DHCP). DHCP relies on the existence of a DHCP server that is responsible for providing configuration information to hosts. Internetwork contains a network part and a host part, and the network part must be the same for all hosts on the same network. Thus, it is not possible for the IP address to be configured once into a host when it is manufactured, since that would imply that the manufacturer knew which hosts were going to end up on which networks, and it would mean that a host, once connected to one network, could never move to another. For this reason, IP addresses need to be reconfigurable.

- IP addresses are some other pieces of information a host needs to have before it can start sending packets.

- The most notable of these is the address of a default router—the place to which it can send packets whose destination address is not on the same network as the sending host.
- Most host operating systems provide a way for a system administrator, or even a user, to manually configure the IP information needed by a host.

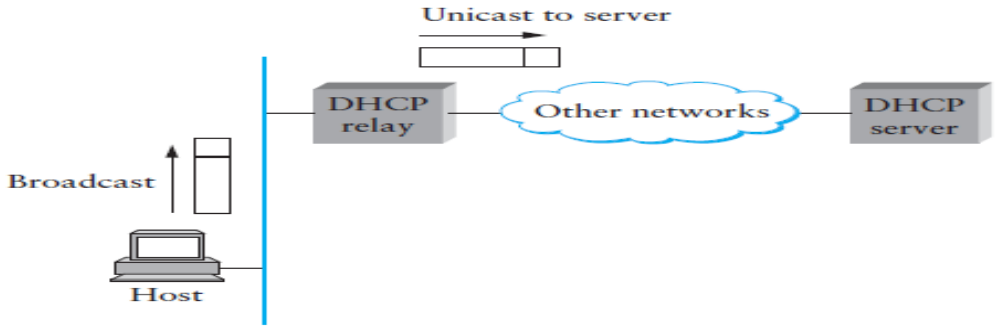
Drawbacks of manual configuration:

- It is a lot of work to configure all the hosts in a large network directly, especially when you consider that such hosts are not reachable over a network until they are configured.
- The configuration process is very error-prone, since it is necessary to ensure that every host gets the correct network number and that no two hosts receive the same IP address

DHCP Server:

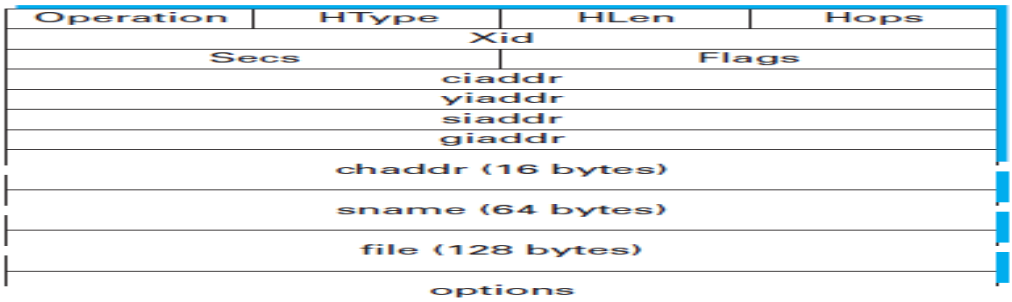
- can function just as a centralized repository for host configuration information.
- saves the network administrators from having to walk around to every host in the company with a list of addresses and network map in hand and configuring each host manually.
- the configuration information for each host could be stored in the DHCP server.
- administrator would still pick the address that each host is to receive; he would just store that in the server
- DHCP saves the network administrator from even having to assign addresses to individual hosts.
- DHCP server maintains a pool of available addresses that it hands out to hosts on demand.
- The goal of DHCP is to minimize the amount of manual configuration required for a host to function, it would rather defeat the purpose if each host had to be configured with the address of a DHCP server.

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



DHCP packet format:

- The message is actually sent using a protocol called UDP (the User Datagram Protocol) that runs over IP.
- It does in this context is to provide a demultiplexing key that says, “This is a DHCP packet.”
- DHCP is derived from an earlier protocol called BOOTP, and some of the packet fields are thus not strictly relevant to host configuration.
- When trying to obtain configuration information, the client puts its hardware address (e.g., its Ethernet address) in the chaddr field.
- The DHCP server replies by filling in the yiaddr (“your” IP address) field and sending it to the client.
- Other information such as the default router to be used by this client can be included in the options field.
- DHCP illustrates an important aspect of scaling: the scaling of network management.
- While discussions of scaling often focus on keeping the state in network devices from growing too rapidly, it is important to pay attention to growth of network management complexity.
- By allowing network managers to configure a range of IP addresses per network rather than one IP address per host, DHCP improves the manageability of a network.



7. Describe about IPv6. (April/May 2012)

The motivation for a new version of IP is the same as the motivation for the techniques to deal with scaling problems caused by the Internet's massive growth. In particular, it is virtually impossible to achieve 100% address utilization efficiency, so the address space will be exhausted well before the four-billionth host is connected to the Internet.

The effort to define a new version of IP was known as IP Next Generation, or IPng. As the work progressed, an official IP version number was assigned, so IPng is now known as IPv6.

In addition to the need to accommodate scalable routing and addressing, some of the other wish list items for IPng were:

- support for real-time services
- security support
- auto configuration
- enhanced routing functionality, including support for mobile hosts

ADDRESSES AND ROUTING

IPv6 address consists of 16 bytes with 128-bits long while 32 bits in IPv4.

IPv4 addresses 4 billion nodes in 100% efficiency while, IPv6 addresses 3.4*10^38

The IPv6 address space is predicted to provide over 1500 addresses per square foot of the earth's surface.

ADDRESS SPACE ALLOCATION

IPv6 addresses do not have classes, but the address space is still subdivided in various ways based on the leading bits.

The leading bits specify different uses of the IPv6 address.

ASSIGNMENT OF PREFIXES

Prefix	Use
0000 0000	Reserved
0000 0001	Unassigned
1111 1110 10	Link local use addresses
1111 1110 11	Site local use addresses
1111 1111	Multicast addresses

From the above list, multicast addresses are easily distinguishable; they start with a byte of all 1s.

Link local use addresses is to enable a host to construct an address that will work on the network to which it is connected (internally unique, not globally).

Site local use addresses allow valid addresses to be constructed on a site (private corporate network) that is not connected to the Internet. Also it is not globally unique.

ADDRESS NOTATION

The standard representation is x:x:x:x:x:x:x:x, where each "x" is a hexadecimal representation of a 16-bit piece of the address. For eg., 47CD:1234:4422:ACO2:0022:1234:A456:0124.

Special notations are used to describe some special types of IPv6 addresses.

For example, an address with a large number of contiguous 0s can be written more compactly by omitting all the 0 fields. i.e., 47CD:0000:0000:0000:0000:0000:A456:0124 could be written as

47CD::A456:0124. Also such form of shorthand can only be used for one set of contiguous 0s in an address.

- Since there are two types of IPv6 addresses that contain an embedded IPv4 address, these have their own special notation that makes extraction of the IPv4 address easier.
- For example, the "IPv4- mapped IPv6 address" of a host whose IPv4 address was 128.96.33.81 could be written as ::FFFF:128.96.33.81.

i.e., the last 32 bits are written in IPv4 notation, rather than as a pair of hexadecimal no.s separated by a colon. Also the double colon at front indicates leading 0s.

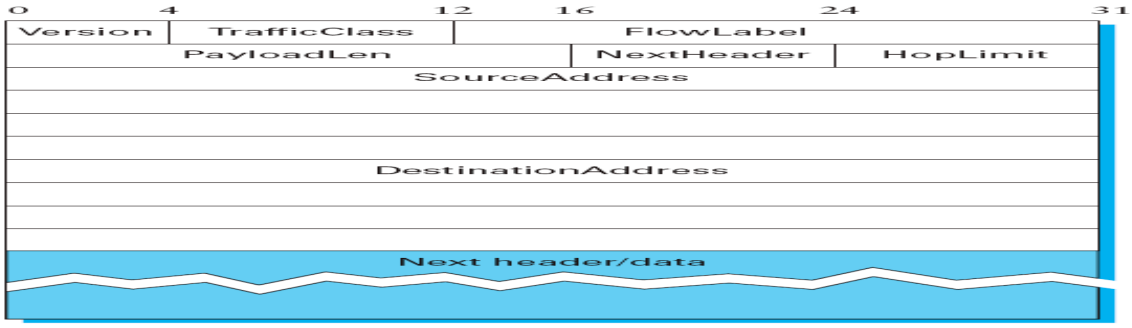
GLOBAL UNICAST ADDRESS

- **Type-ID**: Defines addr as provider based address.
- **Registry ID**: Indicates the agency that has registered the address. Registry centers available are INTERNIC with code 11000 for North America, RIPNIC with code 01000 for Europe and APNIC with code 10100 for Asia Pacific.
- **Provider-ID**: Identifies provider for Internet access. 16 bit length is recommended.
- **Subscriber-ID**: when an organization subscribes to Internet thru a provider, it is assigned a subscriber ID. Again 24 bit length is recommended.
- **Subnet-ID**: Each subscriber can have many sub n/ws with different IDs. Subnet ID defines a specific n/w under the territory of subscriber. A 32 bit length is recommended.

Interface-ID: Identifies node connected to the subnet. A length of 48 bits is recommended to be compatible with link level Ethernet address

PACKET FORMAT: It has two types of formats: 1) IPv6 packet header
2) IPv6 fragmentation extension header.

- **Version**: Defines version no. of IP.
- **Traffic Class**: Defines priority of packet with respect to traffic congestion.
- **Flow Label**: Designed to provide spl. Handling for a particular flow of data.
- **Payload Length**: Defines length of IP datagram excluding base header.
- **Next Header**: Defines the header that follows base header. It replaces both the IP options and Protocol field of IPv4. If options are required, they are carried out in one or more spl. headers following IPv6 header, and this is indicated by the value of Next Header field. If there are no spl. headers, the Next Header field contains demux key identifying the higher level protocol running over IP.
- **Hop Limit**: Serves the same purpose as TTL of IPv4.
- **Source Addr & Dest Addr** : A 16 byte IP addr identifying original source and destination of datagram.

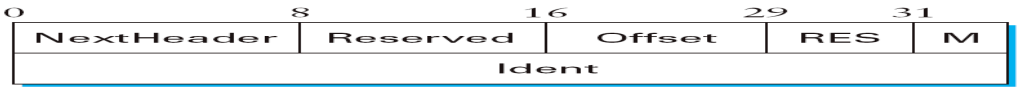


Headers in IPv6

- IPv6 treats options as Extension Headers that must, if present, appear in a specific order.
- A router finds out easily whether the options present are relevant to it or not by looking at the Next Header field, leading to better option processing.

- Options in IPv6 can be of arbitrary lengths. Each option has an extension header whose type is identified by the value of Next Header.
- Each extension header contains a Next Header to identify the header following it. Last extension header will be followed by a transport layer header.
- Therefore Next Header serves dual purpose by identifying the type of extension header to follow as well as in the last extension, it serves as demux key identifying higher layer protocol running over IPv6.

An Example Extension Header:



- This header provides functionality similar to the fragmentation fields in the IPv4 header.
- If we assume that this is the only ext. header present, then the Next Header field of IPv6 would contain value 44 (used to represent fragment header) .
- The Next Header field of fragmentation header itself contains a Next Header, describing the header that follows it.
- Again if we assume no hdrs to follow, then this might be TCP hdr, which results in Next Header containing the value 6. If an authentication header is to follow, then Next Header contains value 51.

AUTO CONFIGURATION

- One goal of IPv6, therefore, is to provide support for auto configuration, sometimes referred to as "plug-and-play" operation.
- New form of auto configuration called *stateless* auto configuration is used (similar to DHCP in IPv4), which does not require a server.
- We can subdivide the auto configuration problem into two parts:

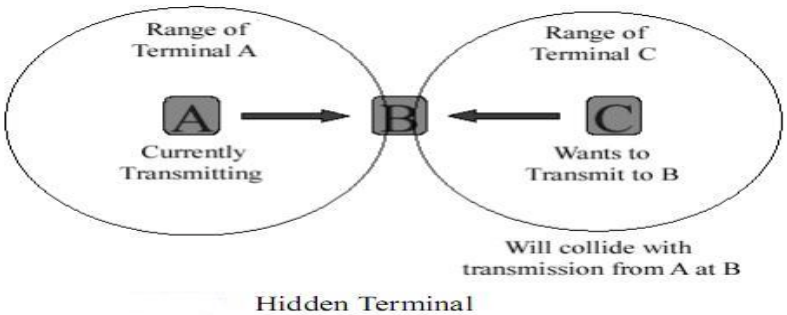
1) Obtain an interface ID (Ethernet addr-48 bits) that is unique on the link to which the host is attached. This could be converted to link local use addr by appropriate prefix to make up 128 bits. 2) Obtain the correct address prefix for this subnet, which could be obtained from the router attached on same link. This prefix should contain enough space to attach an appropriate link level address.

ADVANCED ROUTING CAPABILITIES

- Another of IPv6's extension headers is the routing header containing a list of IPv6 addresses that represent nodes or topological areas that the packet should visit on its way to destination.
- A host could say that it wants some packets to go thru a provider providing high reliability or cheaper cost or offering best security.
- To provide the ability to specify topological entities rather than individual nodes, IPv6 defines an ***anycast*** address.
- An anycast address is assigned to a set of i/fs. Packets sent to that address will go to the "nearest" of those i/fs, with nearest being determined by the routing protocols.
- The anycast address and the routing header are also expected to be used to provide enhanced routing support to mobile hosts.

8.Explain how hidden node and exposed node problem is solved in IEEE 802.11 (Nov/Dec 2013)

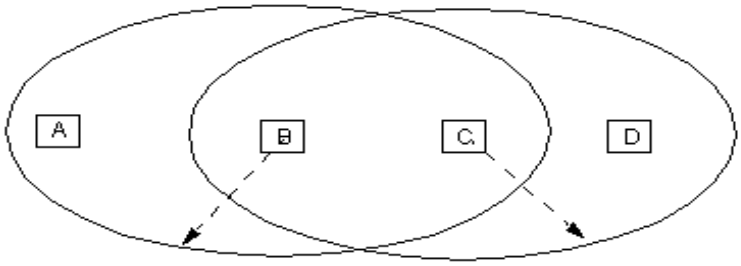
IEEE 802.11: Collision avoidance - Hidden terminal problem



Hidden Terminal

Exposed **Terminal:**

B transmits to A, C wants to transmit to D. C needlessly assumes a full channel.



Multiple Access with Collision Avoidance (MACA)

- **Before every data transmission**
  - Sender sends a Request to Send (RTS) frame containing the length of the transmission
  - Receiver responds with a Clear to Send (CTS) frame, echoing back the length of frame to sender.
  - Any node nearer to receiver also receives CTS, becomes aware that it cannot transmit for a period specified inside CTS.
  - Also any node seeing RTS and not CTS is not close to receiver, hence free to transmit.
  - Sender sends data
  - Receiver sends an ACK; After seeing this ACK only other nodes can send data
- If more than 1 node transmits RTS simultaneously, collision will occur. Nodes realize about collision if they don't get a CTS back.
- Nodes follow random back off time procedure before retransmitting

Distribution system

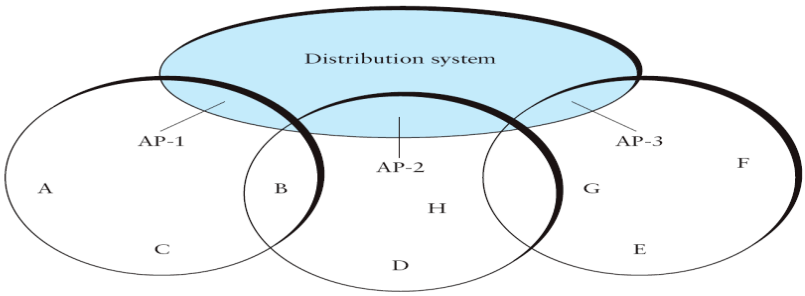


Figure 2.39 Access points connected to a distribution network.

- All the nodes are not alike, some roam (Laptops), some are connected to a wired n/w (base stations).
- Such base stations are called Access points, which are connected to each other by a Distribution System, which in turn could be any wired n/w (Ethernet, Token Ring etc.).
- Even though each node can communicate directly with other node, if they are within reach of each other, they associate themselves with an Access point. For e.g., if node A wishes to communicate with node E,A first sends a frame to its AP (AP-1), which forwards the frame across the Distribution system to AP-3, which finally forwards the frame to node E.

The technique for selecting an AP is called *scanning* and involves the following four steps:

1. The node sends a Probe frame.
2. All APs within reach reply with a Probe Response frame.
3. The node selects one of the access points and sends that AP an Association Request frame.
4. The AP replies with an Association Response frame.

- Scanning is done by a node if it joins the n/w and also if it is unhappy with its current AP.

- This might happen when the signal reaching from its current AP is weak, since the node has moved away from it.
- Whenever a node acquires a new AP, the new AP informs such migration to its old AP thru the Distribution system.
- Node migration is depicted in the fig below.

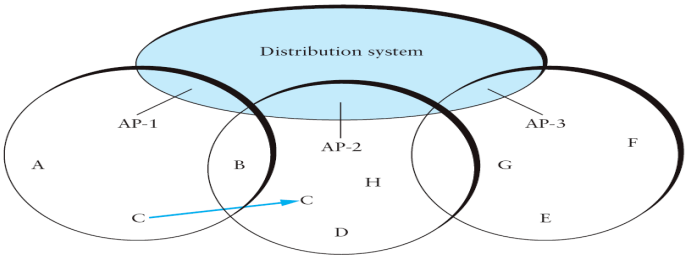


Figure 2.40 Node mobility.

Scanning could be of 2 types.

- **Active scanning**, the one initiated by node itself, if it sends probes continuously, actively searching for an AP.
- APs also periodically send a **Beacon frame**, advertising their own capabilities like transmission rates supported by them. Such type of scanning is referred as **passive scanning**. Any node on receiving such Beacon frame can send a **Associate Request** and join with any specific AP.
  - There are 4 addresses present in 802.11 frame whose interpretations depend on ToDs and FromDs bits present in Frame Control field.
  - If frame is forwarded across Distribution system, the original sender might change to the recent transmitting node i.e., the node which forwards finally to the ultimate destination.
  - When a node sends frame directly to another, both DS bits are 0, ADDR1 identifies target node, ADDR2 identifies source node.ADDR3 & 4 are not applicable.

9. **Describe the CSMA/CD protocol and comment on its performance for medium access. (May/June2014)**

CSMA/CD protocol can be considered as a refinement over the CSMA scheme. It has evolved to overcome one glaring inefficiency of CSMA. In CSMA scheme, when two
packets collide the channel remains unutilized for the entire duration of transmission time of both the packets. If the propagation time is small (which is usually the case) compared to the packet transmission time, wasted channel capacity can be considerable. This wastage of channel capacity can be reduced if the nodes continue to monitor the channel while transmitting a packet and immediately cease transmission when collision is detected. This refined scheme is known as Carrier Sensed Multiple Access with Collision Detection (CSMA/CD) or Listen-While-Talk.On top of the CSMA, the following rules are added to convert it into CSMA/CD:

(i) If a collision is detected during transmission of a packet, the node immediately ceases transmission and it transmits jamming signal for a brief duration to ensure that all stations know that collision has occurred. \

(ii) After transmitting the jamming signal, the node waits for a random amount of time and then transmission is resumed. The random delay ensures that the nodes, which were involved in the collision are not likely to have a collision at the time of retransmissions. To achieve stability in the back off scheme, a technique known as binary exponential back off is used. A node will attempt to transmit repeatedly in the face of repeated collisions, but after each collision, the mean value of the random delay is doubled. After 15 retries (excluding the original try), the unlucky packet is discarded and the node reports an error. A flowchart representing the binary exponential back off algorithm is given

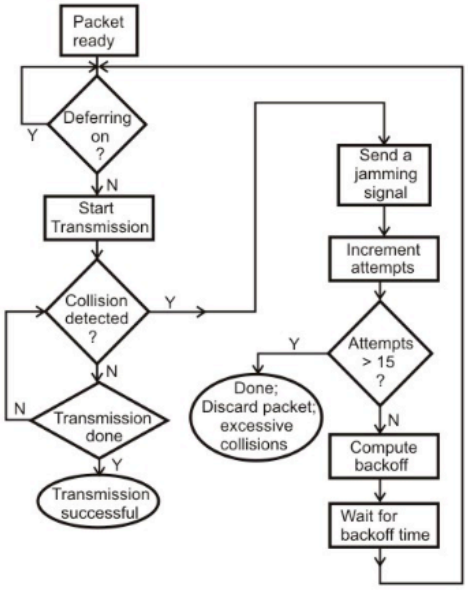


Figure 5.2.11 Binary exponential back off algorithm used in CSMA/CD

Performance Comparisons:

The throughput of the three contention based schemes with respect to the offered load is given in Fig 5.2.12. The figure shows that pure ALHOA gives a maximum throughput of only 18 percent and is suitable only for very low offered load. The slotted ALHOA gives a modest improvement over pure ALHOA with a maximum throughput of 36 percent. Non persistent CSMA gives a better throughput than 1-persistent CSMA because of smaller probability of collision for the retransmitted packets. The non-persistent CSMA/CD provides a high throughput and can tolerate a very heavy offered load. Figure 5.2.13 provides a plot of the offered load versus throughput for the value of a = 0.01

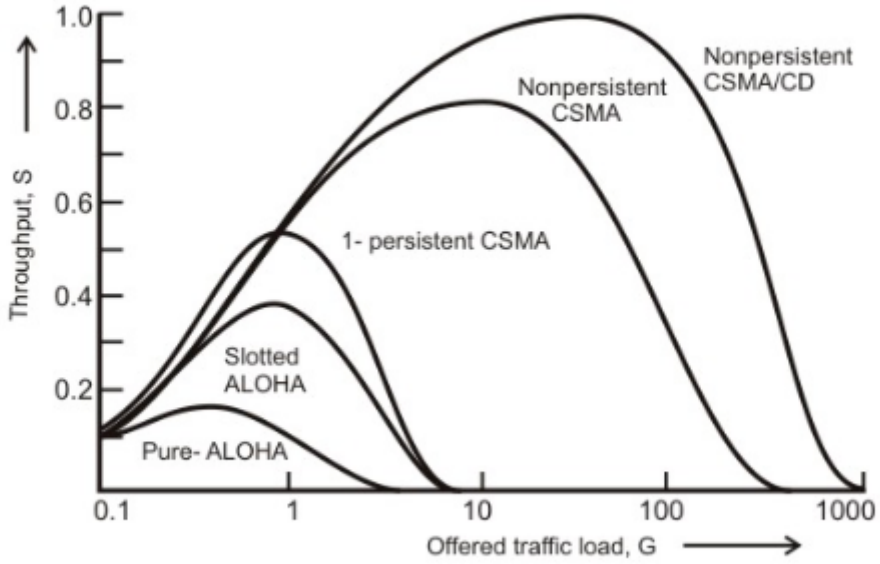


Figure 5.2.13 A plot of the offered load versus throughput for the value of a = 0.01

Performance Comparison between CSMA/CD and Token ring:

It has been observed that smaller the mean packet length, the higher the maximum mean throughput rate for token passing compared to that of CSMA/CD. The token ring is also least sensitive to workload and propagation effects compared to CSMS/CD protocol. The CSMA/CD has the shortest delay under light load conditions, but is most sensitive to variations to load, particularly when the load is heavy. In

CSMA/CD, the delay is not deterministic and a packet may be dropped after fifteen collisions based on binary exponential back off algorithm. As a consequence, CSMA/CD is not suitable for real-time traffic.

10. Write short notes on: (May/June2014)

i) FDDI

FDDI Basics

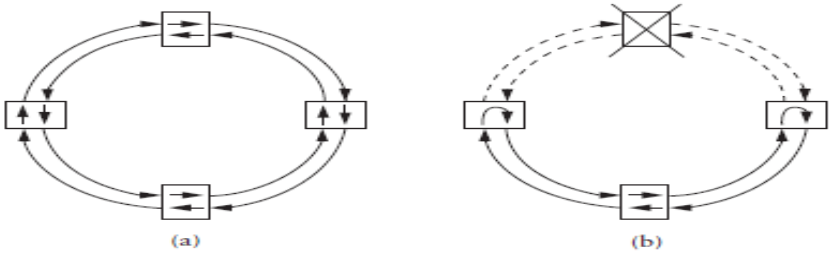
- Fiber Distributed Data Interface (FDDI) high-speed LAN which uses fiber optics, dual ring topology and the token passing access method.

FDDI is frequently used as a backbone technology and to connect high-speed computers in a LAN.

FDDI has four specifications:

1. Media Access Control - defines how the medium is accessed
2. Physical Layer Protocol—defines data encoding/decoding procedures
3. Physical Layer Medium—defines the characteristics of the transmission medium
4. Station Management—defines the FDDI station configuration

- Physical properties: This runs on fiber, not copper. The copper variant is called CDDI.
- It has dual ring. The 2 independent rings send the data in opposite directions. The second ring is not used during normal operation but instead comes into play only if the primary ring fails.
- FDDI network is able to tolerate a single break in the cable or the failure of one station.



- Instead of designating one node as a monitor, all the nodes participate equally in maintaining the FDDI ring.
- FDDI uses 4B/5B encoding instead of Manchester.
- FDDI allows nodes to attach to the network by means of a single cable. Such nodes are called *single attachment stations* (SAS); their dual-connected counterparts are called, not surprisingly, *dual attachment stations* (DAS). A concentrator is used to attach several SASs to the dual ring.

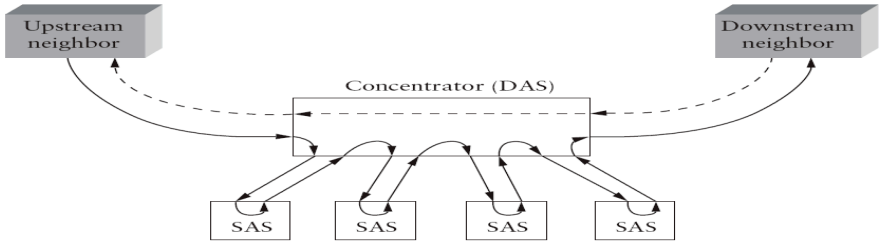


Figure 2.35 SASs connected to a concentrator.

- When a SAS fails, the concentrator detects this and uses an optical bypass to isolate failed SAS, thereby keeping the ring connected.
- Like 802.5, each n/w adaptor holds some no. of bits between its i/p and o/p interfaces. But here the size of buffer varies from station to station, with a minimum of 9 bits to a maximum of 80 bits.
- A station may start to transmit before its buffer becomes full and buffer size of each station determines the total time taken by token to pass around the ring.
- A single FDDI n/w can contain a maximum of 500 hosts with a distance of 2Km between 2 stations. Overall the n/w is limited to 200Km, resulting to a total distance of 100Km, because of the dual nature of the ring.

Timed – Token Algorithm

- THT is the Token Holding Time for each station. TTRT (Timed – Token Rotating Time) is the average time taken by all stations to complete one rotation. TTRT value is accepted and agreed by all stations.
- Each node measures the successive arrivals of token which is named as that node's measured TRT.
- If measured TRT > agreed TTRT, it implies the token is late and node does not transmit any data. If TRT < TTRT, it implies token is early and token stays at node for the calculated time difference. During this time, node transmits its data.
- There are 2 types of data held by a node – synchronous and asynchronous. Synchronous data are real time info and should not be delayed. Asynchronous data are of less priority and could be delayed.
- During each node's hold of token, it transmits the synchronous data first and if THT still remains positive, then an asynchronous data could be sent. If THT becomes 0 after sending synchronous data, asynchronous data is not sent.
- Generally whenever a node receives token it sends its synchronous data regardless of token being early / late.

  During worst case, i.e., when only synchronous / asynchronous data is present in any station, then measured TRT could be as much as 2 x TTRT.

  If a station has already used up one TTRT's worth of time for its single rotation in sending its synchronous data, it cannot send continuously asynchronous data. Therefore it is possible to have a single rotation to consume 2 x TTRT but it cannot have back to back rotations each consuming 2 x TTRT time.
- If the difference in time between TRT and TTRT is very less such that an entire frame cannot be sent, it still goes ahead in sending its full frame. This is because the measured TRT is actually bounded by TTRT plus the time it takes to send a full FDDI frame.

Token Maintenance

All nodes monitor the token. Timer is set to 2.5ms between which either a token or data frame should be seen by each station.

If not, timer expires and any station can send a claim token containing its TRT. If any station finds that TRT higher than its own, then it can overwrite a lower TRT value.

In case of tie, station with a higher address wins.

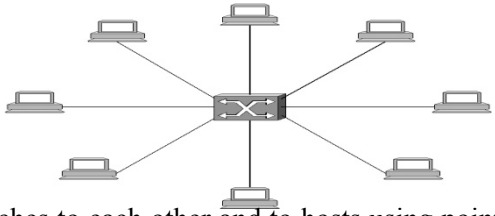
In this way an agreed upon TTRT value is fixed.1

Figure 2.36 FDDI frame format.

ii) Bridges and Switches

A switch is a mechanism that allows us to interconnect links to form a larger network. A switch is a multi-input, multi-output device, which transfers packets from an input to one or more outputs. Thus, a switch adds the star topology (see Figure.1) to the point-to-point link, bus (Ethernet), and ring (802.5 and FDDI) topologies. A star topology has several attractive properties:

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. Fig. A switch provides a star topology.



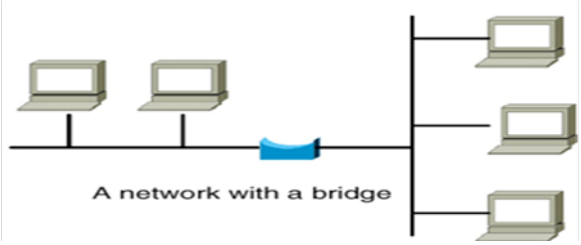
We can connect switches to each other and to hosts using point-to-point links, which typically means that we can build networks of large geographic scope.

Adding a new host to the network by connecting it to a switch does not necessarily mean that the hosts already connected will get worse performance from the network.

A packet switch is a device with several inputs and outputs leading to and from the hosts that the switch interconnects. The core job of a switch is to take packets that arrive on an input and forward (or switch) them to the right output so that they will reach their appropriate destination. There are a variety of ways that the switch can determine the "right" output for a packet, which can be broadly categorized as connectionless and connection-oriented approaches.

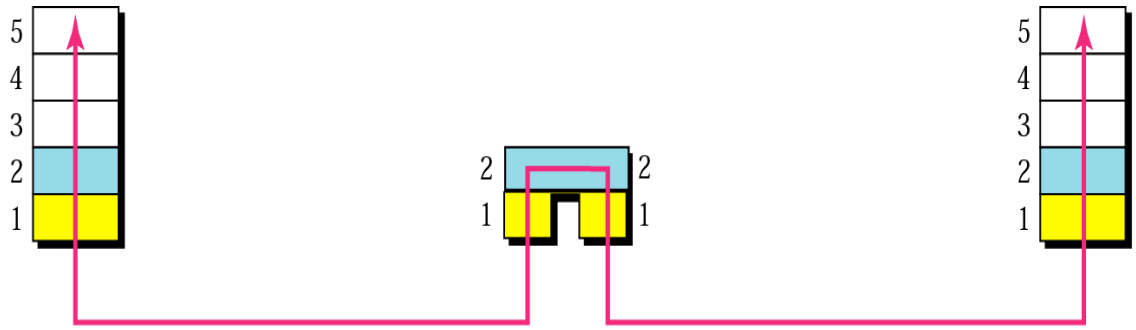
Bridges:

- LAN may need to cover more distance than the media can handle effectively
- When the bridge receives a frame on port1 that is addressed by host A the bridge would not forward the frame out on port2.
- Bridges uses connectionless model.
- Bridge decides on which output to send a frame by looking up address in the table.
- Bridges are used to logically separate network segments within the same network.
- They operate at the OSI data link layer (Layer 2) and are independent of higher-layer protocols.
- The function of the bridge is to make intelligent decisions about whether or not to pass signals on to the next segment of a network.
- When a bridge receives a frame on the network, the destination MAC address is looked up in the bridge table to determine whether to filter, flood, or copy the frame onto another segment
- Broadcast Packets are forwarded
- Multi input device and multi output device.
- Operate in both physical and data link layers.
- Ethernet segment can carry 10Mbps of total traffic.
- Ethernet bridge can carry 10n Mbps where n is the input and output ports of the bridge.
- Used to divide a network into smaller segments.
- May relay frames between separate LANs.
- Keeps traffic from each segment separate; useful for controlling congestion and provides isolation, as well as security.
- Checks address of frame and only forwards to segment to which address belongs.



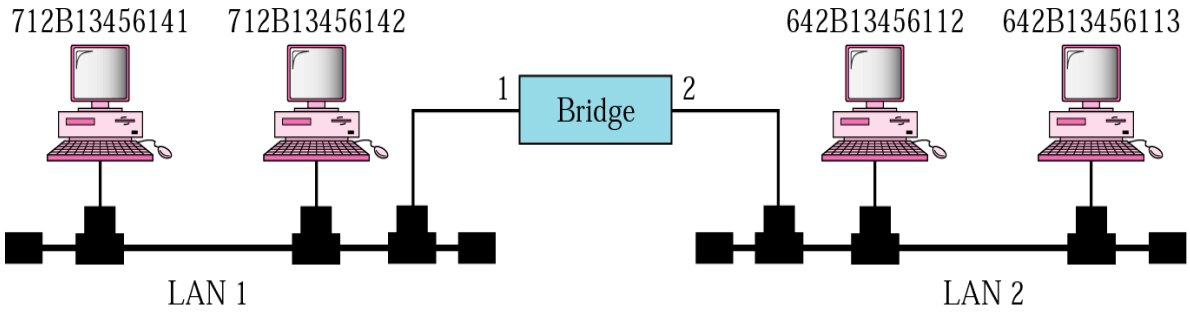
Transparent Bridges & Learning Bridges:

- Builds table by examining destination and source address of each packet it receives
- Learning bridges
  - If address is not recognized, packet is relayed to all stations
  - Stations respond and bridge updates routing table with segment and station ID information.
  - Changes on the network are updated as they occur.
- A bridge has a table used in filtering decisions.

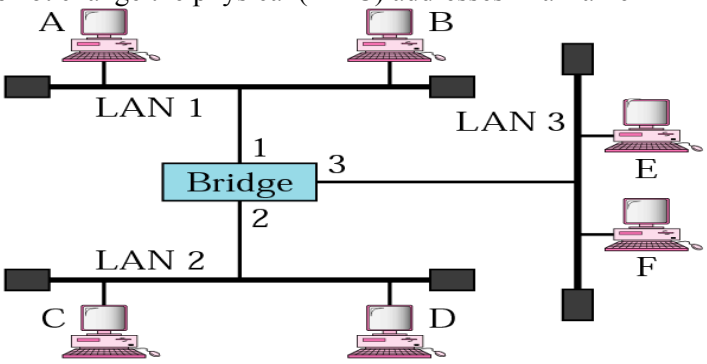


Address	Port
712B13456141	1
712B13456142	1
642B13456112	2
642B13456113	2

Bridge Table



- A bridge does not change the physical (MAC) addresses in a frame



Address	Port

a. Original

Address	Port
A	1

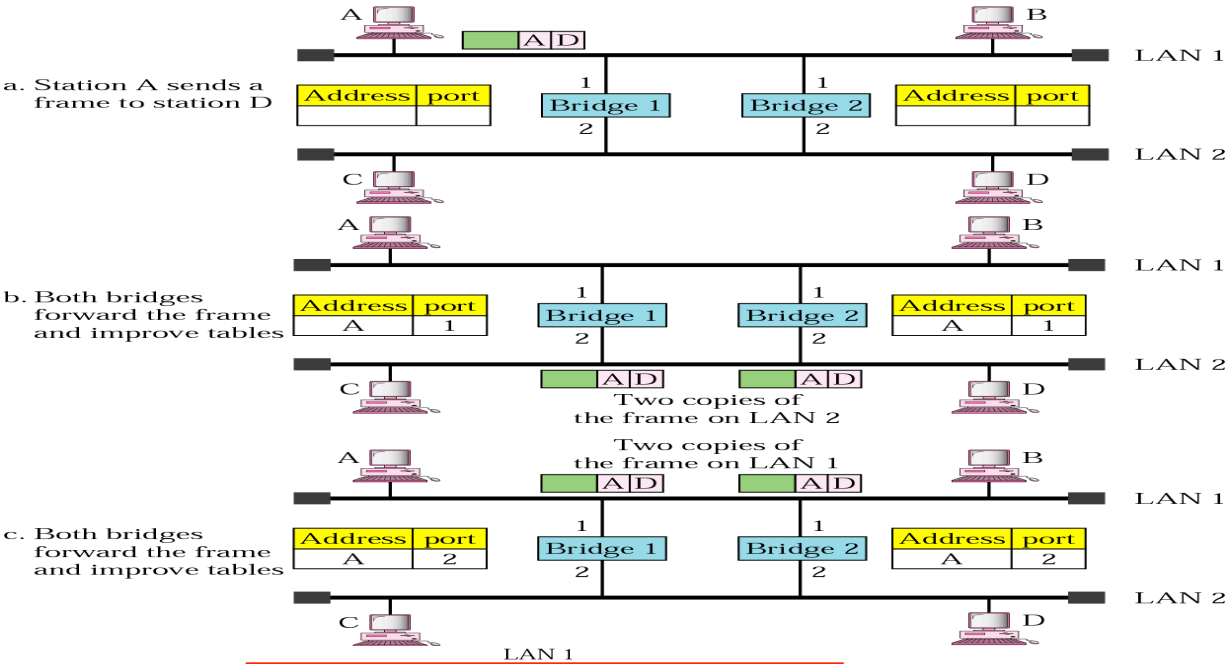
b. After A sends a frame to D

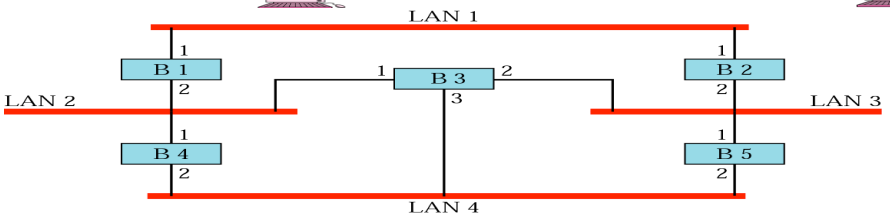
Address	Port
A	1
E	3

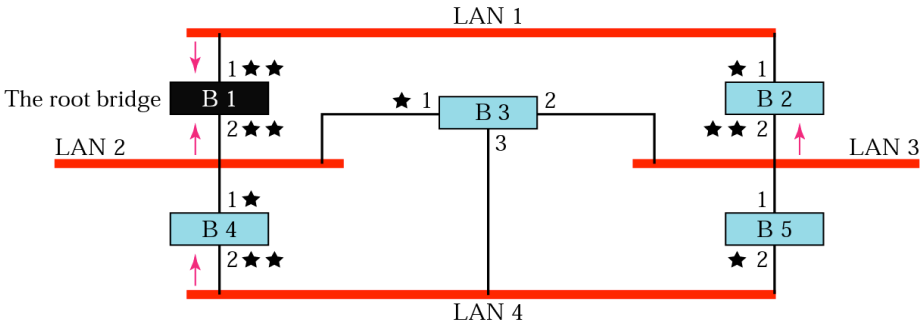
c. After E sends a frame to A

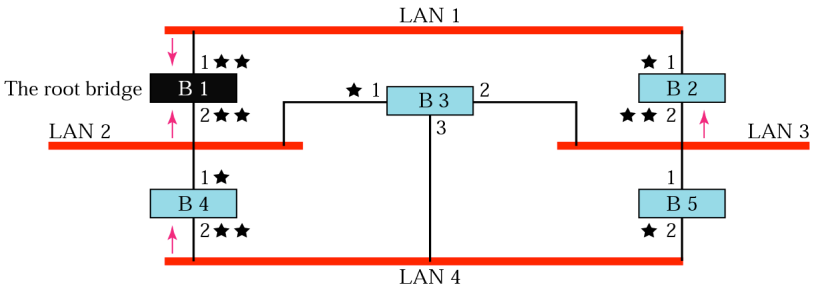
Address	Port
A	1
E	3
B	1

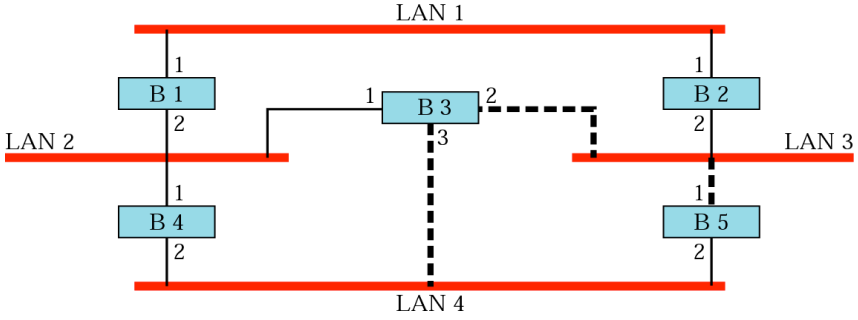
d. After B sends a frame to C


a. Station A sends a frame to station D
b. Both bridges forward the frame and improve tables
c. Both bridges forward the frame and improve tables
A
B
C
D
A D
LAN 1
LAN 2
Address
port
Bridge 1
Bridge 2
Two copies of the frame on LAN 2
Two copies of the frame on LAN 1


LAN 1
LAN 2
LAN 3
LAN 4
B 1
B 2
B 3
B 4
B 5


LAN 1
The root bridge
LAN 2
LAN 3
LAN 4
B 1
B 2
B 3
B 4
B 5


LAN 1
The root bridge
LAN 2
LAN 3
LAN 4
B 1
B 2
B 3
B 4
B 5


LAN 1
LAN 2
LAN 3
LAN 4
B 1
B 2
B 3
B 4
B 5

11. i)Discuss the IP addressing methods. (May/June2014)

There are four forms of IP addressing, each with its own unique properties.

- Unicast: The most common concept of an IP address is in unicast addressing, available in both IPv4 and IPv6. It normally refers to a single sender or a single receiver, and can be used for both sending and receiving. Usually, a unicast address is associated with a single device or host, but it is not a one-to-one correspondence. Some individual PCs have several distinct unicast addresses, each for its own distinct purpose. Sending the same data to multiple unicast addresses requires the sender to send all the data many times over, once for each recipient.
- Broadcast: In IPv4 it is possible to send data to all possible destinations ("all-hosts broadcast"), which permits the sender to send the data only once, and all receivers receive a copy of it. In the IPv4 protocol, the address 255.255.255.255 is used for local broadcast. In addition, a directed (limited) broadcast can be made by combining the network prefix with a host suffix composed entirely of binary 1s. For example, the destination address used for a directed broadcast to devices on the 192.0.2.0/24 network is 192.0.2.255. IPv6 does not implement broadcast addressing and replaces it with multicast to the specially-defined all-nodes multicast address.
- Multicast: A multicast address is associated with a group of interested receivers. In IPv4, addresses 224.0.0.0 through 239.255.255.255 (the former Class D addresses) are designated as multicast addresses.[11] IPv6 uses the address block with the prefix ff00::/8 for multicast applications. In either case, the sender sends a single datagram from its unicast address to the multicast group address and the intermediary routers take care of making copies and sending them to all receivers that have joined the corresponding multicast group.
- Anycast: Like broadcast and multicast, anycast is a one-to-many routing topology. However, the data stream is not transmitted to all receivers, just the one which the router decides is logically closest in the network. Anycast address is an inherent feature of only IPv6. In IPv4, anycast addressing implementations typically operate using the shortest-path metric of BGP routing and do not take into account congestion or other attributes of the path. Anycast methods are useful for global load balancing and are commonly used in distributed DNS systems.

When a remote access client initiates a connection to the remote access server, the remote access client creates a temporary logical interface (also known as a virtual interface or a virtual network adapter) and requests that the remote access server assigns an IP address to this logical interface.
IP address assignment can occur in one of the following ways:

From a DHCP server

The remote access server obtains the IP address to assign to a remote client from a DHCP server on the intranet. This is the default method for IP address assignment. The remote access server behaves like a DHCP client to the DHCP server and obtains 10 IP addresses at a time. As the remote access clients connect to the remote access server, the IP addresses are assigned to the clients using Internet Protocol Control Protocol (IPCP). If no DHCP server is available, the router uses an address from the Automatic Private IP Addressing (APIPA) range 169.254.0.1–169.254.255.254.

From a specified range of addresses

The remote access server obtains the IP address from a static pool of addresses configured on the remote access server. If you configure a static address pool, be sure to use only IP addresses that are not in a range that your DHCP server might assign to another computer and that are not already assigned to computers. The pool can be ranges of addresses that are a subset of addresses from the IP network to which the server is attached or from a separate subnet. If the static IP address pool address ranges represent a different subnet, ensure that routes to the address ranges exist on the routers of your intranet so that traffic to the logical interface of a remote client is forwarded to the remote access server.

From a static address specified in the user account

You configure a static IP address on the **Dial-in** tab of the user account for the remote client or in network policy. When a remote client initiates a connection, creates a temporary logical interface, and requests that the remote access server assign an IP address to this logical interface, the remote access server

assigns the IP address specified in the remote client's user account. This method is best suited for a small number of remote users.

ii) Write short notes on ARP. (May/June2014)

ARP: Associates an IP address with physical address. It is used to find the physical address of the node when its Internet address is known. Any time a host/router needs to find the physical address of another host on its network, it formats an ARP query packet that includes the IP address and broadcasts it. All hosts in the network process the ARP packet but only the required station sends back physical address.

RARP: Allows a host to discover its internet address when it knows only its physical address (a diskless computer). The host wishing to retrieve its internet address broadcasts an RARP query packet that contains its physical address to every host on its physical network. A server on the network recognizes the RARP packet and returns the host's internet address.

To map an IP address into a physical network address is to encode a host's physical address in the host part of its IP address.

- The sender needs the physical address of the receiver.
- The host or router sends an ARP query packet.
- The packet includes the physical and IP address of the sender and a IP address of the receiver.
- Becoz the sender does not know the physical address of the receiver, the query is broadcast over the network.
- a host with physical address 00100001 01001001 (which has the decimal value 33 in the upper byte and 81 in the lower byte) might be given the IP addres128.96.33.81.

Fig. ARP operation.

Goal of ARP:

- To enable each host on a network to build up a table of mappings between IP addresses and link-level addresses.
- Since these mappings may change over time (e.g., because an Ethernet card in a host breaks and is replaced by a new one with a new address), the entries are timed out periodically and removed.
- This happens on the order of every 15 minutes. The set of mappings currently stored in a host is known as the ARP cache or ARP table.

UNIT – III

PART A

1. Define routing. (Nov/Dec 2012)

It is the process of building up the tables that allow the collect output for a packet to be determined. It is a lot harder to create the forwarding tables in large, complex networks with dynamically changing topologies and multiple paths between destinations. Routing is a process that takes place in the background so that, when a data packet turns up, we will have the right information in the forwarding table to be able to forward, or switch, the packet.

2. Write on the packet cost referred in distance vector and link state routing. (Apr/May 2012)

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.

3. What is source routing? (Nov/Dec 2013)

Rotation, stripping off and using pointers are the different types of source routing approach.

4. What is the function of a router? (Nov/Dec 2010)

Routers relay packets among multiple interconnected networks. They route packets from one network to any of a number of potential destination networks on internet. A router operates as the physical, data link and network layer of the OSI model. A router is termed as an intelligent device. Therefore, its capabilities are much more than those of a repeater or a bridge.

A router is useful for interconnecting two or more heterogeneous networks that differ in their physical characteristics such as frame size, transmission rates, topologies, addressing etc. A router has to determine the best possible transmission path among several available paths. Destination, Cost and Next Hop are the important fields in a routing table.

5. Define ARP (or) what is the need of ARP? (Nov/Dec 2013)

Associates an IP address with physical address. It is used to find the physical address of the node when its Internet address is known. Any time a host/router needs to find the physical address of another host on its network, it formats an ARP query packet that includes the IP address and broadcasts it. All hosts in the network process the ARP packet but only the required station sends back physical address.

6. What is the role of VCI? (Apr/May 2011)

An **Incoming virtual circuit identifier (VCI)** uniquely identifies the connection at this switch and that will be carried inside the header of the packets that belong to this connection. It is a potentially different **outgoing VCI** that will be used for outgoing packets. The combination of incoming interface and incoming VCI uniquely identifies the virtual connection. VCI assigned by n/w admin is an unused value on that interface and VCIs are unique on a link and not on entire n/w. Also incoming and outgoing VCIs need not be same.

7. Write the difference between Distance vector routing and Link state routing.

Distance Vector Routing	**Link state routing**
Basic idea is each node sends its knowledge abou the entire network to its neighbors.	Basic idea is every node sends its knowledg about its neighbors to the entire network
It is dynamic routing	It is dynamic routing
RIP uses Distance vector routing	OSPF uses link state routing

8. What is subnetting? (Nov/Dec2011)

The whole network can't managed by single server, so that the entire network divided into small network in order to manage the network easily. 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.

9. State the rules of non boundary-level masking? (May/June 2012)

- The bytes in the IP address that corresponds to 255 in the mask will be repeated in the sub network address
- The bytes in the IP address that corresponds to 0 in the mask will change to 0 in the sub network address
- For other bytes, use the bit-wise AND operator.

Example-

IP address	45	123	21	8
Mask	255	192	0	0
Subnet	45	64	0	0
123	0 1 1 1 1 0 1 1			
192	1 1 0 0 0 0 0 0			
64	0 1 0 0 0 0 0 0			

10. **Define MTU.**

A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network such as the Internet. The Internet's Transmission Control Protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission.

11. What are data grams?

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.

12. What does Border Gateway Protocol (BGP) mean?

Border Gateway Protocol (BGP) is a routing protocol used to transfer data and information between different host gateways, the Internet or autonomous systems. BGP is a Path Vector Protocol (PVP), which maintains paths to different hosts, networks and gateway routers and determines the routing decision based on that. It does not use Interior Gateway Protocol (IGP) metrics for routing decisions, but only decides the route based on path, network policies and rule sets. Sometimes, BGP is described as a reach ability protocol rather than a routing protocol.

13. Explain IPV6 protocol.

IPv6 (Internet Protocol version 6) is a set of basics of IPv6 are similar to those of IPv4. The most obvious improvement in IPv6 over IPv4 is that IP addresses are lengthened from 32 bits to 128 bits. This extension anticipates considerable future growth of the Internet and provides relief for what was perceived as an impending shortage of network addresses. IPv6 also supports auto-configuration to help correct most of the shortcomings in version 4, and it has integrated security and mobility features.

14. What is RIP?

RIP (Routing Information Protocol) is a widely-used protocol for managing router information within a self-contained network such as a corporate local area network or an interconnected group of such LANs. Using RIP, a gateway host (with a router) sends its entire routing table (which lists all the other hosts it knows about) to its closest neighbor host every 30 seconds. The neighbor host in turn will pass the information on to its next neighbor and so on until all hosts within the network have the same knowledge of routing paths, a state known as network convergence.

15. Explain about OSPF.

OSPF (Open Shortest Path First) is a router protocol used within larger autonomous system networks in preference to the Routing Information Protocol (RIP), an older routing protocol that is installed in many of today's corporate networks.Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information.

17. Explain Multicast routing?

Multicast IP Routing protocols are used to distribute data (for example, audio/video streaming broadcasts) to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients.

18. What is PIM?

Protocol-Independent Multicast (**PIM**) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed *protocol-independent* because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols.

There are four variants of PIM:

- **PIM Source-Specific Multicast**

- **Bidirectional PIM**
- **PIM Dense Mode**
- **PIM Sparse Mode**

19. What is DVMRP?

The Distance Vector Multicast Routing Protocol (DVMRP), is a routing protocol used to share information between routers to facilitate the transportation of IP multicast packets among networks. The protocol is based on the RIP protocol. The router generates a routing table with the multicast group of which it has knowledge with corresponding distances. When a multicast packet is received by a router, it is forwarded by the router's interfaces specified in the routing table.

20. Explain IPV4 protocol.

IPv4 (Internet Protocol Version 4) is the fourth revision of the Internet Protocol (IP) used to identify devices on a network through an addressing system. The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks.IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bitaddress scheme

21. What are the differences between IPV4 and IPV6?

IPV4	**IPV6**
A 32-bit numeric address in IPv4 is written in decimal as four numbers separated by periods. Each number can be zero to 255.	IPv6 addresses are 128-bit IP address written in hexadecimal and separated by colons.
For example, **1.160.10.240** could be an IP address.	An example IPv6 address could be written like this: **3ffe:1900:4545:3:200:f8ff:fe21:67cf**

22. Define a switch.

Switches are hardware or software device capable of creating temporary connections between more devices which are not directly connected. It is a multi input/output port device. It transfers data coming from one input port to one or more output ports. This function is called as forwarding. Reliability, performance, security, and geography are the reason for using bridges in LAN.

PART B

1. **Explain Virtual circuit switching techniques. Or In the virtual circuit service model, before a virtual circuit is setup, the source router needs to specify a path from the source to the destination. What additional information do we need to maintain in the routing table to support this function? Write down the resulting routing table. (May 2012)**

Virtual Circuit Switching is also called a connection-oriented model. It requires that we first set up a virtual connection from the source host to the destination host before any data is sent.

- Since host A has to wait for the connection request to reach the far side of the network and return before it can send its first data packet, there is at least one RTT of delay before data is sent 1.

■ While the connection request contains the full address for host B (which might be quite large, being a global identifier on the network), each data packet contains only a small identifier, which is only unique on one link. Thus, the per-packet overhead caused by the header is reduced relative to the datagram model.

■ If a switch or a link in a connection fails, the connection is broken and a new one will need to be established. The old one need to be torn down to free up table storage space in the switches.

■ The issue of how a switch decides which link to forward the connection request on has been glossed over. This is the same problem as building up the forwarding table for datagram forwarding, which requires some sort of *routing algorithm*.

2 stages of process

1) Connection Setup
2) Data transfer

- Connection set up can be done in 2 ways.
  N/W administrator can configure the state, in which case the virtual circuit is permanent or PVC. Such configured states can also be deleted by n/w administrator.

Alternatively, a host can send msg in to n/w to cause the state to be established. This is referred as signaling and the resulting virtual circuit is said to be switched. The SVC can be set up and deleted dynamically by host without involving the n/w admin.

Establishing PVC

The connection state for a single connection consists of an entry in a "VC table" in each switch through which the connection passes. One entry in the VC table on a single switch contains

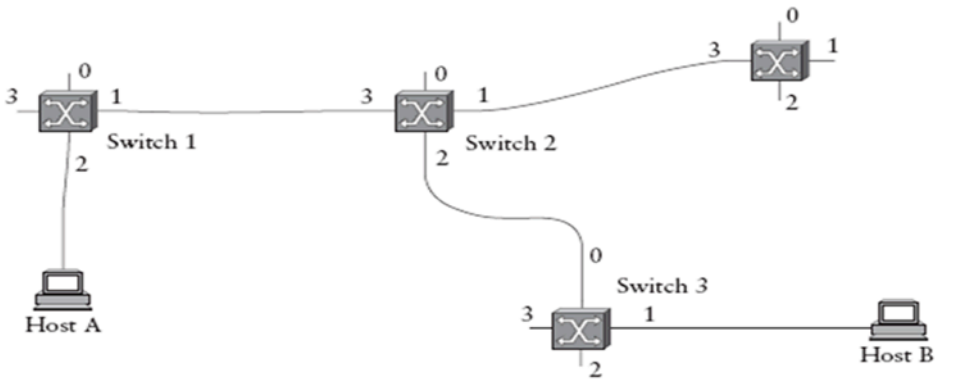
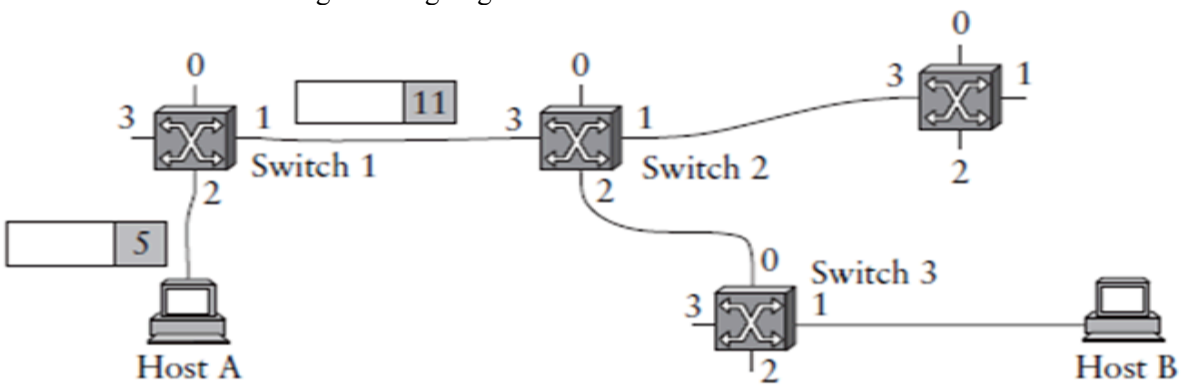


Figure 3.5 An example of a virtual circuit network.

- An **Incoming virtual circuit identifier (VCI)** that uniquely identifies the connection at this switch and that will be carried inside the header of the packets that belong to this connection.
- An **incoming interface** on which packets for this VC arrive at the switch.
- An **outgoing interface** in which packets for this VC leave the switch.
- A potentially different **outgoing VCI** that will be used for outgoing packets.
- Combination of incoming interface and incoming VCI uniquely identifies the virtual connection.

VCI assigned by n/w admin is an unused value on that interface and VCIs are unique on a link and not on entire n/w. Also incoming and outgoing VCIs need not be same.



Incoming Interface	Incoming VCI	Outgoing Interface	Outgoing VCI
2	5	1	11

(a)

Incoming Interface	Incoming VCI	Outgoing Interface	Outgoing VCI
3	11	2	7

(b)

Incoming Interface	Incoming VCI	Outgoing Interface	Outgoing VCI
0	7	1	4

(c)

Table 3.2 Virtual circuit table entries for (a) switch 1, (b) switch 2 and (c) switch 3.

Once the VC tables have been set up, data transfer phase can begin. For transfer from A to B, A puts VCI value of 5 and sends to switch1. Switch1 uses the combination of incoming i/f and incoming VCI to find appropriate table entry i.e., i/f 1 and to use VCI value of 11. This procedure is followed till pkt reaches host B.

Establishing SVC

Host A, when it wants to send data to B, sends a signal i.e., set up msg to switch1, to which it is connected. Set up msg contains complete destination address of B.

Switch1 after receiving request, creates a VC table entry containing port on which msg came, port on which it is going to forward, an incoming VCI, an outgoing VCI. Incoming VCI is fixed by switch1 and for time being it leaves outgoing VCI empty. Then it forwards the msg to switch2.

Switch2, after receiving msg it forwards it to switch3 and creates a VC table entry containing 4 fields as above. Switch3 now forwards to host B and it also creates a VC table entry following the same procedure as above.

If B accepts, it responds and fixes an incoming VCI value. This VCI value will be used by B for identifying all pkts coming from A.

Now B sends its incoming VCI value to switch3 which now fills its 4^{th} field with that value in its VC table. Switch3 now sends its VCI value to switch2 which does the same thing and sends its VCI to switch1, which sends its VCI to A.

Likewise, everyone involved fill up their VC table. At this juncture A has a firm acknowledgement that everything is in place all the way to host B.

Now data transfer begins. Once it gets over, A sends a Tear Down msg to switch1, which deletes its table entry and forwards it to switch2, which does the same, and forwards to switch3, which too follows same procedure and forwards to B which also removes its entry form its VC table.

Once connection tear down is finished, any msg from A to B will be dropped by switch1.

- Since host A has to wait for the connection request to reach the far side of the network and return before it can send its first data packet, there is at least one RTT of delay before data is sent.
- While the connection request contains the full address for host B, each data packet contains only a small identifier, which is only unique on one link. Thus, the per-packet overhead caused by the header is reduced relative to the datagram model.

If a switch or a link in a connection fails, the connection is broken and a new one will need to be established. Also, the old one need to be torn down to free up table storage space in the switches.

2. Explain Packet switching technique in detail. (or) Explain the detail about the datagram approach. (8) (Dec 2012)

Data are transmitted in discrete units Called **Packet.**

- Packets are variable length blocks. The max length of packet is established by network layer.
  - Packet contains Data and Header with control information.
- According to the header info, packets are routed between nodes.

An X.25 network—a packet-switched network that uses the connection-oriented model—employs the following three-part strategy:

1 Buffers are allocated to each virtual circuit when the circuit is initialized.
2 The sliding window protocol is run between each pair of nodes along the virtual circuit, and this protocol is augmented with flow control to keep the sending node from overrunning the buffers allocated at the receiving node.
3 The circuit is rejected by a given node if not enough buffers are available at that node when the connection request message is processed.

Types of Packet Switching Techniques

- Connectionless
  - Each packet is labelled complete destination address. Example: Datagram packet switching
- Connection-oriented
  - Each packet is labelled with a connection ID rather than an address. Example: Virtual circuit switching.

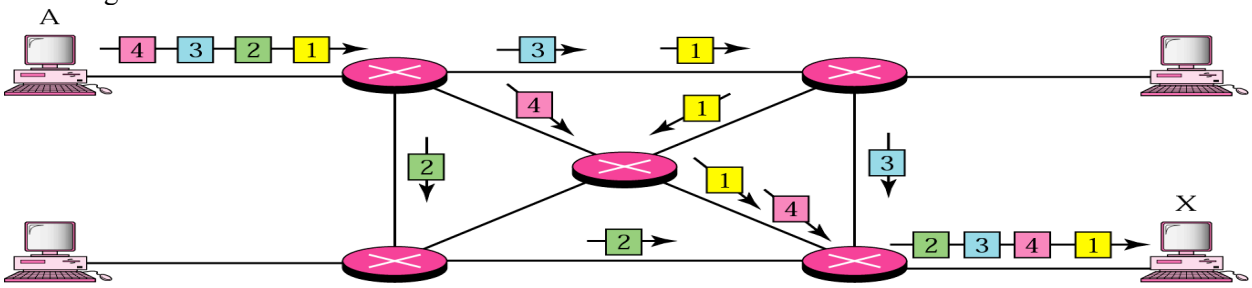


Fig. A datagram network with four switches (routers)

Datagram switching is normally done at the network layer. Figure shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers. That is why we use a different symbol for the switches in the figure.

In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X. This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources. In most protocols, it is the responsibility of an upper-layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application.

The datagram networks are sometimes referred to as connectionless networks. The term *connectionless* here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases. Each packet is treatedthe same by a switch regardless of its source or destination.

Datagram or Connectionless approach

- No connection setup phase.
- Each packet forwarded independently
- Sometimes called **connectionless** model.
- Every packet contains enough information to enable any switch to decide how to get it to its destination.
- Every packet contains the complete destination address.
- how to forward a packet, a switch consults a *forwarding table* (*routing table*)

Datagram forwarding: an example network

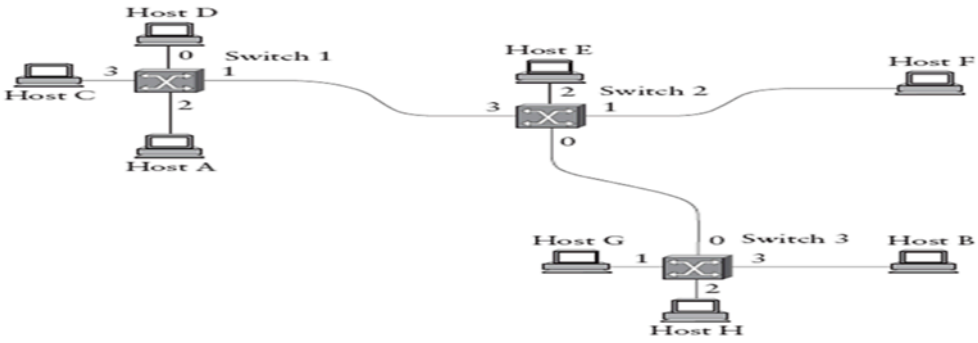


Figure 3.4 Datagram forwarding: an example network.

Such tables could be configured by n/w operator statically. It is a lot harder to create the forwarding tables in large, complex networks with dynamically changing topologies and multiple paths between destinations. That problem is known as **routing**.

- Routing is a process that takes place in the background so that, when a data packet turns up, we will have the right information in the forwarding table to be able to forward, or switch, the packet.

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

Table 3.1 Forwarding table for switch 2.

3. Explain IPv4 packet format and how fragmentation is applied in datagram delivery.

Version: (Version of IP). -The current version of IP is 4, (IPv4), represented by 0100.

Hlen: (Header length) -Length of the header in 32-bit words. A maximum length of 60 bytes can be allocated. If there are no options, length is 20 bytes only

TOS: (Type Of Service) -its basic function is to allow packets to be treated differently based on application needs. It includes bits that define priority of datagram. It also contains bits that specify the type of service expected by the sender such as level of throughput, reliability and delay.

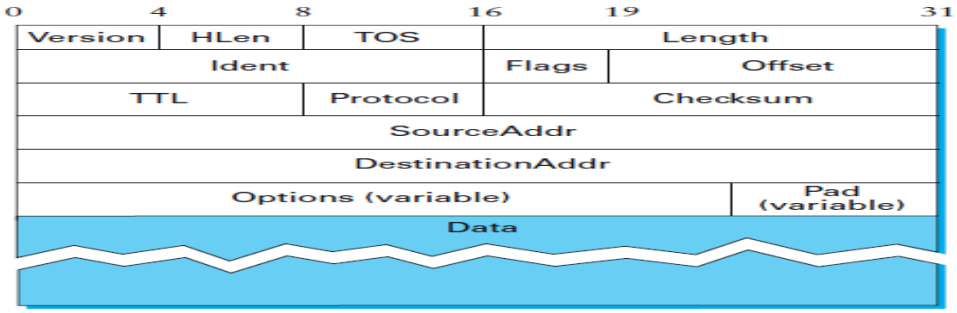
Length: - Length of the datagram includes the header. The Length field counts bytes rather than words. The maximum size of an IP datagram is 65,535 bytes.

Identification: - It is used in fragmentation. A datagram, while passing thru different n/ws may be divided into fragments to match the corresponding n/w frame size. When this happens, each fragment belonging to the same message is identified by this field.

Flags: - Bits in the flag field deal with fragmentation. 1 indicates more fragments and 0 indicates end of fragment.

Offset: - This field is a pointer that shows the offset of data in original datagram.

TTL (time to live): -TTL is set to a specific number of seconds that the packet would be allowed to live. It is fixed by the source host and gets decremented after each hop it makes. If it becomes 0 before reaching destination, it is discarded. Its default value is 64.



Protocol : -is simply a demultiplexing key that identifies the higher-level protocol to which this IP packet should be passed.

Checksum : -It is a 16 bit field used to check the integrity of header and not rest of packet.

Source Address &Destination Address:

- Each 4 byte Internet addresses identify source and destination address for the packet.

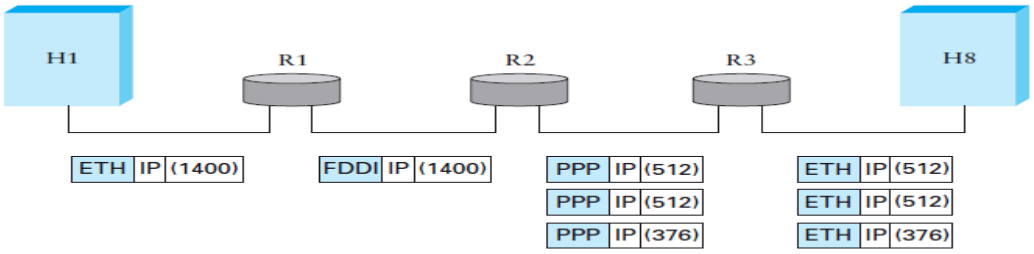
Options : Provides more functionality to the IP datagram. It carries fields that control routing, timing, management and alignment

Fragmentation and Reassembly:

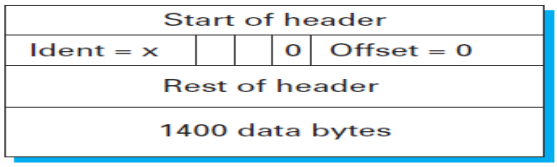
- Packets can be fragmented and reassembled when they are too big to go over a given network technology.
- Every network type has a **Maximum Transmission Unit** (MTU), which is the largest IP datagram size that it can carry in a frame.
- When a host sends an IP datagram, therefore, it can choose any size that it wants. A reasonable choice is the MTU of the network to which the host is directly attached.
- Then fragmentation will only be necessary if the path to the destination includes a network with a smaller MTU. If the transport protocol that sits on top of IP gives IP a packet larger than the local MTU, however, then the source host must fragment it.
- Fragmentation is a better option as it will not require a host to needlessly send only small packets resulting in bandwidth wastage and more resource consumption by requiring more headers for each small packet sent.
- For each fragmented pkt, the host attaches an unique identifier which assists in reassembling at destination.

Assume that the MTU is 1500 bytes for the two Ethernets, 4500 bytes for the FDDI network, and 532 bytes for the point-to-point network. Then a 1420-byte datagram (20-byte IP header plus 1400 bytes of data) sent from H1 makes it across the first Ethernet and the FDDI network without fragmentation. But it must be fragmented into three datagrams at router R2. These three fragments are then forwarded by router R3 across the second Ethernet to the destination host. The figure also serves to reinforce 2important points**:**

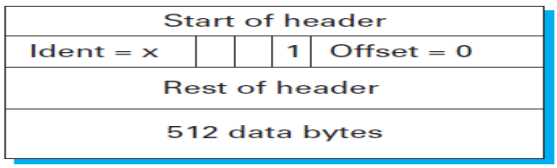
1. Each fragment is itself a self-contained IP datagram that is transmitted over a sequence of physical networks, independent of the other fragments.
2. Each IP datagram is re encapsulated for each physical network over which it travels.

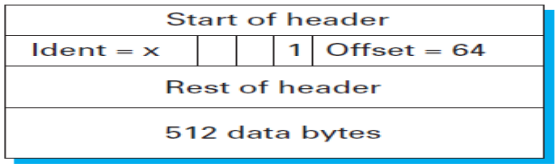


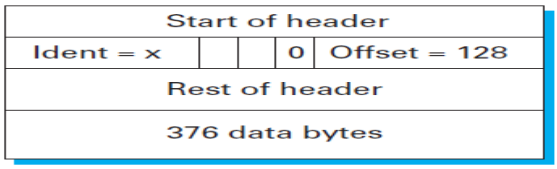
(a)



(b)







4.Discuss about Link-state routing and routers. (Nov/Dec 2012, Nov/Dec 2014)

Each router periodically shares its knowledge about its neighborhood with every other router in the inter n/w.

- Instead of sending its entire routing table, a router sends info abt its neighborhood only
- Every router sends this info to every other routers. It does this by flooding where a router sends its info to all of its neighbors through all of its o/p ports. Every router that receives the packet sends copies to all of its neighbors. Finally every router receives a copy of same info.
- Sharing only if there is any change in n/w since previous update.

Link State (OSPF) reach its directly connected neighbors, and if we make sure that the totality of this knowledge is disseminated to every node, then every node will have enough knowledge Link-state routing is the second major class of intra domain routing protocol. The starting assumptions for link-state routing are rather similar to those for distance vector routing. Each node is assumed to be capable of finding out the state of the link to its neighbors (up or down) and the cost of each link. Again, we want to provide each node with enough information to enable it to find the least-cost path to any destination. The basic idea behind link-state protocols is very simple: Every node knows how to of the network to build a complete map of the network. This is clearly a sufficient condition (although not a necessary one) for finding the shortest path to any point in the network. Thus, link-state routing protocols rely on two mechanisms: reliable dissemination of link-state information, and the calculation of routes from the sum of all the accumulated link-state knowledge.

Reliable Flooding

- 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.
- The basic idea is for a node to send its link-state information out on all of its directly connected links, with each node that receives this information forwarding it out on all of its links.
- This process continues until the information has reached all the nodes in the network.

Link-State Packet (LSP): Each node creates an update packet, also called a link-state packet (LSP), which contains the following information:

1) The ID of the node that created the LSP
2) A list of directly connected neighbors of that node, with the cost of the link to each one
3) A sequence number

4) A time to live for this packet

1 & 2 assist in – Route calculation

3 & 4 assist in – Reliable flooding process

Reliable in the sense that, making sure every node has the recent copy of info as there may be multiple, contradictory LSPs from one node traversing the n/w.

Reliability is achieved in flooding thru acknowledgements and retransmissions.

- For eg., node X receives a copy of an LSP from node Y. Both X & Y are in same n/w. X checks its table to see if it has already a copy, if so, it compares the sequence no.. If received copy's seq.no. is greater than stored one, it replaces old with new else it discards the received copy.
- Now X sends the newly received copy to all of its neighbors except the neighbor from which it received the copy. Likewise the most recent copy of LSP reaches all nodes.

Flooding of link-state packets:

LSP is generated under 2 circumstances:

i. Expiry of periodic timer.

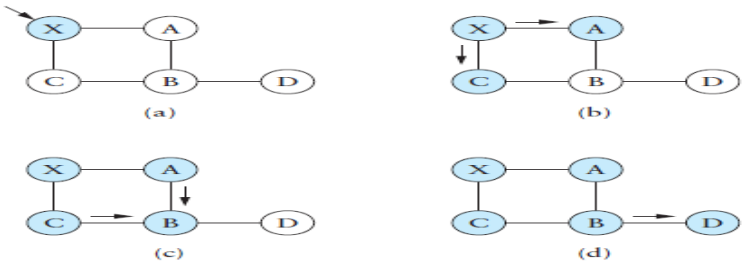
ii. Topology change.

Link failures can be detected using periodic "hello" packets sent by each node to its neighbors. If no ack. Comes or no "hello" packet is received with in specified periodic interval, a link failure is detected and an LSP is sent carrying this info from this node to its neighbors.

Route Calculation

Once a given node has a copy of LSP from every other node, it is able to compute a complete map for the topology of the network, and from this map it is able to decide the best route to each destination.

Fig. (a) LSP arrives at node X; (b) X floods LSP to A and C; (c) A and C flood LSP to B (but not X); (d) flooding is complete.



The solution is based on a well-known algorithm from graph theory.

5.Explain about the inter domain routing (BGP) routing algorithms.

Two major inter domain routing protocols in the recent history of the Internet.

Exterior Gateway Protocol (EGP):

EGP had a number of limitations: it has topological constraints i.e., it adapts to tree topology, where Autonomous systems are connected only as parent and child and not as peers.

The replacement for EGP: **Border Gateway Protocol.** BGP assumes the Internet as an arbitrarily interconnected set of ASs.

Unlike the simple tree-structured Internet, today's Internet consists of an **interconnection** of multiple backbone networks and sites that are connected to each in arbitrary ways.

Some large corporations connect directly to 1/more backbones, while others connect to smaller, non-backbone providers.

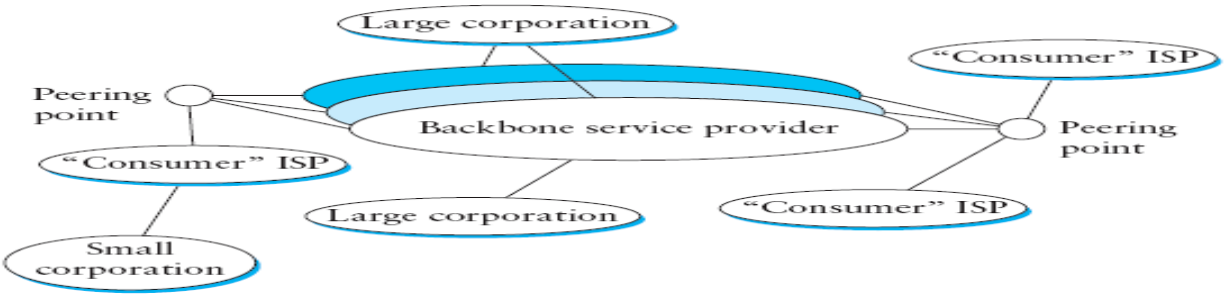
Many service providers exist mainly to provide service to consumers. These providers arrange to interconnect with each other at a single "peering point".

We can classify ASs into **three** types:

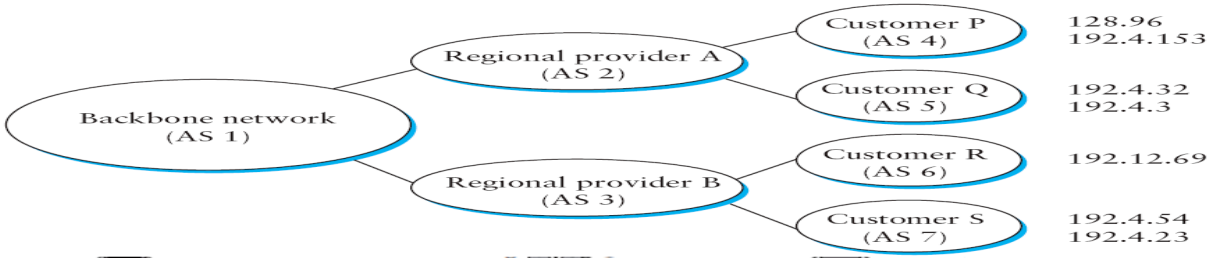
- ■ ***Stub AS****:* an AS that has only a single connection to one other AS; such an AS will only carry local traffic with in that AS. The small corporation in figure is an eg., of a stub AS.
- ■ **Multihomed AS***:* an AS that has connections to more than one other AS but that refuses to carry transit traffic; for example, the large corporation at the top
- ■ ***Transit AS****:* an AS that has connections to more than one other AS and that is designed to carry both transit and local traffic, such as the backbone providers.

The **goal** is to find **any** path to the intended destination that is loop-free. That is, we are more concerned with reachability than optimality.

- The paths must be compliant with the policies of various ASs along the path
- There are a few reasons why interdomain routing is hard. **The first** is simply a matter of scale. An Internet backbone router must be able to forward any packet destined anywhere in the Internet. Maintaining info of all routes at the backbone router is difficult.



- **The second challenge** in interdomain routing arises from the autonomous nature of the domains. Note that each domain may run its own interior routing protocols and use any scheme it chooses to assign metrics to paths.
- **The third challenge** involves the issue of trust. Provider A might be unwilling to believe certain advertisements from provider B for fear that provider B will advertise erroneous routing information.
- When configuring BGP, the administrator of each AS picks at least one node to be a **"BGP speaker" ,** which is essentially a spokesperson for the entire AS. That BGP speaker establishes **BGP sessions** to other BGP speakers in other ASs
- In addition to the BGP speakers, the AS has one or more border **"gateways",** which need not be the same as the speakers. **The border gateways** are the routers through which packets enter and leave the AS.
- BGP differs from Distance Vector and Link State routings as it advertises **complete paths** as an **enumerated list of ASs** to reach a particular network.



- In the above fig, providers are transit n/w and customer network are stubs.
- A BGP speaker for the AS of provider A (AS2) advertises its reachability info to customers P and Q i.e., it advertises n/ws 128.96, 192.4.153, 192.4.32 & 192.4.3 can be reached from it (AS2).
- The backbone n/w on receiving this advertise, advertises the networks reachable thru AS2 can be reached along the path (AS1, AS2). Similar reasoning applies for networks R and S i.e., their reachability is (AS1, AS3).
- An important job of BGP is to **prevent** the **establishment of looping paths.**
- Consider 3 interconnected AS1, AS2 & AS3. AS1 learns that it can reach network 10.0.1 through AS2, so it advertises this fact to AS3, who in turn advertises it back to AS2.
- AS2 could now decide that AS3 was the place to send packets destined for 10.0.1; AS3 sends them to AS1; AS1 sends them back to AS2; and they would loop forever.
- Such loops are prevented in BGP by carrying the complete AS path in the routing messages.
- Here ad received by AS2 from AS3 contains an AS of path AS3, AS1, AS2. AS1 finds itself in this path and concludes that it is not a useful path to use.
- For this to work, the numbering used in ASs should be unique, to prevent looping.
- Also an AS will only advertise routes that it considers good enough for itself. If a BGP speaker has a choice of several different routes to a destination, it will choose the best one according to its own local policies, and then that will be the route it advertises.

- BGP speakers need to be able to cancel previously advertised paths if a critical link or node on a path goes down. This is done with a form of negative advertisement known as a **withdrawn route.** Both positive and negative info is carried in a BGO update message.

6.Explain in detail about IP v4 addressing methods. (Nov/Dec 2012)

A very important concept in IP addressing is the network address. When an organization is given a block of addresses, the organization is free to allocate the addresses to the devices that need to be connected to the Internet. The first address in the class, however, is normally (not always) treated as a special address. The first address is called the network address and defines the organization network. It defines the organization itself to the rest of the world. The first address is the one that is used by routers to direct the message sent to the organization from the outside.

- There are 5 classes. Class A,B,C are unicast addressing. Class D is a multicast addressing. Class E is reserved for future use. Class A: 0.0.0.1 to 127.255.255.255, Class B: 128.0.0.0 to 191.255.255.255, Class C: 192.0.0.0 to 223.255.255.255,
- Class D: 224.0.0.0 to 239.0.0.0 and Class E: 240.0.0.0 to 255. 255.255.255.
- Class A. eg: 127.9.19.89,Class B eg: 120.19.17.15,class C eg: 198.16.12.34,Class D eg:230.16.12.54
- Special IP address is constructed by replacing the normal network ID or host ID (or both) in an IP address with one or two special patterns. The two patterns are:
- **Class A**

0 Netid	Host ID

- **Class B**

10 Net id	Host ID

- **Class C**

110 net id	Host id

- **Class D**

1110	Multicast address

- **Class E**

1111	reserved for future use

All Zeroes: when the network ID or host ID bits are replaced by a set of all zeroes, the special meaning is equivalent to "this", referring to whatever is replaced. It can also be interpreted as the "default" or "the current".

All ones: When the network ID or host ID bits are replaced by a set of all ones this has the special meaning of "all". So replacing the host ID with all ones means the IP address refers to all hosts on the network. This is generally used as a broadcast address for sending a message to everyone.

- There are several other set of IP address set aside for various special uses, which are not available for normal address assignment. These ranges of IP address generally fall into the following three categories: reserved, loopback, and private addresses.

Reserved address: Several blocks of address are designated just as "reserved" with no specific indication given of what they were reserved for. there are a couple of these blocks in each of the three main classes(A,B,C)appearing right at the beginning and end of each class .Even though classes D and E are reserved they aren't used for regular addressing .the term "reserved" is usually used to refer to unusable parts of classes A,B,C.

Loopback Address:

- One special range of address is set aside for loopback functionality. This is the range 127.0.0.0 to 127.255.255.255.IP datagrams sent by a host to a 127.x.x..x loopback address are not passed down to the data link layer for transmission. Instead they "loopback" to the source device at the IP level. In essence this represents a "short circuiting" of the normal protocol stack. Data is sent by a device's layer three IP implementation and the immediately received by it.

The purpose of the loopback range is testing of the TCP/IP protocol implementation on a host.127.0.0.1 is the address most commonly used for testing purposes.

Special Address	Net ID	Host ID	Source/Destination
Network Address	Specific	All 0's	None

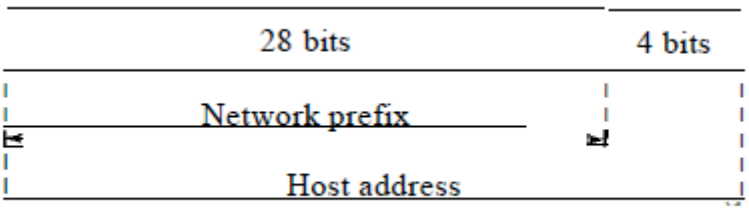
Direct br oadcast	Specific	All 1's	Destination
Limited broadcast address	All 1's	All 1's	Destination
This host on this network	All 0's	All 0's	Source
Specific Host on this network	All 0's	Specific	Destination
Loop back Address	127	Any	Destination

Hierarchy

IP addresses, like other addresses or identifiers we encounter these days, have levels of hierarchy.

Two-Level Hierarchy: No Subnetting

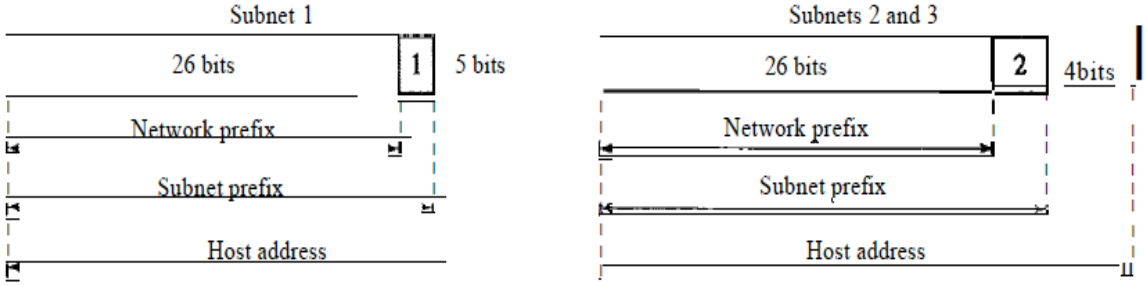
An IP address can define only two levels of hierarchy when not subnetted. The *n* leftmost bits of the address *x.y.z.tJn* define the network (organization network); the 32 – *n* rightmost bits define the particular host (computer or router) to the network. The two common terms are prefix and suffix. The part of the address that defines the network is called the prefix; the part that defines the host is called the suffix. Figure shows the hierarchical structure of an IPv4 address.



Each address in the block can be considered as a two-level hierarchical structure: the leftmost *n* bits (prefix) define the network; the rightmost 32 - *n* bits define the host.

Three-Levels ofHierarchy: Subnetting

An organization that is granted a large block of addresses may want to create clusters of networks (called subnets) and divide the addresses between the different subnets. The rest of the world still sees the organization as one entity; however, internally there are several subnets. All messages are sent to the router address that connects the organization to the rest of the Internet; the router routes the message to the appropriate subnets. The organization, however, needs to create small subblocks of addresses, each assigned to specific subnets. The organization has its own mask; each subnet must also have its own.



7.Describe about Ipv6.

The motivation for a new version of IP is the same as the motivation for the techniques to deal with scaling problems caused by the Internet's massive growth. In particular, it is virtually impossible to achieve 100% address utilization efficiency, so the address space will be exhausted well before the four-billionth host is connected to the Internet.

The effort to define a new version of IP was known as IP Next Generation, or IPng. As the work progressed, an official IP version number was assigned, so IPng is now known as IPv6.

In addition to the need to accommodate scalable routing and addressing, some of the other wish list items for IPng were:

- support for real-time services

- security support
- auto configuration
- enhanced routing functionality, including support for mobile hosts

ADDRESSES AND ROUTING

IPv6 address consists of 16 bytes with 128-bits long while 32 bits in IPv4.

IPv4 addresses 4 billion nodes in 100% efficiency while, IPv6 addresses 3.4*10^38

The IPv6 address space is predicted to provide over 1500 addresses per square foot of the earth's surface.

ADDRESS SPACE ALLOCATION

IPv6 addresses do not have classes, but the address space is still subdivided in various ways based on the leading bits.

The leading bits specify different uses of the IPv6 address.

ASSIGNMENT OF PREFIXES

Prefix	Use
0000 0000	Reserved
0000 0001	Unassigned
1111 1110 10	Link local use addresses
1111 1110 11	Site local use addresses
1111 1111	Multicast addresses

From the above list, multicast addresses are easily distinguishable; they start with a byte of all 1s.

Link local use addresses is to enable a host to construct an address that will work on the network to which it is connected (internally unique, not globally).

Site local use addresses allow valid addresses to be constructed on a site (private corporate network) that is not connected to the Internet. Also it is not globally unique.

ADDRESS NOTATION

The standard representation is x:x:x:x:x:x:x:x, where each "x" is a hexadecimal representation of a 16-bit piece of the address. For eg., 47CD:1234:4422:ACO2:0022:1234:A456:0124.

Special notations are used to describe some special types of IPv6 addresses.

For example, an address with a large number of contiguous 0s can be written more compactly by omitting all the 0 fields. i.e., 47CD:0000:0000:0000:0000:0000:A456:0124 could be written as 47CD::A456:0124. Also such form of shorthand can only be used for one set of contiguous 0s in an address.

- Since there are two types of IPv6 addresses that contain an embedded IPv4 address, these have their own special notation that makes extraction of the IPv4 address easier.
- For example, the "IPv4- mapped IPv6 address" of a host whose IPv4 address was 128.96.33.81 could be written as ::FFFF:128.96.33.81.

i.e., the last 32 bits are written in IPv4 notation, rather than as a pair of hexadecimal no.s separated by a colon. Also the double colon at front indicates leading 0s.

GLOBAL UNICAST ADDRESS

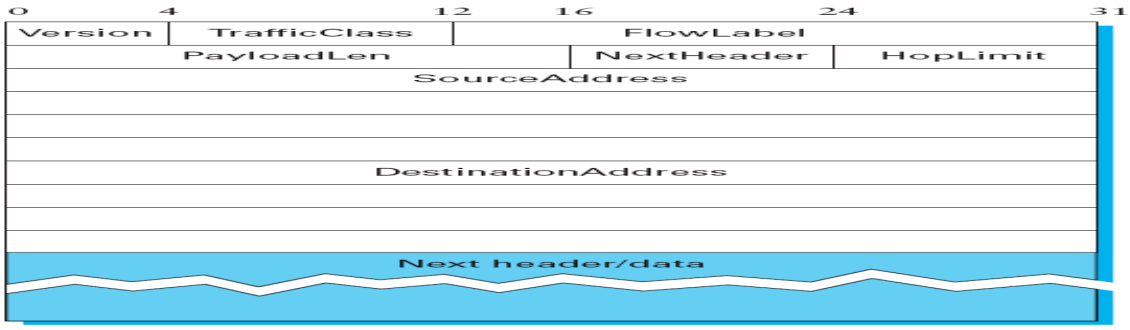
- **Type-ID**: Defines addr as provider based address.
- **Registry ID**: Indicates the agency that has registered the address. Registry centers available are INTERNIC with code 11000 for North America, RIPNIC with code 01000 for Europe and APNIC with code 10100 for Asia Pacific.
- **Provider-ID**: Identifies provider for Internet access. 16 bit length is recommended.
- **Subscriber-ID**: when an organization subscribes to Internet thru a provider, it is assigned a subscriber ID. Again 24 bit length is recommended.

- **Subnet-ID**: Each subscriber can have many sub n/ws with different IDs. Subnet ID defines a specific n/w under the territory of subscriber. A 32 bit length is recommended.

Interface-ID: Identifies node connected to the subnet. A length of 48 bits is recommended to be compatible with link level Ethernet address

PACKET FORMAT: It has two types of formats: 1) IPv6 packet header
2) IPv6 fragmentation extension header.

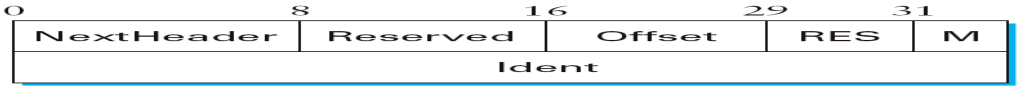
- **Version**: Defines version no. of IP.
- **Traffic Class**: Defines priority of packet with respect to traffic congestion.
- **Flow Label**: Designed to provide spl. Handling for a particular flow of data.
- **Payload Length**: Defines length of IP datagram excluding base header.
- **Next Header**: Defines the header that follows base header. It replaces both the IP options and Protocol field of IPv4. If options are required, they are carried out in one or more spl. headers following IPv6 header, and this is indicated by the value of Next Header field. If there are no spl. headers, the Next Header field contains demux key identifying the higher level protocol running over IP.
- **Hop Limit**: Serves the same purpose as TTL of IPv4.
- **Source Addr & Dest Addr** : A 16 byte IP addr identifying original source and destination of datagram.



Headers in IPv6

- IPv6 treats options as Extension Headers that must, if present, appear in a specific order.
- A router finds out easily whether the options present are relevant to it or not by looking at the Next Header field, leading to better option processing.
- Options in IPv6 can be of arbitrary lengths. Each option has an extension header whose type is identified by the value of Next Header.
- Each extension header contains a Next Header to identify the header following it. Last extension header will be followed by a transport layer header.
- Therefore Next Header serves dual purpose by identifying the type of extension header to follow as well as in the last extension, it serves as demux key identifying higher layer protocol running over IPv6.

An Example Extension Header:



- This header provides functionality similar to the fragmentation fields in the IPv4 header.
- If we assume that this is the only ext. header present, then the Next Header field of IPv6 would contain value 44 (used to represent fragment header) .
- The Next Header field of fragmentation header itself contains a Next Header, describing the header that follows it.
- Again if we assume no hdrs to follow, then this might be TCP hdr, which results in Next Header containing the value 6. If an authentication header is to follow, then Next Header contains value 51.

AUTO CONFIGURATION

- One goal of IPv6, therefore, is to provide support for auto configuration, sometimes referred to as "plug-and-play" operation.
- New form of auto configuration called *stateless* auto configuration is used (similar to DHCP in IPv4), which does not require a server.
- We can subdivide the auto configuration problem into two parts:

1) Obtain an interface ID (Ethernet addr-48 bits) that is unique on the link to which the host is attached. This could be converted to link local use addr by appropriate prefix to make up 128 bits. 2) Obtain the correct address prefix for this subnet, which could be obtained from the router attached on same link. This prefix should contain enough space to attach an appropriate link level address.

ADVANCED ROUTING CAPABILITIES

- Another of IPv6's extension headers is the routing header containing a list of IPv6 addresses that represent nodes or topological areas that the packet should visit on its way to destination.
- A host could say that it wants some packets to go thru a provider providing high reliability or cheaper cost or offering best security.
- To provide the ability to specify topological entities rather than individual nodes, IPv6 defines an ***anycast*** address.
- An anycast address is assigned to a set of i/fs. Packets sent to that address will go to the "nearest" of those i/fs, with nearest being determined by the routing protocols.
- The anycast address and the routing header are also expected to be used to provide enhanced routing support to mobile hosts.

8.Explain the Routing Information protocol/Distance vector routing in detail. (Nov/Dec 2013)

Distance Vector Routing

- Each router periodically shares its knowledge about the entire internet with its neighbors
  - Sharing the knowledge about the entire autonomous system (n/w)
  - Sharing only with neighbors
  - Sharing at regular intervals for eg., every 30 seconds whether or not the n/w has changed since the last info was exchanged.

RIP – Routing Information Protocols

- Interior routing protocol used inside an autonomous system
- Based on distance vector routing which uses Bellman-Ford algorithm for calculating the routing tables

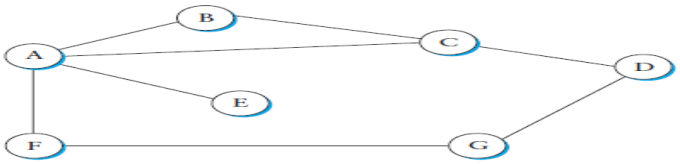


Figure 4.15 Distance-vector routing: an example network.

Distance Vector Routing Algorithm

Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	∞	1	1	∞
B	1	0	1	∞	∞	∞	∞
C	1	1	0	1	∞	∞	∞
D	∞	∞	1	0	∞	∞	1
E	1	∞	∞	∞	0	∞	∞
F	1	∞	∞	∞	∞	0	1
G	∞	∞	∞	1	∞	1	0

Table 4.5 Initial distances stored at each node (global view).

- The cost of each link is set to 1, so that a least-cost path is simply the one with the fewest hops.
- Those nodes that are directly connected have a distance of 1 and not directly connected nodes are marked infinity initially.

- When each node shares this info with its directly connected neighbors, it gets a clear view of the cost required to reach every other node in the n/w.
- For eg., node F tells A , it can reach G with cost 1. A knows it can reach F with cost 1 and ultimately reach G with cost 2, which is less than infinity, which it records in its table.
- Like wise each node shares its info about the entire n/w with its neighbors and the final routing table of A will be as shown.
- Also the final updated table containing shortest paths between each pair of nodes is also given.

In case of any topological changes, each node exchanges some amount of information to complete the entries of the routing table. This process is called **Convergence.**

There are two types of updates that are done in the table every row:

- **Periodic update** : This is done by sending update messages to all of its adjacent nodes periodically even though there are no changes so as to check the functionality of other nodes
- **Triggered update** : This is done by sending an update message when there are any changes in topology of the network

  In case of any failure of link or node, the neighboring node will immediately react to it and do the necessary changes so as to maintain the flow of network
- Failure is detected by two ways:
  - One way is that each node sends a control packet and waits for acknowledgement. If there is no acknowledgement then there is a failure.
  - Another way is that if the periodicity of the periodic update information is not maintained then there may be a link failure.

Distance Vector Routing Algorithm

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

Table 4.6 Initial routing table at node A.

Destination	Cost	NextHop
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	2	F

Table 4.7 Final routing table at node A.

Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

Table 4.8 Final distances stored at each node (global view).

Example: When F detects its link to G has failed, its sets its destination to G as infinity and passes this info along to A. Now A accordingly sets its table value also to infinity. However with next update from C to A, A learns C can reach G with 2 hops and ultimately A can reach G with 3 hops. Now A sends this updated info to F which updates its cost of reach to G as 4.

9 i)What is the need for ICMP? Mention ICMP MESSAGES and their purpose. (May/June 2013)
ii) Describe with example how CIDR addresses the two scaling concern in the internet. (Nov/Dec 2013)

ICMP is an error reporting mechanism. It does not specify the action to be taken for each possible error. The source must relate the error to an individual application program and take other actions to correct the problem. **ICMP** allows routers to send error messages to other router or hosts. It is informing the source that the error has occurred and the source has to take actions to rectify the errors.

Types of Messages:

- Error reporting Messages: A router or hosts reports the problems encountered when it processes a packet
- Query Messages: Helps a host or a network manager to get specific information from a router or another host. Ex: nodes can discover their neighbor.

Category	*Type*	*Message*
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply
	17 or 18	Address mask request or reply
	10 or 9	Router solicitation or advertisement

B) Describe with example how CIDR addresses the two scaling concern in the internet. (10) (dec 2013)

- IP address space was depleting rapidly.

– The Internet Engineering Task Force (IETF) introduced Classless Inter-Domain Routing (CIDR)

• CIDR uses Variable Length Subnet Masking (VLSM) to help conserve address space

• VLSM is simply subnetting a subnet.

Classless Inter-domain Routing (CIDR – RFC 1517)

– Advantage of CIDR :

• More efficient use of IPv4 address space

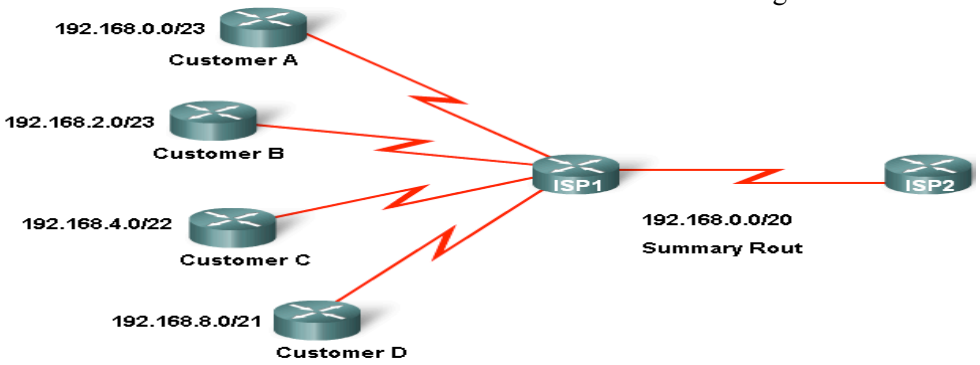
• Route summarization

– Requires subnet mask to be included in routing update because address class is meaningless

– Recall purpose of a subnet mask:

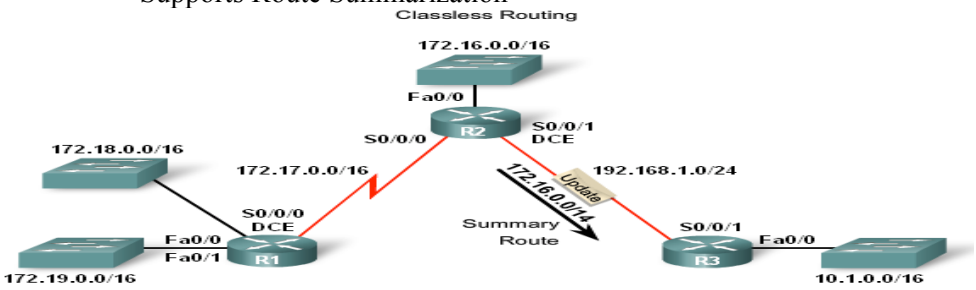
• To determine the network and host portion of an IP address

- Classless IP Addressing
- CIDR & Route Summarization
  - Variable Length Subnet Masking (VLSM)
  - Allows a subnet to be further sub-netted according to individual needs
  - Prefix Aggregation a.k.a. Route Summarization
  - CIDR allows for routes to be summarized as a single route.



Characteristics of classless routing protocols:

- Routing updates include the subnet mask
- Supports VLSM
- Supports Route Summarization

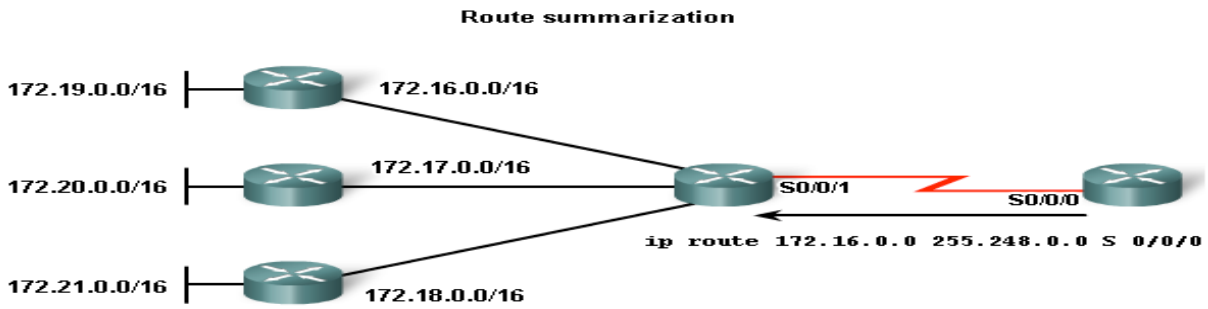


Routing Protocol	Routing updates Include subnet Mask	Supports VLSM	Ability to send Supernet routes
Classful	No	No	No
Classless	Yes	Yes	Yes

Route summarization done by CIDR

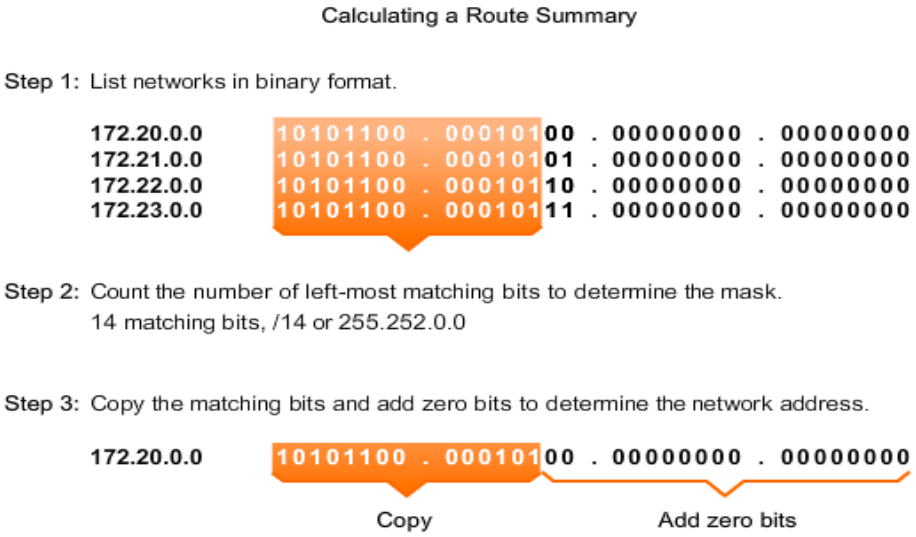
– Routes are summarized with masks that are less than that of the default classful mask

Example: 172.16.0.0 / 13 is the summarized route for the 172.16.0.0 / 16 to 172.23.0.0 / 16 classful networks



Steps to calculate a route summary

– List networks in binary format
– Count number of left most matching bits to determine summary route's mask
– Copy the matching bits and add zero bits to determine the summarized network address



CIDR

– Uses IP addresses more efficiently through use of VLSM

•VLSM is the process of subnetting a subnet

– Allows for route summarization

•Route summarization is representing multiple contiguous routes with a single route

▪ Classless Routing Updates

– Subnet masks are included in updates

10 i) Discuss about address Resolution protocols. (Nov/Dec 2013)

ii) Explain in detail about DHCP.

ARP: Associates an IP address with physical address. It is used to find the physical address of the node when its Internet address is known. Any time a host/router needs to find the physical address of another host on its network, it formats an ARP query packet that includes the IP address and broadcasts it. All hosts in the network process the ARP packet but only the required station sends back physical address.

RARP: Allows a host to discover its internet address when it knows only its physical address (a diskless computer). The host wishing to retrieve its internet address broadcasts an RARP query packet that contains its physical address to every host on its physical network. A server on the network recognizes the RARP packet and returns the host's internet address.

To map an IP address into a physical network address is to encode a host's physical address in the host part of its IP address.

- The sender needs the physical address of the receiver.
- The host or router sends an ARP query packet.
- The packet includes the physical and IP address of the sender and a IP address of the receiver.
- Becoz the sender does not know the physical address of the receiver, the query is broadcast over the network.

- a host with physical address 00100001 01001001 (which has the decimal value 33 in the upper byte and 81 in the lower byte) might be given the IP addres128.96.33.81.

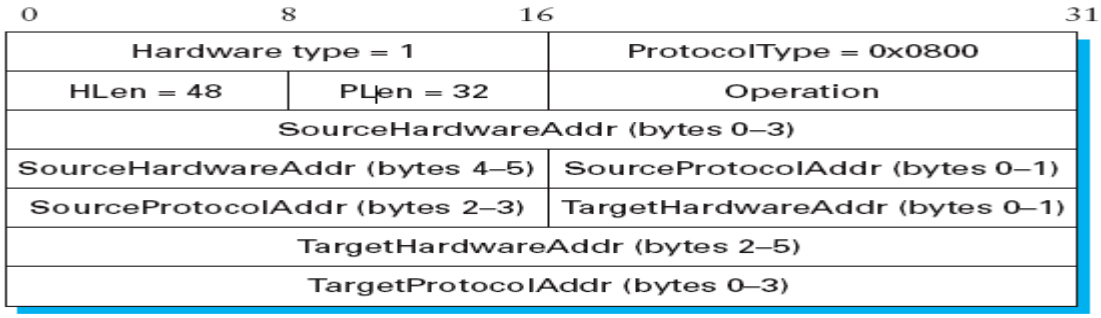


Fig. ARP operation

ARP packet format for mapping IP addresses into Ethernet addresses.

In addition to the IP and link-layer addresses of both sender and target, the packet contains

- a Hardware Type field, which specifies the type of physical network (e.g., Ethernet)
- a Protocol Type field, which specifies the higher-layer protocol (e.g., IP)
- HLen ("hardware" address length) and PLen ("protocol" address length) fields, which specify the length of the link-layer address and higher-layer protocol address, respectively
- an Operation field, which specifies whether this is a request or a response the source and target hardware (Ethernet) and protocol (IP) addresses

Goal of ARP:

- To enable each host on a network to build up a table of mappings between IP addresses and link-level addresses.
- Since these mappings may change over time (e.g., because an Ethernet card in a host breaks and is replaced by a new one with a new address), the entries are timed out periodically and removed.
- This happens on the order of every 15 minutes. The set of mappings currently stored in a host is known as the ARP cache or ARP table.

ARP takes advantage of the fact that many link-level network technologies, such as Ethernet and token ring, support broadcast.

- In Broadcast, each bridge forwards a frame with a destination broadcast address out on each active port other than the one on which the frame was received.

The disadvantage here is that the network's physical addresses can be no more than 16 bits long. A more general solution would be for each host to maintain a table of address pairs.

- If a host wants to send an IP datagram to 6another host on the same network, it first checks for a mapping in the cache.
- If no mapping is found, it invokes the Address Resolution Protocol over the network.
- It does this by broadcasting an ARP query onto the network.
- This query contains the "target IP address".
- Each host receives the query and checks to see if it matches its IP address.
- If it matches, the host sends a response message that contains its link-layer address back to the originator of the query.
- The originator adds the information contained in this response to its ARP table.
- The query message also includes the IP address and link-layer address of the sending host.
- Thus, when a host broadcasts a query message, each host on the network can learn the sender's link-level and IP addresses and place that information in its ARP table.
- If the host already has an entry for that host in its table, it "refreshes" this entry.
- If the host is the target of the query, then it adds the information about the sender to its table, even if it did not already have an entry for that host.
- If a host is not the target and does not already have an entry for the source in its ARP table, then it does not add an entry for the source.

DHCP

Automated configuration methods use a protocol known as the Dynamic Host Configuration Protocol (DHCP). DHCP relies on the existence of a DHCP server that is responsible for providing configuration information to hosts. Internetwork contains a network part and a host part, and the network part must be the same for all hosts on the same network. Thus, it is not possible for the IP address to be configured once into a host when it is manufactured, since that would imply that the manufacturer knew which hosts were going to end up on which networks, and it would mean that a host, once connected to one network, could never move to another. For this reason, IP addresses need to be reconfigurable.

- IP addresses are some other pieces of information a host needs to have before it can start sending packets.
- The most notable of these is the address of a default router—the place to which it can send packets whose destination address is not on the same network as the sending host.
- Most host operating systems provide a way for a system administrator, or even a user, to manually configure the IP information needed by a host.

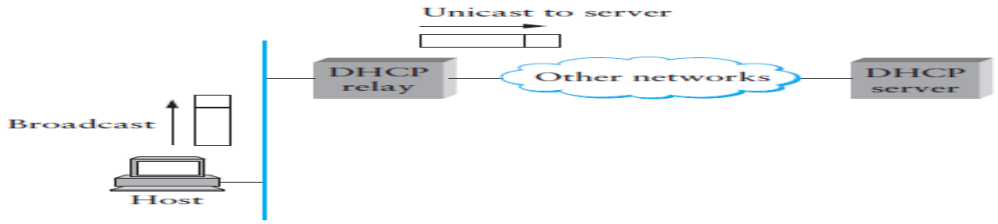
Drawbacks of manual configuration:

- It is a lot of work to configure all the hosts in a large network directly, especially when you consider that such hosts are not reachable over a network until they are configured.
- The configuration process is very error-prone, since it is necessary to ensure that every host gets the correct network number and that no two hosts receive the same IP address

DHCP Server:

- can function just as a centralized repository for host configuration information.
- saves the network administrators from having to walk around to every host in the company with a list of addresses and network map in hand and configuring each host manually.
- the configuration information for each host could be stored in the DHCP server.
- administrator would still pick the address that each host is to receive; he would just store that in the server
- DHCP saves the network administrator from even having to assign addresses to individual hosts.
- DHCP server maintains a pool of available addresses that it hands out to hosts on demand.
- The goal of DHCP is to minimize the amount of manual configuration required for a host to function, it would rather defeat the purpose if each host had to be configured with the address of a DHCP server.

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



DHCP packet format:

- The message is actually sent using a protocol called UDP (the User Datagram Protocol) that runs over IP.
- It does in this context is to provide a demultiplexing key that says, “This is a DHCP packet.”
- DHCP is derived from an earlier protocol called BOOTP, and some of the packet fields are thus not strictly relevant to host configuration.
- When trying to obtain configuration information, the client puts its hardware address (e.g., its Ethernet address) in the chaddr field.
- The DHCP server replies by filling in the yiaddr (“your” IP address) field and sending it to the client.
- Other information such as the default router to be used by this client can be included in the options field.
- DHCP illustrates an important aspect of scaling: the scaling of network management.

- While discussions of scaling often focus on keeping the state in network devices from growing too rapidly, it is important to pay attention to growth of network management complexity.
- By allowing network managers to configure a range of IP addresses per network rather than one IP address per host, DHCP improves the manageability of a network.

UNIT – IV

PART A

1. **Give any two Transport layer service. (Dec 2012)**

Multiplexing: Transport layer performs multiplexing/demultiplexing function. Multiple applications employ same transport protocol, but use different port number. According to lower layer n/w protocol, it does upward multiplexing or downward multiplexing.

Reliability: Error Control and Flow Control.

2. **Mention the various adaptive retransmission policy of TCP.**
   - Simple average
   - Exponential / weighted average
   - Exponential RTT backoff
   - Jacobson's Algorithm

3. **Define congestion. (Nov '11)**

Congestion in a network occurs if user sends data into the network at a rate greater than that allowed by network resources. Any given node has a number of I/O ports attached to it. There are two buffers at each port. One to accept arriving packets & another one to hold packets that are waiting to depart. If packets arrive too fast node than to process them or faster than packets can be cleared from the outgoing buffers, then there will be no empty buffer. Thus causing congestion and traffic in the network.

4. **Why the congestion occur in network?**

Congestion occurs because the switches in a network have a limited buffer size to store arrived packets. And also because the packets arrive at a faster rate than what the receiver can receive and process the packets.

5. **What is Tinygram?**

A very small packet of data is called a tinygram. Too many tinygrams can congest a network connection.

6. **Give the datagram format of UDP?**

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

Source Port Address 16 bits	Destination Port Address 16 bits
Total Length 16 bits	Checksum 16 bits

- **Source port address**: It is the address of the application program that has created the message.
- **Destination port address:** It is the address of the application program that will receive the message.
- **Total Length:** It defines the total length of the user datagram in bytes.
- **Checksum:** It is a 16 bit field used in error correction.

7. **What is the main difference between TCP & UDP?(Nov/Dec 2014)**

TCP	**UDP**
It provides Connection oriented service	Provides connectionless service.
Connection Establishment delay will be there	No connection establishment delay
Provides reliable service	Provides unreliable, but fast service
It is used by FTP, SMTP	It is used by DNS,SNMP, audio, video and multimedia applications.

8. **What are the advantages of using UDP over TCP? (Nov/Dec 2010)**

UDP is very useful for audio or video delivery which does not need acknowledgement. It is useful in the transmission of multimedia data. Connection Establishment delay will occur in TCP.

9. **What is TCP? (Nov/Dec 2011)**

Transmission Control Protocol provides Connection oriented and reliable services. 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. It is used by FTP, SMTP. The different phases in TCP state machine are Connection Establishment, Data transfer and Connection Release. TCP services to provide reliable communication are Error control, Flow control, Connection control and Congestion control.

10. Name the policies that can prevent (avoid) congestion.

- DEC (Digital Equipment Corporation) bit.
- Random Early Detection (RED).
- Source based congestion avoidance.

The congestion may be avoided by two bits:
BECN - Backward Explicit Congestion Notification
FECN - Forward Explicit Congestion Notification.

11. List out various congestion control techniques.

- AIMD (Additive Increase Multiplicative Decrease)
- slow start
- Fast retransmit
- Recovery.

12. What is the difference between service point address, logical address and physical address?

Service point addressing	Logical addressing	Physical addressing
The transport layer header includes a type of address called a service point address or port address, which makes a data delivery from a specific process on one computer to a specific process on another computer.	If a packet passes the network boundary we need another addressing to differentiate the source and destination systems. The network layer adds a header, which indicates the logical address of the sender and receiver.	If the frames are to be distributed to different systems on the network, the data link layer adds the header, which defines the source machine's address and the destination Machine's address.

13. What is the use of UDP's Pseudo header?

The pseudo header consists of three field from the IP header protocol number ,source IP address and destination IP address plus the UDP length field (which is included twice in checksum calculation).The pseudo header is used to check whether the message is delivered between 2 endpoints.

14. What are the two categories of QoS attributes?

User Oriented and Network Oriented. User related attributes are

- SCR – Sustainable Cell Rate
- PCR – Peak Cell Rate
- MCR- Minimum Cell Rate
- CVDT – Cell Variation Delay Tolerance.

The network related attributes are, Cell loss ratio (CLR), Cell transfer delay (CTD), Cell delay variation (CDV), Cell error ratio (CER).

15. Suppose TCP operates over a 1-Gbps link, utilizing the full bandwidth continuously. How long will it take for the sequence numbers to wrap around completely? Suppose an added 32-bit timestamp field increments 1000 times during this wrap around time, how long it will take timestamp filed to wrap around? (May2013)

Once a segment with sequence x survives in Internet, TCP cannot use the same sequence no. How fast 32-bit sequence no space can be consumed? 32-bit sequence no is adequate for today's network.
Wrap Around Time for T3-45Mbps (2^{32} x 8) /45Mbps=763.55sec=12.73 min.

16. Write short notes on congestion control. (Nov/Dec 2012)

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.

15. Differentiate congestion control and flow control. (Nov/Dec 2013)

Congestion Control	Flow Control

Congestion control means preventing the sourc from sending data that will end up getting droppe by a router because its queue is full.	Flow control means preventing the sourc from sending data that the receiver will end u dropping because it runs out of buffer space.
This is more complicated, because packets from different sources travelling different paths can converge on the same queue.	This is fairly easy with a sliding windo protocol

18. What do you mean by QoS? (May/June 2012,Nov/Dec 2014)

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.

19. What are the four aspects related to the reliable delivery of data? (May/June 2012)

The four aspects are Error control, Sequence control, Loss control and Duplication control.

20. What is UDP?

It stands for User Datagram Protocol. It is part of the TCP/IP suite of protocols used for data transferring. UDP is a known as a "stateless" protocol, meaning it doesn't acknowledge that the packets being sent, have been received.

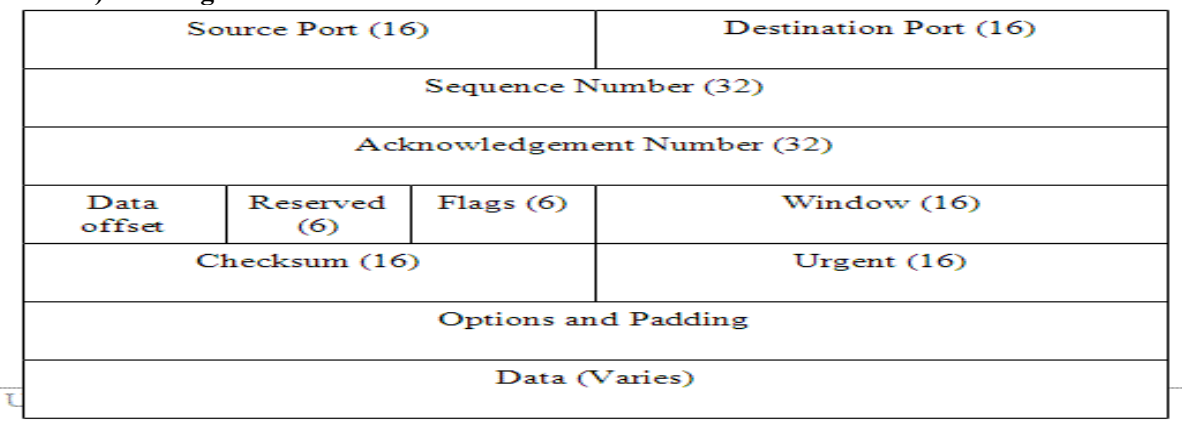
PART-B

1. Write short notes on (May/June 2012)

(i) TCP segment format

(ii) silly window syndrome (Or) discuss the silly window syndrome and explain how to avoid it.

1. **i)TCP Segment Format**:



Each TCP segment contains the header.

The **SrcPort**and **DstPort** fields identify the source and destination ports, resp. like UDP. These two fields, plus the source and destination IP addresses, combine to uniquely identify each TCP connection. TCP's demux key is given by the 4-tuple - SrcPort, SrcIPAddr, DstPort, DstIPAddr

The Acknowledgment, SequenceNum, and AdvertisedWindow fields are all involved in TCP's sliding window algorithm.

TCP is a byte-oriented protocol. So each byte of data has a **sequence number**; SequenceNum field contains the sequence number for the first byte of data carried in that segment.

The **Acknowledgment** and **Advertised Window** fields carry information about the flow of data going in the other direction.

The 6-bit Flags field is used to relay control information between TCP peers.

The flags include SYN, FIN, RESET, PUSH, URG, and ACK. The SYN and FIN flags are used when establishing and terminating a TCP connection.

Code Bits:

U	A	P	R	S	F
R	C	S	S	Y	I

URG =1 : Activates URGENT PTR field.

ACK =1 : Activates the acknowledgement field.

PSH =1 : pushes the data even before buffer fills.
RST = 1: Reset the connection.
SYN =1: Synchronize the sequence number.
FIN = 1 : Sender has reached end of its data.

The **ACK** flag is set any time the Acknowledgment field is valid, implying that the receiver should pay attention to it.
The **URG** flag signifies that this segment contains urgent data.
When this flag is set, the UrgPtr field indicates where the non urgent data contained in this segment begins.
The **PUSH** flag signifies that the sender invoked the push operation, which indicates to the receiving side of TCP that it should notify the receiving process of this fact.
The **RESET** flag signifies that the receiver has become confused—for example, because it received a segment it did not expect to receive—and so wants to abort the connection.
The **Checksum** covers the TCP segment - The TCP header and the TCP data. This is a mandatory field that must be calculated by the sender and then verified by the receiver.
A**HdrLen** field gives the length of the header in 32-bit words. This field is also known as the Offset field, since it measures the offset from the start of the packet to the start of the data.

ii) Silly window syndrome:

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.
The silly window syndrome occurs when either the sender transmits a small segment or the receiver opens the window to a small amount only. Both involve inefficient use of BW.
If neither of these two happens, then small sized segments are never introduced into the stream. But if sending appln specifically goes for invoking PUSH, then small sized segments can be introduced.
Receiver could be stopped from advertising small window and asked to wait until a space equal to *Maximum Segment Size(*MSS) is available.
This is just a partial soln, as the receiver, in no way knows how long to delay acknowledgements.
The answer is to introduce a timer and to transmit when the timer expires. Nagle introduced an elegant self-clocking solution.
The idea is that as long as TCP has any data in flight, the sender will eventually receive an ACK. This ACK can be treated like a timer firing, triggering the transmission of more data.
Nagle's algorithm provides a simple, unified rule for deciding when to transmit:
When the application produces data to send

```
if both the available data and the window ≥ MSS
        send a full segment
else
if there is unACKed data in flight
        buffer the new data until an ACK arrives
else
        send all the new data now
```

Nagle's algorithm can also be turned off by setting the TCP NODELAY option

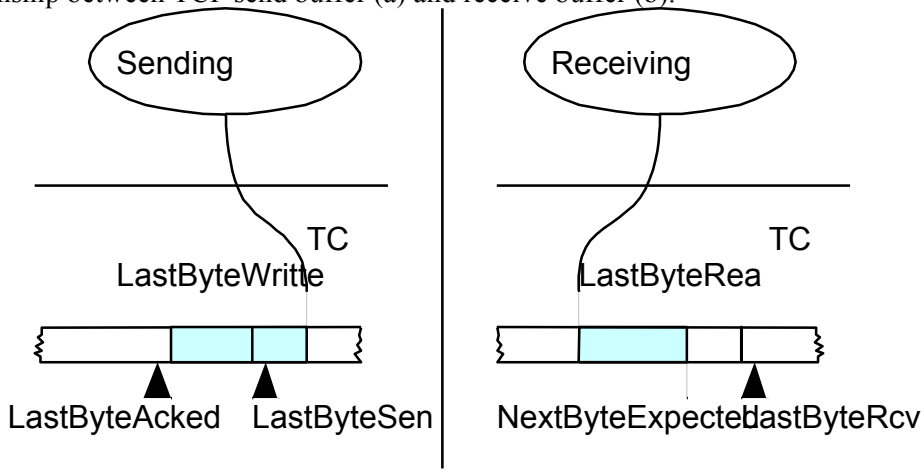
Suppose receiver buffer is full. It advertises window is zero. Effective window becomes a negative value. Sender will not transmit any data to receiver, finally sender buffer will fill. This will stop its own application program from writing in buffer.

As soon as receiver process starts to read again, its advertiser window will become > 0 that allows sender to transmit data out of its buffer. This allow sender application program to restart its writing. The sender knows this from advertised a window of size. Then the interactive application reads one character from the TCP stream. This action makes the receiving TCP happy, so it sends a window update to the sender saying that it is all right to send 1 byte. The sender obliges and sends 1 byte.

The buffer is now full, so the receiver acknowledges the 1 –byte segments but sets the window to 0. This behavior can go on forever. In applications each byte is sent as TCP segment:
1byte data + 20 byte IP header + 20 byte TCP header=41 byte => known as 'TINYGRAM' overhead is more. (- for one byte data over head is 40 byte).

2. Explain TCP sliding window algorithm for flow control.

Relationship between TCP send buffer (a) and receive buffer (b).



Sending side :

LastByteAcked< = LastByteSent
LastByteSent< = LastByteWritten
Buffers bytes between LastByteAcked and LastByteWritten

Receiving Side:

LastByteRead<NextByteExpected
NextByteExpected< = LastByteRcvd+1
Buffers bytes between NextByteRead and LastByteRcvd.
Send buffer size: **MaxSendBuffer**

Receive buffer size:**MaxRcvBuffer**

Receiving side, to avoid overflow maintains:

LastByteRcvd - LastByteRead< = **MaxRcvBuffer**

AdvertisedWindow = **MaxRcvBuffer** – **((NextByteExpected – 1) - LastByteRead**), which represents amt of free space remaining in its buffer**.**

Sending side should maintain a window at any time , equal to

LastByteSent - LastByteAcked< = **AdvertisedWindow**

EffectiveWindow at sender = **AdvertisedWindow** - (**LastByteSent - LastByteAcked**)

The local process should not overflow sender buffer. Therefore it must be of size

- **LastByteWritten - LastByteAcked**< = **MaxSendBuffer**
- Also the sender should block sending process if (**LastByteWritten - LastByteAcked**) + y >**MaxSendBuffer,**

Where y is the new byte written by sending process inside sender buffer.

Receiver may advertise a window size of 0 and still acknowledge received data.

Sender may free its buffer space, making the sender process to generate data. But sender cannot send data as the Advt.Window = 0. Eventually sender buffer fills up and it blocks the sending process.

Change of window size will not be intimated by receiver. Instead the sender should persist in sending 1 byte of data very often, for which the receiver always responds with the latest values for Acknowledge and Advt.Window. This alerts the sender about the change in window size on the receiver side, and it starts sending data.

3. Describe with examples the three mechanisms by which congestion control is achieved in TCP. (Nov/Dec 2013)

TCP maintains a new state variable for each connection, called **CongestionWindow**, which is used by the source to limit how much data it is allowed to have in transit at a given time.

TCP is modified such that the maximum number of bytes of unacknowledged data allowed is now the minimum of the congestion window and the advertised window.

Thus, TCP's effective window is as follows:

MaxWindow = MIN (CongestionWindow, AdvertisedWindow)
EffectiveWindow = MaxWindow − (LastByteSent − LastByteAcked).
Thus, a TCP source should not send faster than what the n/w or destination host can accommodate.

1) Additive Increase/Multiplicative Decrease (AIMD):

TCP source sets the congestion window based on the level of congestion it perceives to exist in the n/w. This involves decreasing the congestion window when the level of congestion goes up and increasing the congestion window when the level of congestion goes down. Taken together, the mechanism is commonly called **AIMD.**

If packets are not delivered, a timeout results, congestion is present in them. TCP interprets timeouts as a sign of congestion and reduces the rate at which it is transmitting.

Whenever timeout occurs, the source sets congestion window to half of its previous value each time – **multiplicative decrease**. Suppose now congestion window is 16 packets. If a loss is detected, congestion window is set to 8. Additional losses cause congestion window to be 4, then to 2 finally to 1.

Now how congestion window takes the advantage of newly available capacity in the network. Every time the source successfully sends a congestion window, it adds 1 packet to the congestion window.-**additive increase.** This pattern of continually increasing and decreasing congestion window continues throughout life time of the connection. If we draw congestion window as a function of time, the curve is saw tooth form.

TCP interprets timeouts as a sign of congestion and reduces the rate at which it is transmitting. Specifically, each time a timeout occurs, the source sets CongestionWindow to half of its previous value. This halving of the CongestionWindow for each timeout corresponds to the "multiplicative decrease" part of AIMD.

Suppose the CongestionWindow is currently set to 16 packets. If a loss is detected, CongestionWindow is set to 8. An additional loss cause CongestionWindow to be reduced to 4, then 2, and finally to 1 packet.CongestionWindow is not allowed to fall below the size of a single packet, or the *Maximum Segment Size (MSS)*.

Every time the source successfully sends a Congestion Window's worth of packets and gets acknowledgement for the same, it adds the equivalent of one packet to CongestionWindow.

This is the ***additive increase part*** of AIMD. In practice, TCP does not wait for an entire window's worth of ACKs to add 1 packet's worth to congestion window, but instead increments congestion window as given below:

Increment = MSS × (MSS/CongestionWindow)
CongestionWindow + = Increment

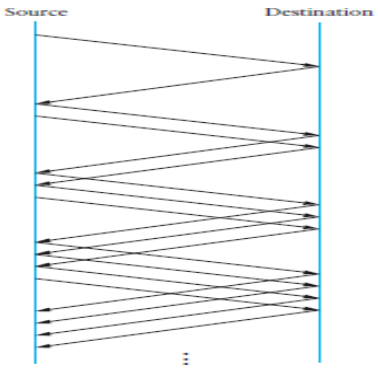


Figure 6.8 Packets in transit during additive increase, with one packet being added each RTT.

i.e., rather than incrementing congestion window by an entire MSS bytes for each RTT, we increment it by a fraction of MSS every time an ACK is received. Assuming that each ACK acknowledges the receipt of MSS bytes, then that fraction is MSS / Congestion Window. The important concept of AIMD is that the source is willing to reduce its congestion window at a much faster rate than it is willing to increase its congestion window.

The additive increase mechanism just described is the right approach to use when the source is operating close to the available capacity of the network. For a source, which has just begun from scratch, it is not suitable.

1. Slow start:

It is a congestion control technique. The additive increase mechanism is the right approach to use when the source is operating close to the available capacity of the network, but it takes too long to ramp up a connection when it is starting from scratch. TCP therefore 472 6 Congestion Control and Resource Allocation & Source Destination provides a second mechanism, ironically called *slow start*, that is used to increase the congestion window rapidly from a cold start. Slow start effectively increases the congestion window exponentially, rather than linearly. Specifically, the source starts out by setting CongestionWindow to one packet. When the ACK for this packet arrives, TCP adds 1 to CongestionWindow and then sends two packets. Upon receiving the corresponding two ACKs, TCP increments CongestionWindow by 2—one for each ACK—and next sends four packets. The end result is that TCP effectively doubles the number of packets it has in transit every RTT.

The source starts out by setting congestion window to one packet. When ACK for this packet arrives, TCP adds 1 to congestion window and then sends 2 packets. Upon receiving 2 ACK, TCP increments congestion window to be 4.

Consider the case when timeout occurs. By that time source will not transmit any more packets. After sometime, source will receive a single cumulative ACK that re opens a entire advertised window.

Now source uses slow start rather than using effective windows (i.e.) window size is 1. It uses slow start (i.e.) multiplicative increase until window size is half value of congestion window size because of what loss occurs just now. This target congestion window size is also known as threshold value. Slow start is used to rapidly increase the sending rate up to the value. Then additional increase is used beyond d this point.

Two different situations in which slow start runs:

- The first is at the very beginning of a connection, at which time the source has no idea how many packets it is going to be able to have in transit at a given time.
- The second situation, it is used is when the connection at source goes dead while waiting for a timeout to occur. This might happen when a packet is lost, source reaches a point where it has sent its entire data as specified by advertised window and it blocks for ACK to arrive, which will not arrive. Eventually a time out happens; source receives a single cumulative ACK that reopens the entire advertised window, making the source to begin slow start to restart flow of data.

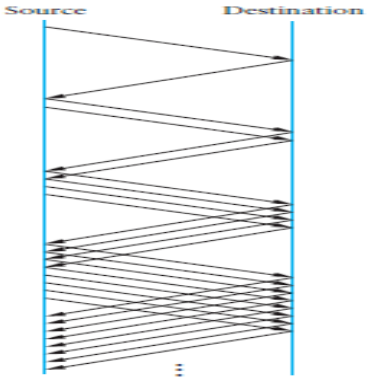


Figure 6.10 Packets in transit during slow start.

Although the source is using slow start again, it now knows more information than it did at the beginning of a connection. The source now knows the congestion window value (target congestion window value) that existed before packet loss. Due to packet loss, multiplicative decrease happened and the congestion window has now reduced to one half of what it was before. The new reduced value of congestion window is stored in a temporary variable Congestion Threshold. Source starts slow start phase, increasing exponentially till it reaches the Congestion Threshold value. After reaching, it begins Additive Increase phase begins where the congestion window size is reset to 1 packet. Now the congestion window grows linearly till it reaches the target congestion window value or till next time out.

1) Fast retransmit and fast recovery

The mechanisms described so far were part of the original proposal to add congestion control to TCP. A new mechanism called **fast re-transmit** was added to TCP. Fast retransmit is a heuristic that sometimes triggers the retransmission of a dropped packet sooner than the regular timeout mechanism. Every time a

data packet arrives at the receiving side, the receiver responds with an acknowledgment, even if this sequence number has already been acknowledged.

Thus, when a packet arrives out of order, TCP resends the same acknowledgment it sent the last time. This second transmission of the same acknowledgment is called a **duplicateACK**. Whenthe sending side sees a duplicate ACK, it knows that the other side must have received a packet out of order, which suggests that an earlier packet might have been lost. The sender waits until it sees some number of duplicate ACKs and then retransmits the missing packet. TCP waits until it has seen three duplicate ACKs before retransmitting the packet.

When the fast retransmit mechanism signals congestion, rather than drop the congestion window to 1 packet and start slow start, it is possible to use the ACKs that are still in the pipe to clock the sending of packets. This mechanism, which is called **fast recovery**, effectively removes the slow start phase that happens between when fast retransmit detects a lost packet and additive increase begins.

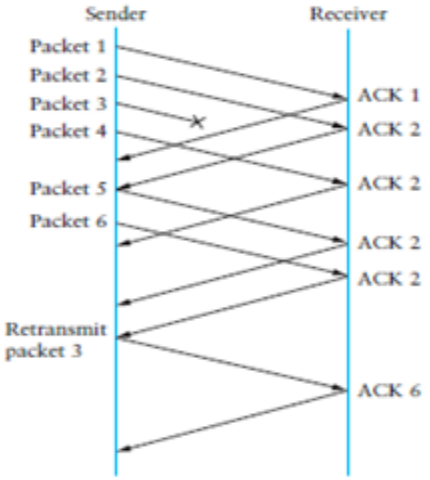


Figure 6.12 Fast retransmit based on duplicate ACKs.

4. Discuss TCP congestion avoidance algorithm in detail. (Or) DEC bit method. (Apr/May 2012)

It is a congestion avoidance technique. Each router monitors the load and explicitly notifies the end nodes when congestion is about to occur.

- If avg. queue length is >= 1, then notify.
- Notification is implemented by setting a binary congestion bit in the packets that flow thru the router.

The destination host then copies the bit into ACK, it sends to source. The source records how many of its packets resulted in some router setting the congestion bit. Source maintains a congestion window and checks what fraction of last window's packets resulted in the bit being set.Source adjusts its sending rate to avoid congestion

- If less than 50% packets/ACKs have the bit set, increase congestion window by 1
- If 50% or more packets have congestion bit set, decrease congestion window to 0.875 of previous value.

b) **Random early detection (RED)**

This method***implicitly***notifies the source of congestion by dropping one of the packets.

The gateway drops packets earlier (before its queue fills up), notifying sender to decrease its congestion window or a router drops few packets before its buffer space gets exhausted, so as to cause the source to slow down, so that it need not drop lots of packets later on.

Rather than wait for the queue to become completely full and then be forced to drop each arriving packet, we could decide to drop each arriving packet with some **drop probability** whenever the queue length exceeds some *drop level*. This idea is called **early random drop**.

RED alg defines how to monitor the queue length and when to drop a pkt.

RED computes an avg. queue length using a weighted running average.

AvgLen= (1-weight) AvgLen + weight X SampleLen

Where 0 < weight < 1 and SampleLen is length of queue when a sample measurement is made.

Two queue length thresholds, MinThreshold&MaxThreshold which trigger certain activity are defined. When a pkt arrives at gateway, RED compares the current AvgLen with these 2 thresholds as below:

i) ifAvgLen<= MinThreshold, queue the pkt.

ii) ifMinThreshold<AvgLen<MaxThreshold, calculate probability P and drop arriving pkt with probability P.

iii) ifMaxThreshold<= AvgLen, drop arriving pkt.

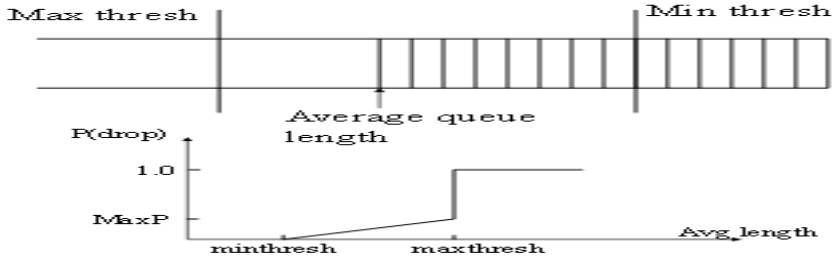
In the following graph, if AvgLen is between min & max thresholds, packets are dropped gently. When maxP is reached, all arriving pkts are dropped.

Dropping probability is a function of both AvgLen and how long it has been since the last pkt was dropped.

TempP = MaxP(AvgLen – MinThreshold) / (MaxThreshold – MinThreshold)

Just marking based on TempPcan lead to clustered dropping. (can cause multiple drop in a single connection, which is unfair, similar to tail drop). Dropping should be evenly distributed over timeline. Better to bias TempP by history of undropped packets ***P = TempP / (1 - count*TempP)***, where count equals the number of packets not dropped since the last drop.

RED operation



c)Source Based Congestion Avoidance

The general idea of these techniques is to watch for some sign from the network that some router's queue is building up and that congestion will happen soon if nothing is done about it.

Increasing RTT:

- We have seen that Timeout is considered as indication of congested state.
- Increment in RTT is an indicator of increased load in bottleneck router, which will soon reach 'congested state'.
- Sending packets in loaded state will probably only increase queue length in the bottleneck router.

TCP Vegas controls its window size based on achieved sending rate .

Step: 1

- Define ***BaseRTT*** for a given flow, to be the minimum of all RTTs when flow is not congested. That is when all Acks returns within a round trip time.
- Initially it is set to the RTT of first packet.
- If connection is not overflowing, then

Expected Rate = CongestionWindow / BaseRTT, where CongestionWindow gives the no. of bytes in transit.

Step: 2

Next we see if this rate is achieved in next RTT period.

Compute current sending rate (Actual Rate) for a distinguished packet and measure the RTT of this packet.

Record sending time of a distinguished packet and then count how many bytes have been sent to network by TCP till the acknowledgement of this distinguished packet returns. Then compute SampleRTT for distinguished packet when itsAck returned and dividing no. of bytes transmitted by SampleRTT. This calculation is done once per RTT.

Step: 3

Compute ***Diff = ExpectedRate - Actual Rate*****,** the RTT should be changed if Diff < 0.

- If Actual Rate >ExpectedRate, BaseRTT changes to NewRTT.

If Actual Rate <ExpectedRate, (Diff >=0) Change Congestion Window as follows:
Define α <β , corresponding to too little or too much extra data in the network

- If Diff < α increase cwnd linearly in next RTT
- If Diff > β decrease cwnd linearly in next RTT
- If α <Diff <β , leave cwnd unchanged.
- Therefore, if actual thruput gets farther away from expected thruput, more congestion is there in n/w, which implies that the sending rate should be reduced. Beta threshold triggers this decrease.
- If actual thruput gets too close to expected thruput, the connection is in danger of not utilizing the available BW. Alpha threshold triggers this increase.
- Overall goal is to keep BW between alpha and beta bytes in the n/w.
- This method decreases congestion window linearly in conflict with the rule that multiplicative decrease is needed to ensure stability. Multiplicative decrease is used only when time out occurs.
- Linear decrease described here is an early decrease in congestion window which hopefully happens before congestion occurs and pkts start being dropped.

5. Why does TCP uses adaptive retransmission and describe its mechanism.(Nov/Dec 2013) (Or) Illustrate the features of TCP that can be used by the sender to insert record boundaries into the byte stream. Also mention their original purpose. (Apr/May2013)

TCP uses an adaptive retransmission mechanism, as in real time RTTs may vary (even between same pair of hosts over time).

Original Algorithm

It is a simple algorithm for computing a timeout value between a pair of hosts.

When TCP sends a segment, it records time and upon receiving ACK, it records time again. Difference of these 2 times gives sample RTT.

TCP then computes an EstimatedRTT as a weighted average between the previous estimate and this new sample.

$$\text{EstimatedRTT} = \alpha \times \text{EstimatedRTT} + (1 - \alpha) \times \text{SampleRTT}$$

The parameter α is selected to smooth the EstimatedRTT. The original TCP specification recommended a setting of α between 0.8 and 0.9.

TCP then uses EstimatedRTT to compute the timeout in a rather conservative way:
TimeOut = 2 × EstimatedRTT.
It is necessary to know which transmission to associate it with so as to compute an accurate SampleRTT.

Solution:

* Do not measure sample RTT when retransmitting &
* Double timeout after each retransmission to avoid congestion

After each retransmission, set next RTO (Retransmission Timeout Policy) to be double the value of the last, rather than adopting the last estimated RTT. i.e., TCP uses Exponential backoff. This is because:
- Congestion occurs because of lost segments, where in the source reacts aggressively for each time out. Instead, the more times the connection times out, the more cautious the source should be.

2.Karn/Partridge Algorithm:

Ambiguity/difficulty in sampling - If a segment is retransmitted, it is hard to tell if the ACK is for the first transmission or another.

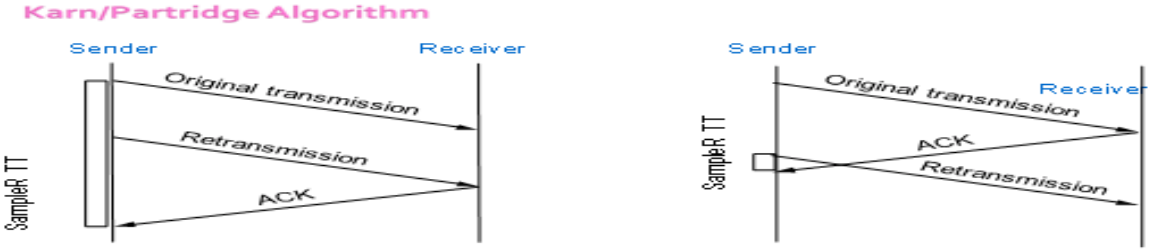
- It is necessary to know which transmission to associate it with so as to compute an accurate SampleRTT.

Assumption: packet loss is due to queue overflow (since wired links are highly reliable)
Two degenerate cases with timeouts and RTT measurements

Solution: Do not sample RTT when retransmitting
Double timeout after each retransmission to avoid congestion

- After each retransmission, set next RTO to be double the value of the last
  - Exponential backoff is well known control theory method
  - Loss is most likely caused by congestion so be careful.

- Whenever TCP retransmits a segment, it stops taking samples of the RTT; it only measures SampleRTT for segments that have been sent only once. This solution is known as the Karn/Partridge algorithm.



Associating the ACK with (a) original transmission versus (b) retransmission.

3) **Jacobson/Karels Algorithm**

These people proposed when TCP should timeout and when to retransmit a segment.

Variance in sample RTT values were not considered (in previous methods) when setting timeout value

- If variance is small, we could set RTO = EstRTT
- If variance is large, we may need to set RTO > 2 x EstRTT
- New algorithm calculates both variance and mean for RTT

Diff = SampleRTT - EstRTT
EstRTT = EstRTT + (d x Diff)
Dev = Dev + d (|Diff| - Dev)

Sample RTT is measured as usual. Initially settings for EstRTT and Dev will be given to you. Also d is a factor between 0 and 1. Typical value is 0.125.

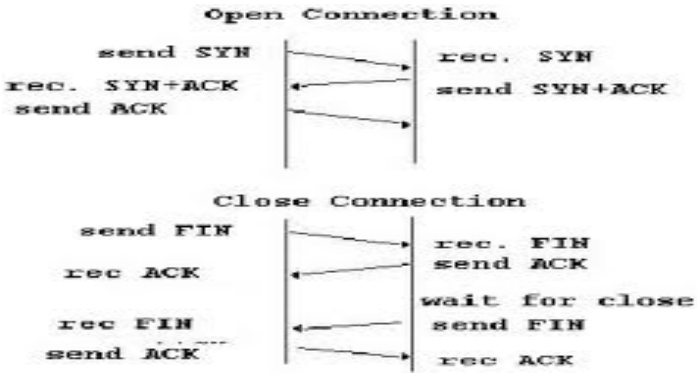
The timeout value is calculated as a function of both EstimatedRTT and Deviation as follows:

TimeOut = m x **EstRTT** + f x **Dev** where m = 1 and f = 4. (based on experience)

Thus, when variance is small, TimeOut is close to EstRTT. When variance is large Dev dominates the calculation

6.Explain connection establishment and connection closing in TCP. orDescribe how reliable and ordered delivery is achieved through TCP. (dec 2013)

Fig. TCP Connection Establishment & Termination:



- The client sends a segment to the server stating the initial sequence number it plans to use (Flags = SYN, SequenceNum = x).
- The server responds with a single segment that both acknowledges the client's sequence number (Flags = ACK, ACK = x +1) and states its own beginning sequence number, (Flags = SYN, SequenceNum = y). Both the SYN and ACK bits are set in the Flags field of this second message.
- The client responds with a third segment that acknowledges the server's sequence number, (Flags = ACK, ACK = y + 1).
- The reason that each side acknowledges a sequence number that is one larger than the one sent is that the Acknowledgment field actually identifies the "next sequence number expected".

TCP State Transition Diagram: Connection Establishment

When opening a connection, the server first invokes a passive open operation on TCP, which causes TCP to move to the LISTEN state.

At some later time, the client does an active open, which causes its end of the connection to send a SYN segment to the server and to move to the SYN_SENT state.

When the SYN segment arrives at the server, it moves to the SYN_RCVD state and responds with a SYN+ACK segment.

The arrival of this segment causes the client to move to the ESTABLISHED state and to send an ACK back to the server.

When this ACK arrives, the server finally moves to the ESTABLISHED state.

Connection Termination:

The application process on both sides of the connection must independently close its half of the connection (tear down).

If only one side closes the connection, then this means it has no more data to send, but it is still available to receive data from the other side.

On any one side there are three combinations of transitions that get a connection from the **ESTABLISHED** state to the **CLOSED** state:

1. **This side closes first:**

ESTABLISHED → FIN WAIT 1 → FIN WAIT 2 → TIME WAIT → CLOSED.

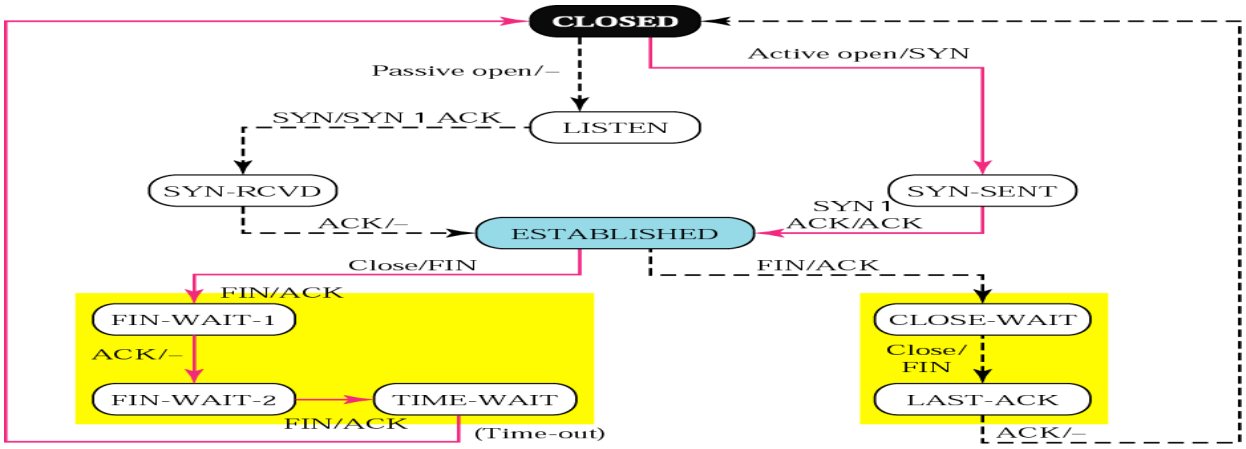
2. **The other side closes first:**

ESTABLISHED → CLOSE WAIT → LAST ACK → CLOSED.

3. **Both sides close at the same time:**

ESTABLISHED → FIN WAIT 1 → CLOSING → TIME WAIT → CLOSED.

4. Another sequence of transitions that leads to the **CLOSED** state; it follows the arc from **FIN WAIT 1** to **TIME WAIT**.



7. What is meant by QoS in networking? State the techniques to improve QoS. (Apr/May 2012)

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.Quality of service comprises requirements on all the aspects of a connection, such as service response time, loss, signal-to-noise ratio, cross-talk, echo, interrupts, frequency response, loudness levels, and so on. A subset of telephony QoS is Grade of Service (GoS) requirements, which comprises aspects of a connection relating to capacity and coverage of a network, for example guaranteed maximum blocking probability and outage probability.

The techniques to improve QoS: Scheduling, Traffic shaping, Resource reservation and Admission control.

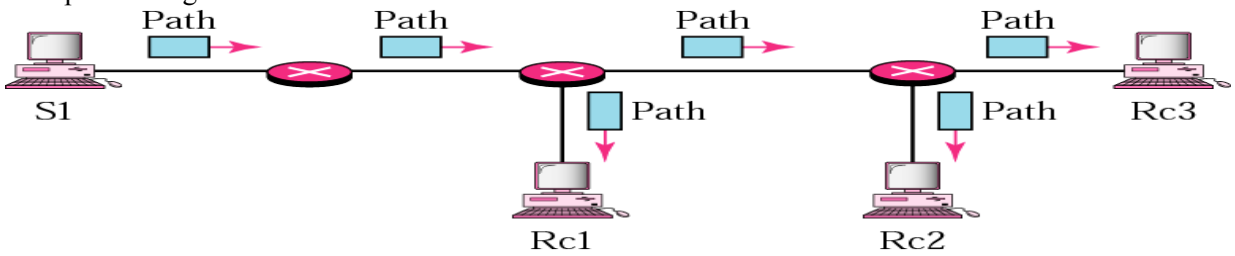
EXPLAIN

RSVP: It is a connectionless, datagram, packet switching protocol, out of which a virtual circuit should be created. This VC should be signaled before data traffic begins on it. RSVP is a signaling protocol which helps IP to create a flow and consequently make a reservation.

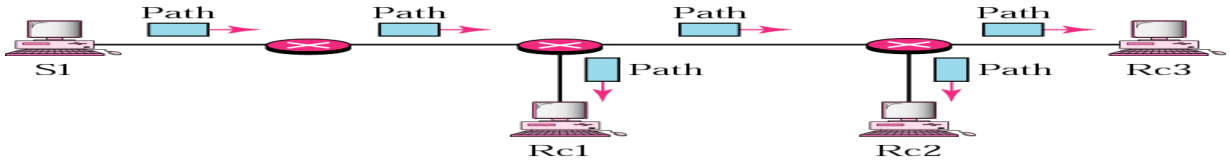
Receiver Based Reservation & Reservation Messages: Only receivers and not senders make reservations. 2 of the important messages used in making reservation are – Path &Resv.

Path Msg– Receivers in order to reserve resource should know the path travelled by packets.

A path msg, travels from source and reaches all receivers in the multicast path. On its way, it stores the information necessary for receivers. Since it is sent in multicast environment, a new message is created when path diverges.

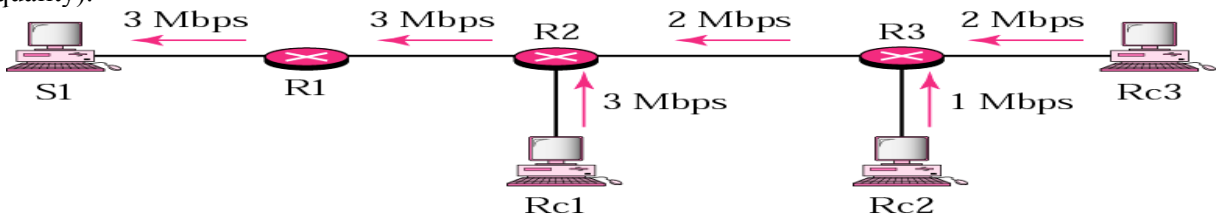


ResvMsg- After path msg is received by receiver, it sends Resv message towards sender and reserves resources on the routers that support RSVP. For those routers, which don't support RSVP, "best effort" delivery of IP is followed.



Reservation Merging

In RSVP resources are not reserved for each receiver in a flow, instead reservation is merged. In multimedia environment, different receivers may handle different grades of quality. For e.g, RC2 may be able to receive video only at 1mbps (low quality), while RC3 may be able to receive video at 2mbps (high quality).



Reservation Styles

1. **Wild Card Style**: The router makes a single reservation for all senders based on largest request. This is used when flow from different senders do not occur at same time.
2. **Fixed Filter Style**: Distinct reservation is made for each flow. This is made when flows from different senders occur at same time.
3. **Shared Explicit Style**: A single reservation made by router, which is shared by all senders.

Soft State: Flow info maintained at each router should be refreshed periodically. Default refreshing interval is 30sec.

8. Explain the significance of Clark's solution and Nagle's algorithm. (Or) What is the need for Nagle's algorithm? How does it determine when to transmit data? (Apr/May 2013)

Clark's solution is to prevent the receiver from sending a window update for 1 byte. Instead it is forced to wait until it has a decent amount of space available and advertise that instead. Specially, the receiver should not send a window update until it can handle the maximum segment size it advertised when the connection was established, or its buffer is half empty, whichever is smaller.

The sender can also help by not sending tiny segments. Instead, it should try to wait until it has accumulated enough space in the window to send a full segment or at least one containing half of the

receiver's buffer size (It must estimate from the pattern of window updates it has received in the past).

To overcome this, Nagle proposed that at any point of time there can be only one outstanding packet. Till the ack. is received, data is accumulated and on receipt of ack. Accumulated data is transmitted. N/W utilization increases. Nagle's algorithm can be turned off by setting the TCP NODELAY option

9.Discuss about queuing disciplines.

- Each router must implement some queuing discipline that governs how packets are buffered while waiting to be transmitted.
- It also directly affects the latency experienced by a packet, by determining how long a packet waits to be transmitted.
- The two common queuing algorithms are first-in-first-out (FIFO) and fair queuing (FQ).

1.FIFO:

- The first packet that arrives at a router is the first packet to be transmitted.
- Figure 6.5(a), shows a FIFO with "slots" to hold up to eight packet.
- If a packet arrives and the queue (buffer space) is full, then the router discards that packet, as shown in Figure 6.5(b).
- This is sometimes called *tail drop*
- FIFO is a *scheduling discipline*—it determines the order in which packets are transmitted.
- Tail drop is a *drop policy*—it determines which packets get dropped.

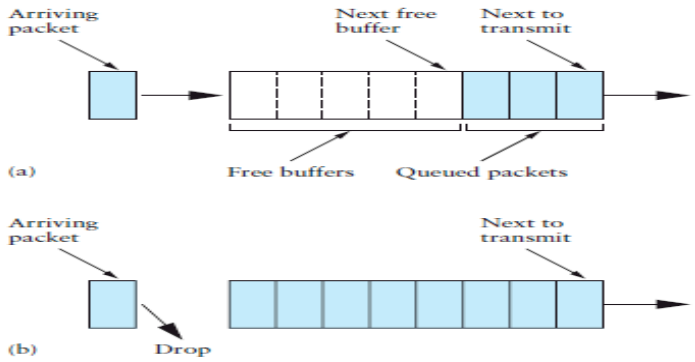
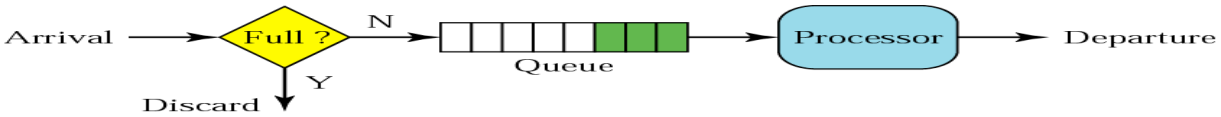


Figure 6.5 (a) FIFO queuing; (b) tail drop at a FIFO queue.



- The bundle is often referred to simply as "FIFO queuing", more precisely called as "FIFO with tail drop".
- FIFO with tail drop is most widely used in Internet routers at the time of writing.
- A simple variation on basic FIFO queuing is *priority queuing.*
- The idea is to mark each packet with a priority.
- The mark could be carried, for example, in the IP Type of Service (TOS) field.
- The routers then implement multiple FIFO queues, one for each priority class.

- The router always transmits packets out of the highest-priority queue if that queue is nonempty

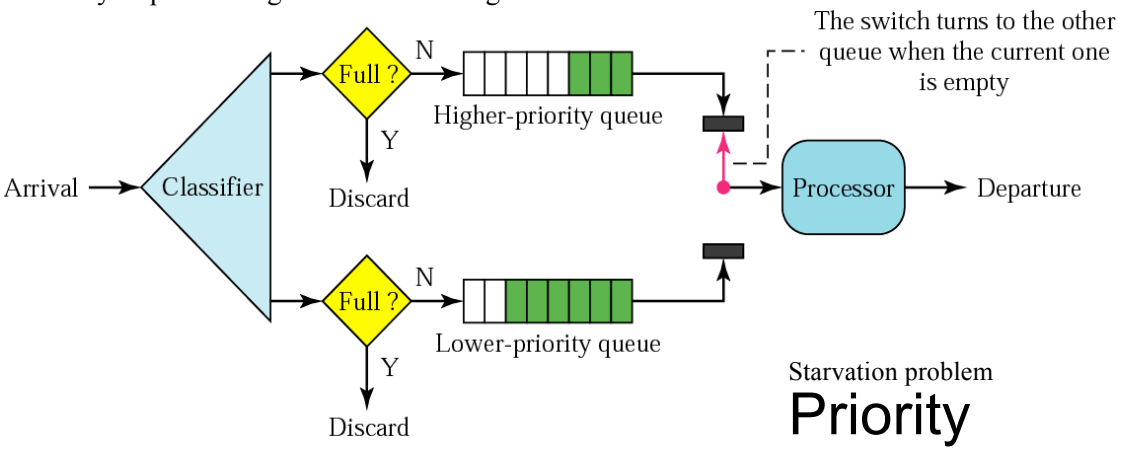
Problem - The high-priority queue can starve out all the other queues.

- ***Rectification*** - We can't allow users to set their own packets to high priority in an uncontrolled way
- Use economics—the network could charge more to deliver high priority packets than low-priority packets.
- One situation in which priority queuing is used in the Internet is to protect the most important packets—typically the routing updates.

2.FAIR QUEUING (FQ):

- The idea of FQ is to maintain a separate queue for each flow currently being handled by the router.
- The router then services these queues in a round-robin manner, as illustrated in Figure 6.6.
- When a flow sends packets too quickly, then its queue fills up.
- When a queue reaches a particular length, additional packets belonging to that flow's queue are discarded.

FQ is designed to be used in conjunction with an end -to- end congestion-control mechanism. It simply segregates traffic so that ill-behaved traffic sources do not interfere with those that are faithfully implementing the end-to end algorithm.



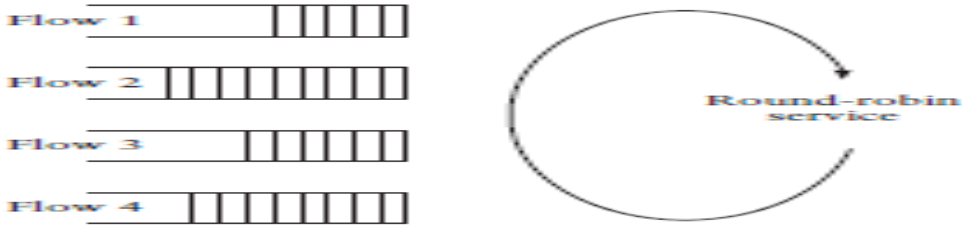


Figure 6.6 Fair queuing at a router.

10. Describe about Demultiplexing and UDP. (Dec 2012) Or If UDP does not provide any service guarantees or reliable transfer, why can't the application directly access IP and o without it? Explain UDP in detail. (8) (May 2012)

SIMPLE DEMULTIPLEXER:

- TRANSPORT PROTOCOL – Extends host-to-host delivery service into process-to-process communication service.
- When many process are running on the *given host* the protocol needs to add levels of *demultiplexing* hence allowing multiple appln processes to share the network. Eg: Internet's User Datagram Protocol.
- This protocol contains the *address* to identify the *Target* process.
- In UDP a process is identified *indirectly* using an abstract locater, often called a *portor mailbox* .
- The header for an end-to-end protocol implements this demultiplexing function.
- It contains an *identifier*(port) for both *sender* (source) and *receiver*(destination) of the message. UDP port is 16 bit long.
- The process is identified by a port on a host using a<port, host> pair. This pair constitutes the demultiplexing key for the UDP protocol.
- A client process initiates a message exchange with a server process. Once a client has connected to a server, the server knows the client's port and replies to it.

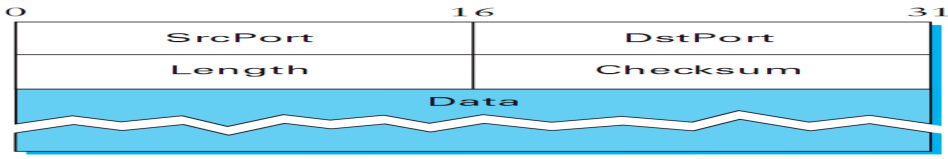


Figure 5.1 Format for UDP header.

- UDP ensures the correctness of the message using *CHECKSUM*. UDP computes its checksum over the UDP header, contents of message body, and *pseudoheader*.
- The pseudoheader consists of three fields from the IP header---protocol number, source IP address and destination IP address plus the UDP length field (which is included twice in checksum calculation).
- The pseudoheader is used to check whether the message is delivered between 2 endpoints.
- For eg, if the destination IP address *was modified* while the packet was in transit , causing the packet to be misdelivered , this fact would be *detected* by *UDPchecksum*.

The problem is the client learns the server's port in the first place.

- A common approach is for the server to accept msgs at a *well-known port*.
- Server will receive the message only from the well-known port no 911.

Domain Name Server----port 53
Mail service -----port 25.
Unix talk prog----port 517.

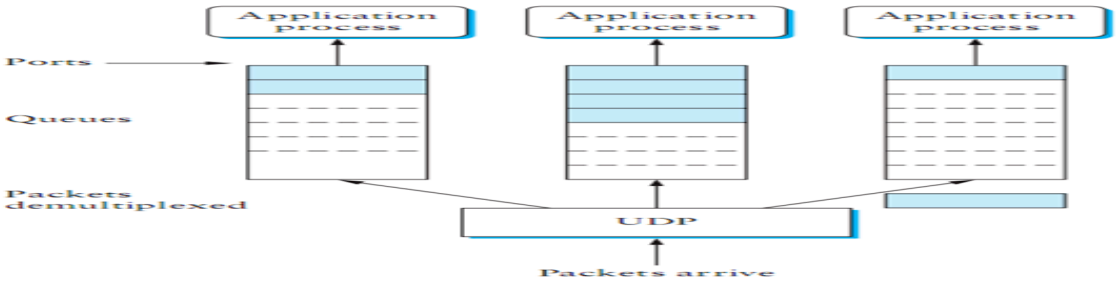
- Sometimes the well-known port is the starting point for communication. The client and server uses the *well-known port* to agree on some other port that they will use for subsequent commn, leaving the well-known port free for other clients.

PORT MAPPER: The client would *send the message* to a "port mapper" service functioning at the server's well known port asking for the port it should talk to.

- This returns the appropriate port. This makes each host to use *different port* for the same service.
- The port is purely an abstraction. It varies from system to system and from OS to OS.

- A port is implemented by a *message Queue*. When a message arrives the protocol appends the message to the end of the queue.
  - When the *queue is full* the message is discarded. There is *no control flow mechanism* that tells the sender to slow down.
- An appln process retrieves process from *the top of the queue*. If the queue is *empty*, the *process blocks* until a message becomes available.

UDP Message queue



UNIT – V

PART A

1. Why do we need a Domain Name System? What role does the DNS Resolver play in the DNS system? (Nov/Dec 2012)

Domain Name System can map a name to an address and conversely an address to name. The Domain Name System converts domain names into IP numbers. IP numbers uniquely identify hosts on the Internet: however they are difficult to remember. We therefore need a memorable way of identifying hosts. A DNS Resolver is responsible for making requests of the local DNS server in behalf of clients. A DNS Resolver must know the IP address of at least one DNS server. It uses this address to start the DNS Lookup process.

2. What are the four main properties of HTTP?

- Global Uniform Resource Identifier.
- Request-response exchange.
- Statelessness.
- Resource metadata.

3. What are the four groups of HTTP Headers? What are the two methods of HTTP?

The four groups of HTTP headers are

- General headers
- Entity Headers
- Request Headers
- Response Headers.

Two methods of HTTP are

- GetMethod( )
- PostMethod( ).

4. What is WWW and SMTP? (Nov/Dec 2010,May/June 2014))

World Wide Web is an internet application that allows user to view pages and move from one web page to another. It helps to store and share data across varied distances. The TCP/IP protocol that 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.

5. What is PGP? (Nov/Dec,2010 Apr/May 2012,May/June 2014)

Pretty Good Privacy (PGP) is used to provide security for electronic mail. It provides authentication, confidentiality, data integrity, and non repudiation. It is a program using public key encryption popularly used with email.

6. What are the transmission modes of FTP?

- Stream mode: Default mode and data is delivered from FTP to TCP as a continuous stream of data.
- Block mode: Data is delivered from FTP to TCP in terms of blocks. Each data block follows the three byte header.
- Compressed mode: File is compressed before transmitting if size is big. Run length encoding method is used for compression.

7. Why is an application such as POP needed for electronic messaging? (Apr/May 2012)

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. 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.

8. What are the TCP connections needed in FTP?

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. Compare the HTTP and FTP.

FTP	HTTP

FTP transfers the file from client to server and server to client.	HTTP transfer the file from server to client.(i.e. web pages)
It uses two different port connections. (i.e. port 20 and port 21)	HTTP use only one port connection. (i.e. Port 80)
FTP uses two parallel TCP connections to transfer a file. They are Control Connection and Data connection.	It also uses TCP protocol.
Out – of – band	In – band

10. What is the use of MIME Extension?(Nov/Dec 2014)

Multipurpose Internet Mail Extensions (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.

MIME converts binary files, executed files into text files. Then only it can be transmitted using SMTP.

11. Which protocol support email and give details about that protocol? What are the basic functions of e-mail?

SMTP is a standard protocol for transferring mails using TCP/IP

- SMTP standardization for message character is 7 bit ASCII
- SMTP adds log info to the start (i.e.) path of the message.

Basic functions of e-mail: composition, Transfer, Reporting, Displaying, and Disposition.

12. What is POP3?

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.

13. What is IMAP?

Internet Message Access Protocol (IMAP) is a standard protocol for accessing e-mail from your local server. IMAP 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.

14. What is use of digital signature?

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. Data appended to, or a data unit that allows a recipient of the data unit to prove the source and integrity if the data unit and protect against forgery.

15. What is a URL, web browser and rlogin?

- Uniform Resource Locator is a string identifier that identifies a page on the World Wide Web.
- Web browser is a software program that interprets and displays the contents of HTML web pages.
- Remote login or rlogin is used to login into remote system and access its contents.

16. Discuss the three main division of the domain name space. (Apr/May 2012)

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.

17. Name four factors needed for a secure network?

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.

18. Define SNMP. (May/June 2012)

Simple Network Management Protocol (**SNMP**) is an "Internet-standard protocol for managing devices on IP networks". Devices that typically support SNMP include routers, switches, servers, workstations, printers, & modem. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

19. What is meant by cryptography? (Nov/Dec 2012)

Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. 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.

20.ExplainCyberSquatting.

The practice of registering a domain only to turn around and sell it off to an interested party at a much higher price even has a name. It is called cybersquatting.

21. Define Name Resolution.

To improve reliability, some of the name servers can be located outside the zone. The process of looking up a name and finding an address is called name resolution.

22. Explain Email.

E-mail (electronic mail) is the exchange of computer-stored messages by telecommunication. Email messages are usually encoded in ASCII text. The architecture of the email system consists of two kinds of subsystems: the user agents, which allow people to read and send email, and the message transfer agents, which move the messages from the source to the destination.

23. What is Telnet?(May/June2014)

A Telnet 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:

- The concept of a network virtual terminal
- The principle of negotiated options
- A symmetric view of terminals and processes.

Telnet is the standard TCP/IP protocol for virtual terminal service.

24. What if TFTP?

Trivial file transfer protocol is designed for transferring bootstrap and configuration files. It is so simple and can fit into ROM of a disc less memory. TFTP does reading and writing of files.

Reading means copying files from server site to client site and writing in FTP means copying a file from client site to server site.

25. Describe why HTTP is defined as a stateless protocol.

Maintaining state across request – Response connections significantly increases the initial interactions in a connections since the identity of each party needs to be established and any saved state much be retrieved. HTTP is therefore stateless to ensure that internet is scalable since state is not contained in a HTTP request / response pairs by default.

26. List the two types of DNS message.

There are two types of DNS messages,

- Query
- Response

Query message – consists of the header and question records.

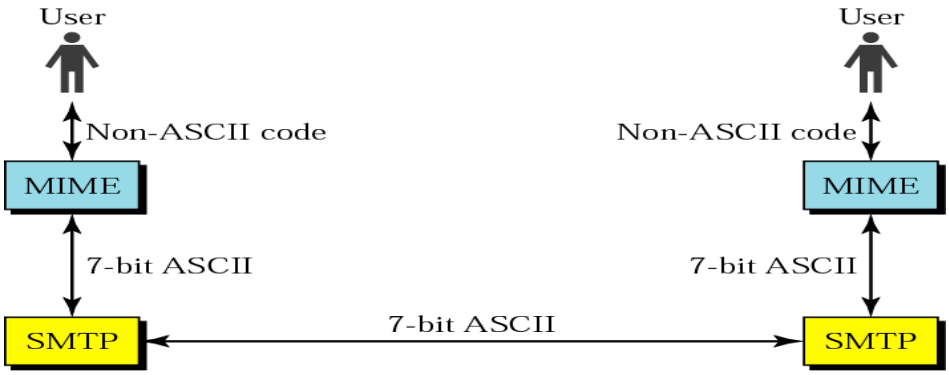
Response message – consists of header, question record, authoritative record and additional record.

PART B

1. **Discuss how the Simple Mail Transfer Protocol (SMTP) is useful in electronic mail. (Apr/May 2012/Nov/Dec 2013)**

It has 2 parts – header & Body, both represented in ASCII. The pure text content of body has been augmented by MIME to carry all sorts of data. Even that data is encoded in ASCII form as SMTP allows only ASCII characters.

Msg Hdr contains a series of CRLF(carriage return & line feed) terminated lines. Hdr is separated from body by a blank line.



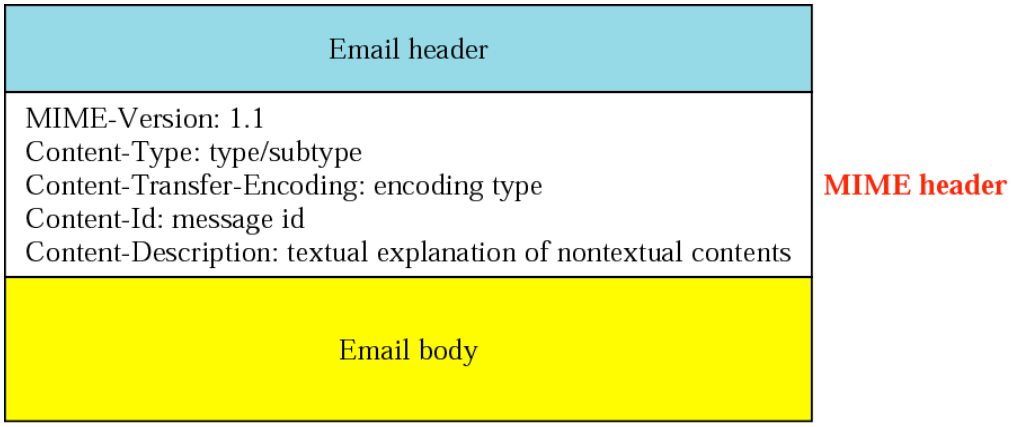
Each hdr contains a type & value separated by a colon. For eg., TO: Hdr identifies msg recipient, SUBJECT: hdr refers to the purpose of the msg, FROM: refers to user who is sending msg etc.

Some hdrs like DATE, RECEIVED(each mail server that handled this msg) are filled by in by underlying mail delivery s/m.

MIME- Multipurpose Internet Mail Extensions

Using MIME contents other than text like audio, video, pictures can be included inside msg body.

MIME header contents are shown below:



Message Transfer

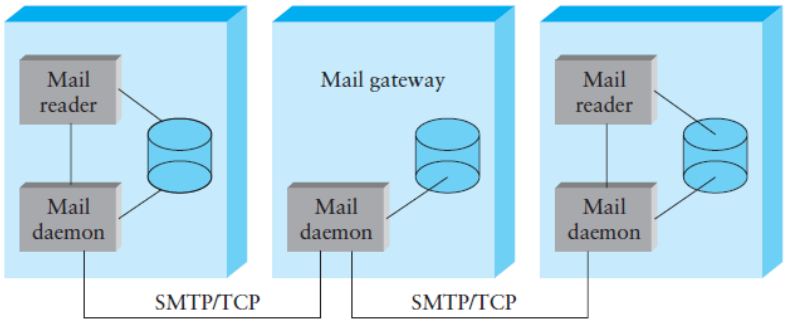
SMTP is the mail transfer protocol. The following are its key players:

i. Mail Reader: It's a s/w appln with which users interact while composing, filing, searching and reading their mails.

ii. Mail Daemon: A back ground process, running on each host. It receives mail from sender, using SMTP, running over. TCP, the daemon transmits the msg to another daemon running on another machine. The daemon also puts the incoming msgs into user's mail box.

The mail traverses thru a no. of mail gateways which buffer the msgs on disk and try to retransmit the msg to next m/c for several days. The mail daemon and mail gateways have send mail s/w pgm installed on them.

While the send mail program on a sender's machine establishes an SMTP/TCP connection to the send mail program on the recipient's machine, the mail traverses one or more *mail gateways* on its route from the sender's host to the receiver's host. Gateways run a send mail process. These intermediate nodes are called "gateways". since their job is to store and forward email messages. An "IP gateway" are referred to as a router stores and forwards IP datagrams.



Advantages of Mail Gateways

The mai l recipient will not include the host on which he reads emails in his addr. The forwarding gateways, in turn maintain a database that maps users in to the m/c on which they currently want to receive their mail. The sender need not be aware of this specific name. The list of **RECEIVED** hdr lines in the msg helps to trace the mail gateways that a given msg traversed.

Also the recipient's m/c may not be always up, in which case the mail gateway stores the msg until it can be delivered.

Independent of how many gateways are in the path, an independent SMTP conn. is used between each host to move the msg closer to recipient.

Each SMTP session involves a dialog between 2 mail daemons, with one acting as client and other as server.

The following is an exchange between sending host cs.princeton.edu and receiving host cisco.com.

In this case, user Bob at Princeton is trying to send mail to users Alice and Tom at Cisco.

Extra blank lines have been added to make the dialog more readable.

For e.g., mail delivered to Bob@cs.princeton.edu is first

sent to a mail gateway in the CS Department at Princeton (i.e., to the host named cs.princeton.edu),

Then forwarded—involving a second SMTP/TCP connection—to the specific machine on which Bob happens to be reading his email today.

The forwarding gateway maintains a database that maps users into the machine on which they currently want to receive their mail.

The sender need not be aware of this specific name.

The recipient's machine may not always be up. So the mail gateway holds the message until it can be delivered.

Each SMTP session involves a dialog between the two mail daemons, with one acting as the client and the another as the server.

Multiple messages might be transferred between the two hosts during a single session.

SMTP example: The following is an exchange between sending host cs.princeton.edu and receiving host cisco.com. User Bob at Princeton is trying to send mail to users Alice and Tom at Cisco.

HELO cs.princeton.edu
250 Hello daemon@mail.cs.princeton.edu [128.12.169.24]
MAIL FROM:<Bob@cs.princeton.edu>
250 OK
RCPT TO:<Alice@cisco.com>
250 OK
RCPT TO:<Tom@cisco.com>
550 No such user here
DATA
354 Start mail input; end with <CRLF>.<CRLF>
Blah blah blah.....etc.
<CRLF>.<CRLF>
250 OK
QUIT

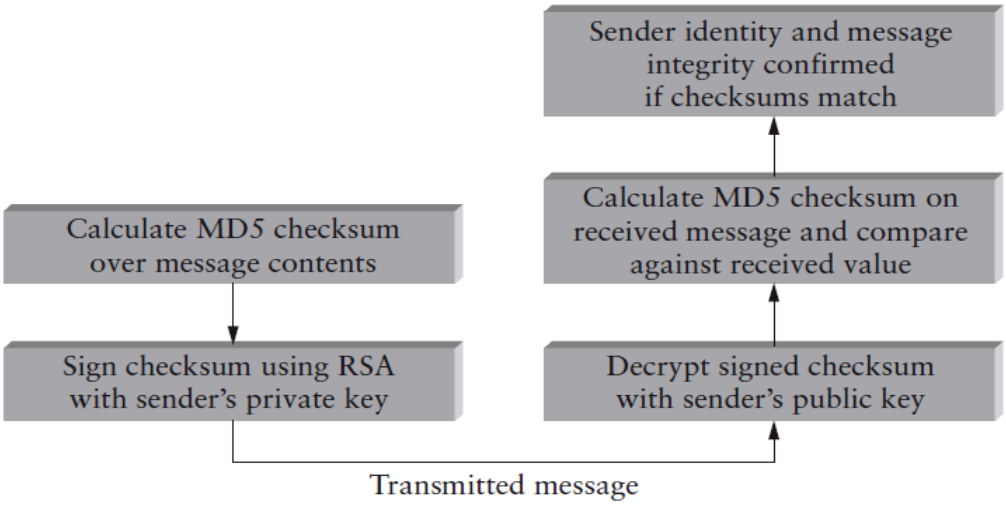
221 Closing connection
SMTP involves a sequence of exchanges between the client and the server.
In each exchange, the client posts a command (e.g., HELO, MAIL, RCPT, DATA, QUIT) and the server responds with a code (e.g., 250, 550, 354, 221).
The server returns a human-readable explanation for the code (e.g., No such user here).
For e.g., the client first identifies itself to the server with the HELO command. It gives its domain name as an argument.
The server verifies that this name corresponds to the IP address being used by the TCP connection.
The server states this IP address back to the client.
The client then asks the server if it is willing to accept mail for two different users.
The server responds by saying "yes" to one and "no" to the other.
The client sends the message, which is terminated
by a line with a single period (".") on it.
Finally, the client terminates the connection.
The mail daemon parses the message to extract the information it needs to run SMTP.
The information it extracts is said to form an *envelope* for the message.
The SMTP client uses this envelope to parameterize its exchange with the SMTP server.

2. Write in detail about PGP.

- Popular approach to providing Encryption and Authentication capabilities for electronic mail. PGP acknowledges that each user has his own set of criteria by which he wants to trust keys certified by someone else and provides the tools needed to manage the level of trust he puts in these certificates.
- E.g. Consider A, a person you know well, gives you his public key in person.
- If A gives you a certificate for B, signed by A, you might have to wonder

whether, A is the type of person that would falsely sign a certificate in exchange for money, he was a bit sloppy in checking that it really was B and not someone else who asked him to sign the certificate.

- You might trust A to sign certificates for some people (e.g., his co-workers) but not others (e.g., politicians).
- Privacy Enhanced Mail (PEM) done in an earlier secure email system forces a rigid hierarchy of Certification.
- PGP allows,
- Certification relationships to form an arbitrary mesh.
- user to decide for themselves how much trust they wish to place in a given certificate.
- For example,
- You have a certificate for B provided by A and assign a moderate level of trust to that certificate.
- Additional certificates for B that were provided by C and D, each of whom are also moderately trustworthy, that might considerably increase your level of confidence that the public key you have for B is valid.
- PGP recognizes that the problem of establishing trust is quite a personal matter and gives users the raw material to make their own decisions, rather than assuming that they are all willing to trust in a single hierarchical structure of Cas.
- PGP has become quite popular in the networking community, and PGP key signing parties are a regular feature of IETF meetings.



- At these gatherings, an individual can
- Collect public keys from others whose identity he knows
- Provide his public key to others
- Get his public key signed by others, thus collecting certificates that will be persuasive to an increasingly large set of people
- Sign the public key of other individuals, thus helping them build up their set of certificates that they can use to distribute their public keys
- Collect certificates from other individuals whom he trusts enough to sign keys
- PGP stores a set of certificates with varying degrees of trust in a file called a key ring.

⊡ If they agree, B knows that A sent the message and that it was not modified after A signed it.

⊡ In addition PGP tells B the level of trust that he had previously assigned to this public key, based on the number of certificates he has for A and the trustworthiness of the individuals who signed the certificates.

3. Describe about Secure Shell (SSH).

The Secure Shell (SSH) provides a remote login service and is intended to replace the less secure Telnet and rlogin programs used in the early days of the Internet.

- It can also be used to remotely execute commands and transfer files, like the Unix rsh and rcp commands

➢ SSH is most often used to provide strong client/server authentication.
➢ But it also supports message integrity and confidentiality.
➢ Consider that a few short years ago telecommuters used dial-up modems to connect their home computers to work (or school).

- This meant that when they logged in, their passwords were sent in the clear over a phone line and the LAN at work.
- Sending your password in the clear over a LAN isn't a great idea, but at least it's not as risky as sending it across the Internet.
- Today, however, telecommuters often subscribe to ISPs that offer high-speed cable modem or DSL service, and they go through these ISPs to reach work.
- This means that when they login, both their passwords and all the data they send or receive potentially passes through countless untrusted networks.
- SSH provides a way to encrypt the data sent over these connections and to improve the strength of the authentication mechanism they use to login.
- The latest version of SSH, version 2, consists of three protocols:

- SSH-TRANS: a transport layer protocol
- SSH-AUTH: an authentication protocol
- SSH-CONN: a connection protocol

- SSH-TRANS provides an encrypted channel between the client and server machines.
- It runs on top of a TCP connection.
- Any time a user uses SSH to log onto a remote machine, the first step is to set up an SSH-TRANS channel between those two machines.
- The two machines establish this secure channel by first having the client authenticate the server using RSA.
- Once authenticated, the client and server establish a session key used to encrypt any data
- SSH-TRANS includes a message integrity check of all data exchanged over the channel.

MAIN ISSUE:

How the client came to possess the server's public key that it needs to authenticate the server?

- The server tells the client its public key at connection time.
- The first time a client connects to a particular server, SSH warns the user that it has never talked to this machine before and asks if the user wants to continue.
- SSH then remembers the server's public key, and the next time the user connects to that same machine, it compares this saved key with the one the server responds with.
- If they are the same, SSH authenticates the server. If they are different, however, SSH again warns the user that something is amiss, and the user is then given an opportunity to abort the connection.

- Once the SSH-TRANS channel exists, the next step is for the user to actually log onto the machine.

THREE MECHANISMS TO AUTHENTICATE TO THE SERVER:

First, since the two machines are communicating over a secure channel, it is OK for the user to simply send his or her password to the server.

- The *second mechanism* uses public key encryption.

This requires that the user has already placed his or her public key on the server.

- The *third mechanism*, called host-based authentication, basically says that any user claiming to be so-and-so from a certain set of trusted hosts is automatically believed to be that same user on the server.
- Host-based authentication requires that the client *host authenticate* itself to the server when they first connect
- However, what sometimes makes SSH a challenge to understand is all the keys a user has to create and manage, where the exact interface is operating system Dependent.

- Finally, SSH has proven so useful as a system for securing remote login that it has been extended to also support other insecure TCP-based applications, such as XWindows and IMAP mail readers.
- SSH runs these applications over a secure"SHH tunnel."
- This capability is called *port forwarding, and it uses the SSH-CONN* protocol.
- The idea is illustrated in Figure 8.15, where we see a client on host A indirectly communicating with a server on host B by forwarding its traffic through an SSH connection.
- The mechanism is called port forwarding - when messages arrive at the well-known SSH port on the server, SSH first decrypts the contents, and then "forwards" the data to the actual port at which the server is listening.

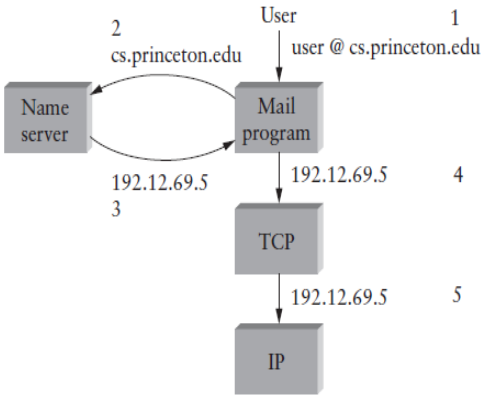
4. Explain the role of a DNS on a computer network, including its involvement in the process of a user accessing a web page. (Apr/May 2013)

An unique name is assigned to each host in a n/w. There should be a naming service to map such user friendly names to router friendly addresses. In the past, mapping of IP addresses was static using

a host file, hosts.txt maintained by a central authority called N/W Information Center (NIC). New sites are added to hosts.txt by sending email to NIC which in turn forwarded the modified contents of hosts.txt to every site.

At each site, the sys.admin saved the table on every host in their sites. Name resoln. was implemented by a procedure that looked up at hosts name in the local copy of the table and returned corresponding address. As Internet grew, this became impossible in today's dynamic environment

Domain Name System (DNS) was created to divide mapping information to be stored on multiple computers to be accessed when needed

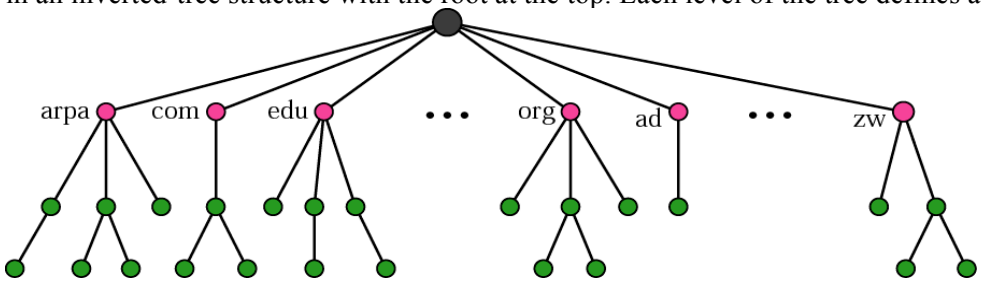


Domain Name Hierarchy

DNS names are processed from left to right and use periods (.) as separators.

DNS hierarchy is not very wide at the first level. There are domains for each country, plus the big six domains - .edu, .com, .gov, .mil, .org, .net. Additional domains have been introduced at top level that include - .biz, .coop & .info.

Domain Name Hierarchy is a structure for organizing the name space in which names are defined in an inverted-tree structure with the root at the top. Each level of the tree defines a hierarchical level.



Domain Names

Full domain name is a sequence of labels separated by dots (.) Fully qualified domain name (FQDN) contains the full name of a host

cis.usouthal.edu.

Partially qualified domain name (PQDN) does not include all the levels between host and root node. Resolver supplies the suffix to create an FQDN.

Domains may be divided into subdomains.

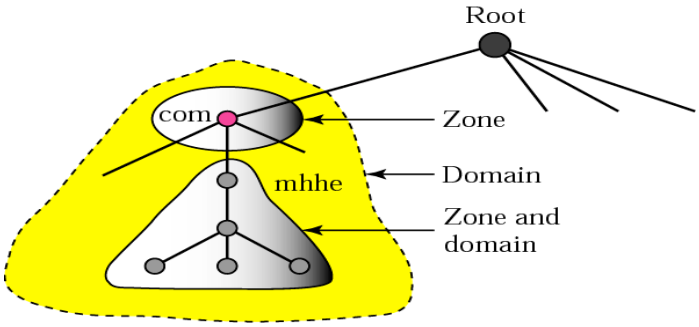
Name Servers

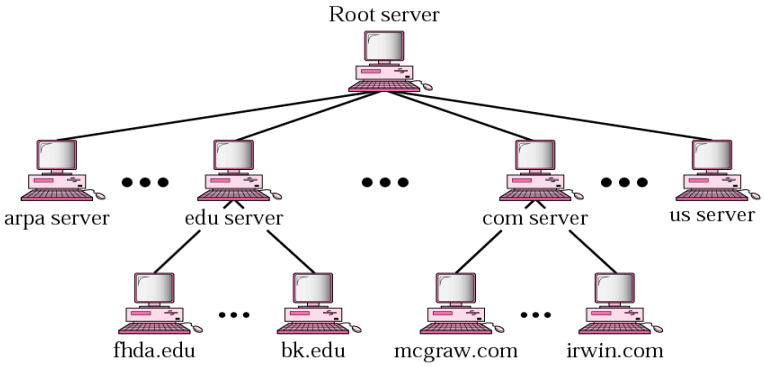
Complete domain name hierarchy exists only in the abstract format. The first step is to partition the hierarchy into subtrees called zones. Each zone could be an administrative authority responsible for that portion of the hierarchy.

Information contained in each zone is implemented in 1/2 name servers. Each name server in turn is a program that can be accessed over Internet. Clients send queries to name servers, which respond with requested info. Response may be final answer for client or pointer to another server,

to which the client should query next. Therefore from an implementation point of view, DNS is represented as **hierarchy of name servers** rather than as hierarchy of domains.
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
Name – Domain name in request.
Value – Address returned.
Type – specifies how value should be interpreted. It could be:

i. A – indicates value is an IP addr.

ii. NS – Value field gives domain name for a host which runs a name server for resolving names within specified domain.

iii. MX – Value field gives domain name for a host, running a mail server that accepts msgs foe the specified domain.

iv. Cname – Value field gives the canonical name for a particular host. It is used to define aliases which are convenient names for machines, which may be used to provide a level of indirection.

Name Resolution

Mapping a name to an address or an address to a name. Resolver is a DNS client used by an address to provide mapping.
In recursive resolution, the client sends its request to a server that eventually returns a response
In iterative resolution, the client may send its request to multiple servers. Caching may be used to store information in memory to speed up resolution.

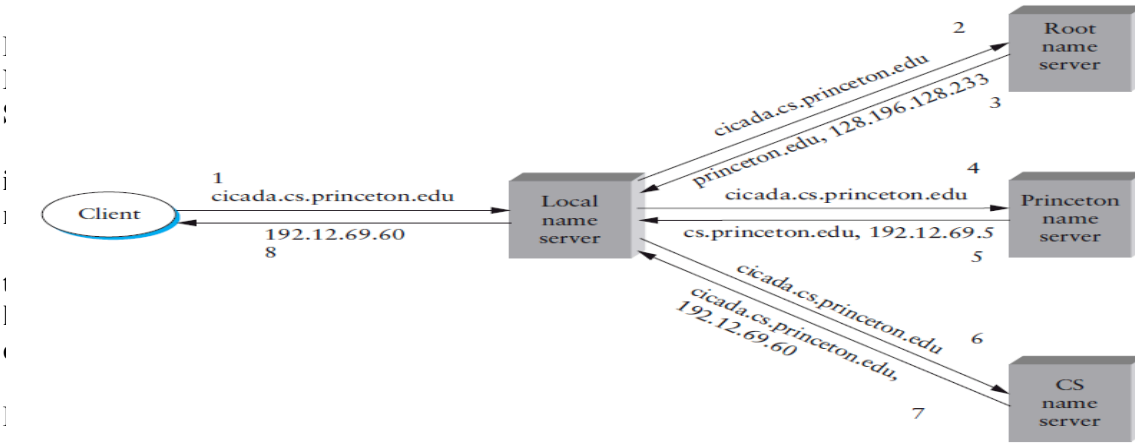
Outline Steps:

1. Client queries the local name server, which relays the request to a root name server.
2. Root server is unable to match entire name, returns the best match it has – the NS record for edu that points to the top level domain server a3.nstld.com. It has also sends an A record with an IP addr.
3. The local name server passes on the query to each server returned as response, till the final result is obtained, which is passed back to the client.

The info about root server is known to local name server, which will now act as client in extracting the response from each server till it got the final response.

Advantage of such model is that all hosts in Internet do not have to be kept up to date on where the current root servers are located. Only the local server have to know about root servers.

2nd advantage is the local server views results of all queries posted by all clients which it caches for future resolving. TTL field in resource records returned by remote servers indicate the validity of info cached.



t

ernet

Domain name space is divided into three sections: generic, country and inverse

Generic domains define hosts by generic behavior

Country domains are also used to identify national designations

Inverse domain is used to map an address to a name (address-to-name resolution)

Encapsulation

DNS uses either UDP or TCP to send request, response messages using a well-known port no. 53. UDP for messages less than 512 bytes Otherwise uses TCP

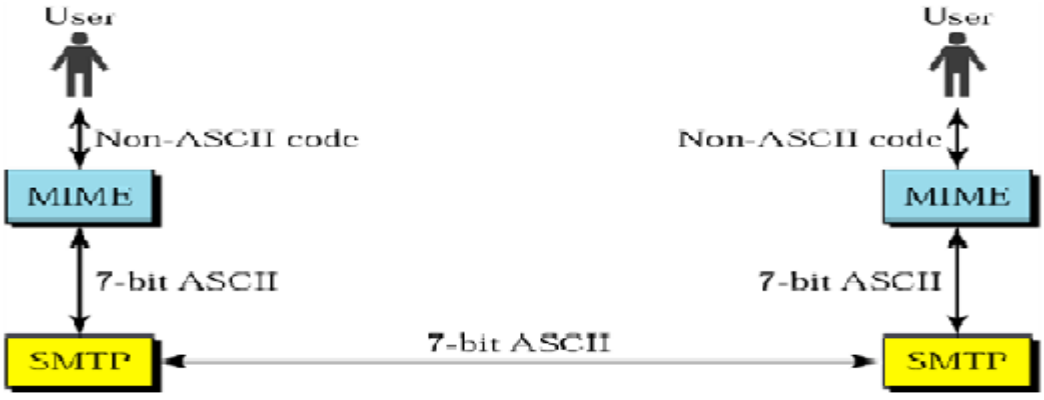
5. Discuss about MIME, IMAP and POP3.

Understanding how email works requires understanding the difference between

* User interface(mail reader) and message transfer protocol(SMTP)

* SMTP and Companion protocol(MIME).

Message Format: It has 2 parts – header & Body, both represented in ASCII. The pure text content of body has been augmented by MIME to carry all sorts of data. Even that data is encoded in ASCII form as SMTP allows only ASCII characters.



Msg Hdr contains a series of CRLF (carriage return & line feed) terminated lines. Hdr is separated from body by a blank line.

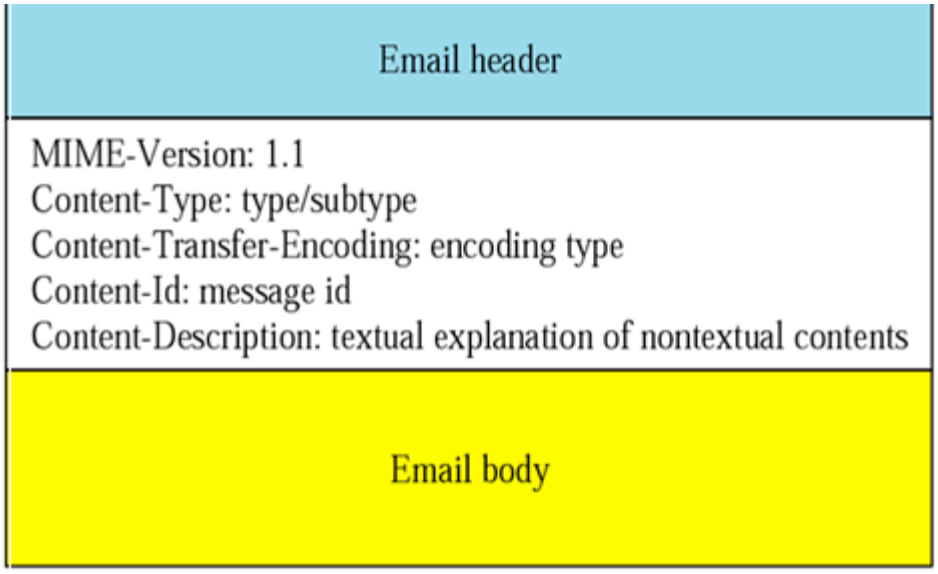
Each hdr contains a type & value separated by a colon. For eg., TO: Hdr identifies msg recipient, SUBJECT: hdr refers to the purpose of the msg, FROM: refers to user who is sending msg etc.

Some hdrs like DATE, RECEIVED(each mail server that handled this msg) are filled by in by underlying mail delivery s/m.

MIME- Multipurpose Internet Mail Extensions

Using MIME contents other than text like audio, video, pictures can be included inside msg body.

MIME header contents are shown below:



Type	Subtype	Description
Text	Plain	Unformatted text
Multipart	Mixed	Body contains ordered parts of different data types
	Parallel	Same as above, but no order
	Digest	Similar to mixed, but the default is message/RFC822
	Alternative	Parts are different versions of the same message
Message	RFC822	Body is an encapsulated message
	Partial	Body is a fragment of a bigger message
	Ext. Body	Body is a reference to another message
Image	JPEG	Image is in JPEG
	GIF	Video is in GIF format
Video	MPEG	Video is in MPEG format
Audio	Basic	Single-channel encoding of voice at 8 KHz
Application	PostScript	Adobe PostScript
	Octet-Stream	General binary data (8-bit bytes)

These different types of MIME contents (audio, video, pictures etc) need to be encoded in ASCII format before being transmitted.

This is because, email msgs pass thru many intermediate s/ms which think msg contains only ASCII. Characters other than ASCII get corrupted by such s/ms . This could be addressed by **content transfer encoding** sub header of MIME.

Content-transfer encoding Table

Category	Description
Type	ASCII characters and short lines
7bit	Non-ASCII characters and short lines
8bit	Non-ASCII characters with unlimited-length lines
Binary	6-bit blocks of data are encoded into 8-bit ASCII characters
Base64	Non-ASCII characters are encoded as an equal sign followed by an ASCII code

6. Explain about HTTP. Give their uses, state strengths and weaknesses. (Nov/Dec 2010, Nov/Dec 2013)

The web contains a set of cooperating clients & servers, speaking the same language HTTP. Users are exposed to web thru a graphical client pgm / web browser.

All web browsers have a function, allowing the user to open a URL, which provides info about the location of objects on the web.

On opening an URL, web browser opens a TCP connection to web server and retrieves the specified page. Such pages may contain text, images, sounds, video etc. Some may include URLs pointing to other files, which may be internal / external.

Such embedded URLs are called **hyperlinks,** clicking upon, opens a new connection and displays a new file. This is called "following a link".

HTTP is a text oriented protocol. General format of HTTP msg is:

Start_Line <CRLF>
Msg_Hdr <CRLF>
<CRLF>
Msg_Body <CRLF>

- Start_Line specifies Request / response msg. If request, it identifies a remote procedure to be executed. If response, it specifies status of request.
- Msg_Hdr specifies a collection of options & parameters that qualify the req / resp. It could be 0 or more lines, terminated by a blank line.
- HTTP defines many hdrs pertaining to req & resp, some pertaining to data carried in the msg body.
- Msg_Body is empty for req msg and for resp, it contains the requested contents

Request message

HTTP req specifies 3 things: operation to be performed, the web page the operation should be performed on, HTTP version.

Possible HTTP operations:

* GET- Fetches specified web page.
* Head – Fetches status info about specified web page, used to test the validity of link / to see if a page has been modified since the browser last fetched it.

An absolute URL could be specified as : GET http:// www.cs.princeton.edu/index.html. Alternatively a relative identifier can be used thru which host name could be specified in one of Msg_Hdr as shown: GET index.html HTTP/1.1

Host: www.cs.princeton.edu. Here Host refers to Msg_Hdr Another Msg_Hdr called If_Modified_Since gives the client a way to conditionally request a web page. The server returns the page only if it has been modified since the time specified in that hdr line.

Request Messages

Operation	Description
OPTIONS	request information about available options
GET	retrieve document identified in URL
HEAD	retrieve metainformation about document identified in U
POST	give information (e.g., annotation) to server
PUT	store document under specified URL
DELETE	delete specified URL
TRACE	loopback request message
CONNECT	for use by proxies

Response Message

They also begin with a single Start_Line. Here version of HTTP is used with a 3 digit code indicating whether or not the request was successful, and a text string giving the reason for the response.

Example:

i. HTTP/1.1 202 Accepted, indicates that the server was able to satisfy the request.

ii. HTTP/1.1 404 Not Found, indicates that the server was not able satisfy the request.

Similar to req msg, resp msgs can contain 1/more Msg_Hdr lines which relay additional info back to sender.

Response Messages

Code	Type	Example Reasons
1xx	Informational	request received, continuing process
2xx	Success	action successfully received, understood, and accepted
3xx	Redirection	further action must be taken to complete the request
4xx	Client Error	request contains bad syntax or cannot be fulfilled
5xx	Server Error	server failed to fulfill an apparently valid request

The resp msg will also carry the requested page, which is an HTML document, but since it may carry non textual data, it is encoded using MIME.

Certain Msg_Hdr lines give attributes of page contents, including **Content_Length** (no. of bytes in the contents), **Expires** (time at which contents are considered stale) and **Last_Modified** (time at which the contents were last modified at server)

TCP Connections

HTTP 1.0 was highly inefficient, since it needed a separate TCP conn. for each data item received from the receiver.

HTTP 1.1 allowed persistent connections where client and server exchange multiple req / resp over a single TCP conn.

Though the conn is persistent, both client & server do not know, how long to keep TCP conn open. It becomes very critical as server needs to provide service to 1000s of clients. It times out and closes the conn if it did not receive requests for a period of time. Also client & server must watch each other to see if the other side has elected to close the conn, and they must use this info as a signal that they should close their side of conn as well

Caching

If a web page is cached on client, it could be retrieved from there and could be displayed quickly. On the server, a cache can intercept and satisfy a request, thereby reducing load on the server

Cache Implementation

1. At user's browser – Here the browser can simply display the cached copy if the user visits the same page again.

2. Single site wide cache – This feature should be supported by a site. User can retrieve previously downloaded pages by other users.

3. ISPs too can cache pages.

In 2nd method, users of a site know which machine is caching pages on behalf of the site, configure their browsers to connect directly to that caching host. The caching host is referred as **proxy**.

In 3rd method, the users that connect to the ISPs are not aware that the

ISP is caching pages. The HTTP req / resp coming out of various sites pass thru a common ISP router, which are cached and used for future req / resp.

The cache needs to make sure, it is not responding with an out of date version of the page. A server can assign an expiration date to each page it sends back to client / cache.

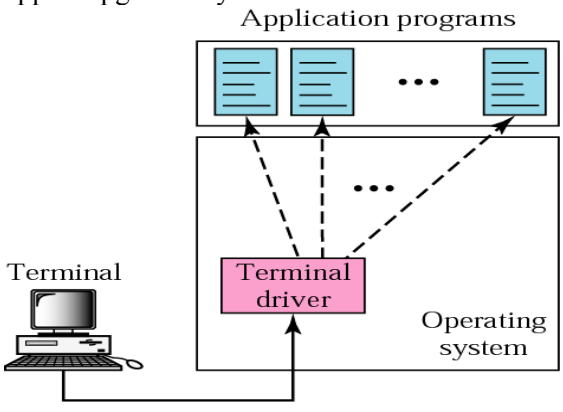
Cache uses Head / conditional Get operation (Get with If_Modified_Since hdr line) to verify if it has the most recent copy of the page. Cache directives need to be obeyed by all caching mechanisms along the req/resp chain. These directives specify whether / not a document can be cached, how long it can be cached, how fresh a document must be and so on.

7. a) Illustrate the features of TELNET. What is the need for network virtual terminal? (Apr/May 2013)

Telnet is the standard TCP/IP protocol for virtual terminal service. It enables the establishment of a connection to a remote s/m in such a way that the local terminal appears to be a terminal at remote system. In a time sharing environment, the interaction between a user and the computer occurs thru a terminal, usually a combination of keyboard, monitor & mouse.

To access the s/m, the user logs into the s/m with a user-id/log-in name and password.

A local log-in as shown below is where a user logs into a local time sharing s/m. The user types at a terminal running a terminal emulator, where the keystrokes are accepted by terminal driver that passes the characters to OS. The OS interprets the combination of characters and invokes the desired appln pgm/utility.



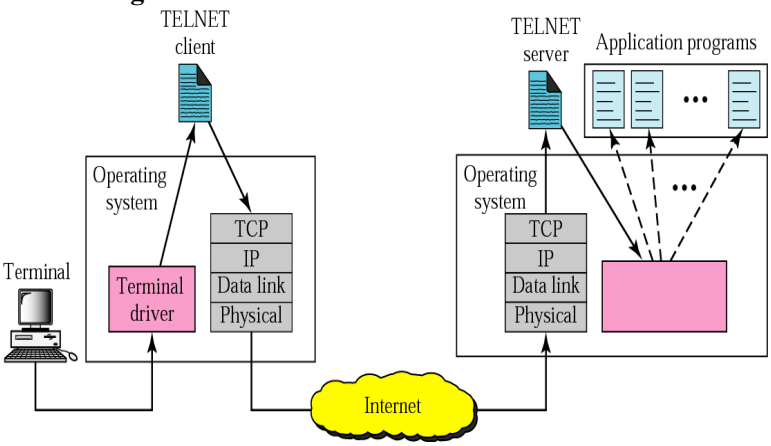
When user accesses appln pgms located in a remote computer, it is called remote login. Here Telnet client & Telnet server come into use.

User's keystrokes are sent to terminal driver, where local OS accepts the characters but does not interpret them. These characters are sent to Telnet client, which converts them into a universal character set called **Network Virtual Terminal(NVT)** characters and delivers them to local TCP/IP protocol suite.

NVT cmds/text travel thru Internet, reach TCP/IP stack at remote m/c. The characters are delivered to OS and passed to Telnet server, which changes the characters to local format.

Telnet server cannot pass such converted characters to OS, as OS can receive characters only from terminal driver. Hence a s/w called Pseudo Terminal is added which creates an illusion that the characters are coming from terminal driver. Now the OS passes the characters to the appropriate appln pgms.

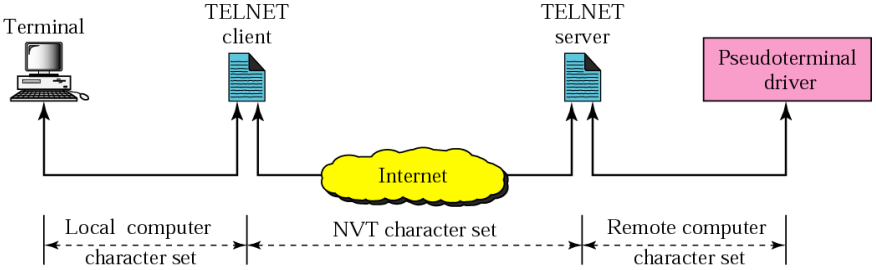
Remote login



Client/Server communication occurs in a heterogeneous environment. Both these s/ms should be compatible to enable communication between them.

Compatibility is ensured thru NVT character set, which provides an universal i/f thru which client Telnet translates characters(data/cmd) coming from local terminal into NVT form and delivers to the n/w.

Server Telnet translates data/cmds from NVT form into local computer's acceptable format.



b) Discuss the protocols used in SSH.

Secure shell provides a secured remote login service in Internet. SSH client runs on user's desktop and SSH server runs on remote m/c.

SSH provides authentication, msg integrity & confidentiality which are not provided by Telnet & rlogin. SSH provides a way to encrypt data sent over untrusted n/ws and improves the strength of authentication mechanism (user-id/pwd), they use to login.

The latest version of SSH, version 2, consists of three protocols:

- SSH-TRANS: a transport layer protocol
- SSH-AUTH: an authentication protocol
- SSH-CONN: a connection protocol

SSH-TRANS

This provides a secured channel b/w client and server, running on top of TCP. This channel is first set, whenever user logs into a remote m/c.

Channel is set, by client first authenticating itself to server using RSA. Once authenticated, client & server establish a session key which they will use to encrypt msgs exchanged b/w them.

SSH-TRANS includes a msg integrity check on all data exchanged over the channel.

When client authenticates itself to server using RSA, public key of server is needed which the client learns from server itself. This is usually done by user despite the warning given by SSH.

Once server's public key is known, it could be saved for future use. SSH may then compare the saved key with rcvd key and inform user accordingly.

Once SSH-TRANS channel is set, next step is for client to login to remote server and authenticate itself. 3 different mechanisms can be used:

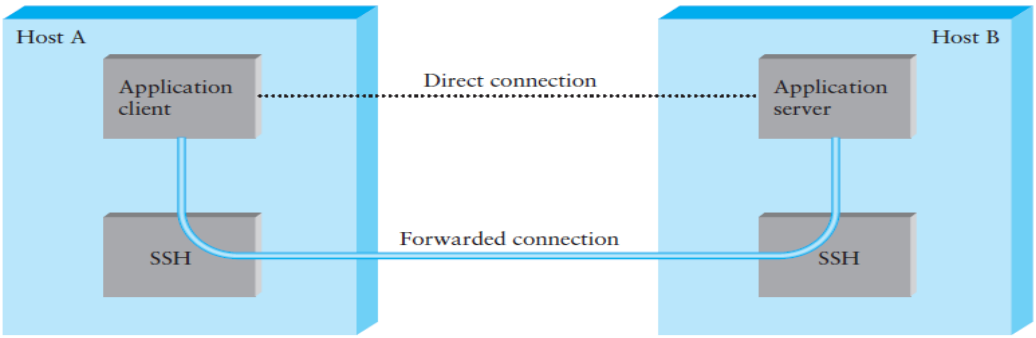
i. Since communication is taking place over a secured channel, it is ok for the user to send his pwd which will be encrypted in the SSH-TRANS channel.

ii. Go for public key encryption. This requires that server knows client's public key earlier itself.

iii. Go for host (m/c) based authentication, where an user claiming to be so and so from a certain set of trusted host is automatically believed to be that same user on the server. This method requires that the client host authenticate itself to server when they connect for the first time.

Apart from providing secure login, SSH can be extended to support other insecure TCP based applns such as IMAP. IMAP is run over this secure SSH tunnel. This capability is called **port forwarding** and it uses the **SSH-CONN** protocol.

A client on host A indirectly communicates with a server on host B by forwarding its traffic thru SSH connection. It is called port forwarding because when ms arrives at well known SSH port on server, SSH first decrypts the contents and then forwards the data to the actual port at which server is listening.



8. Explain about FTP. (Nov/Dec 2013, Nov/Dec 2012, Apr/May 2013)

FTP differs from client / server appln in the way that it established 2 conn between client & server – one for data transfer and the other for control information (commands & responses). Such a separation makes FTP more efficient.

The control conn uses simple rules of communication as only one line of cmd / resp is transferred at a time. The data conn needs more complex rules due to the variety of data types transferred.

FTP uses well known port 21 for ctrl and port no 20 for data conn. Ctrl conn is maintained during entire interactive session and data conn is opened & closed for each file transferred.

When ctrl conn is open, data conn can be opened & closed multiple times if several files are transferred.

Control Connections:

It is created in a similar way as other appln pgms. Conn remains open for an entire session. IP should provide a minimized delay service as it is an interactive session between human and server. Resp should reach without any delay.

Data Connections:

A data conn may be opened & closed several times during a session. IP should provide maximized thruput service.

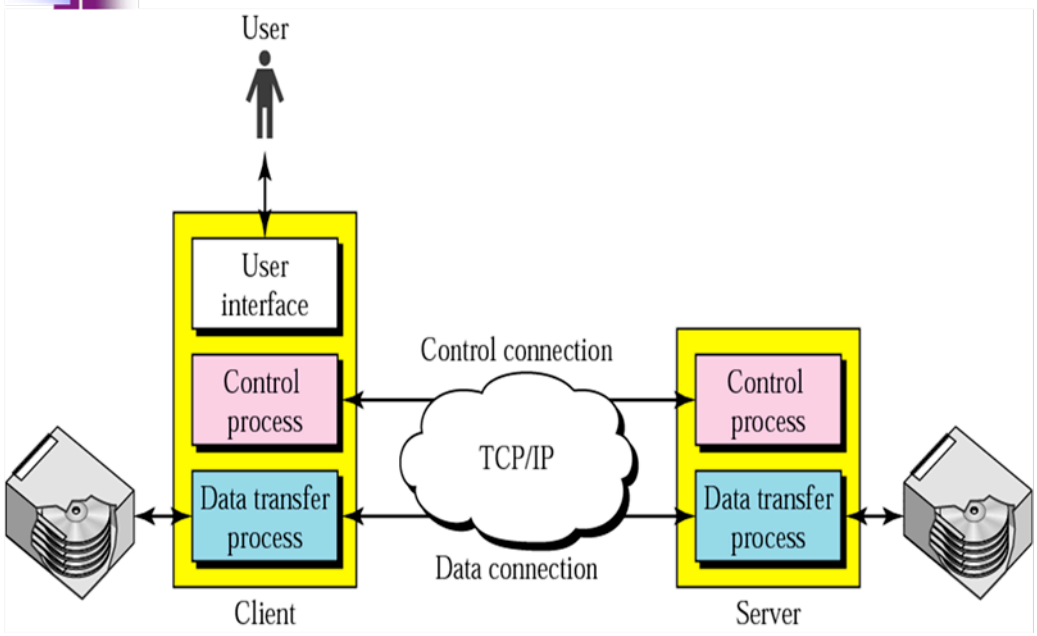
Communication:

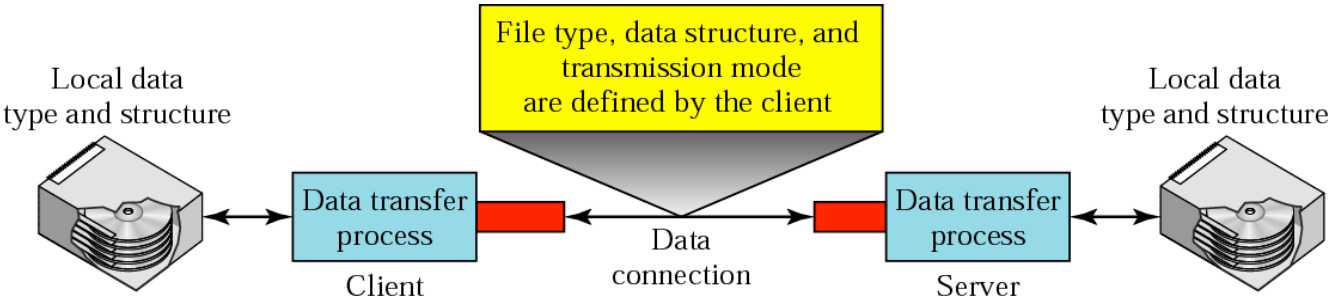
FTP client & server s/ms may use different OS, character sets, file structures and file formats. FTP must make this heterogeneity compatible.

Communication Over Control Connection:

Same approach as that of SMTP is used. It uses ASCII character set. Communication is achieved thru cmds & resps. Only one cmd is sent in one short line, terminated by end of line token.

Figure 26.12 FTP





Communication Over Data Connection:

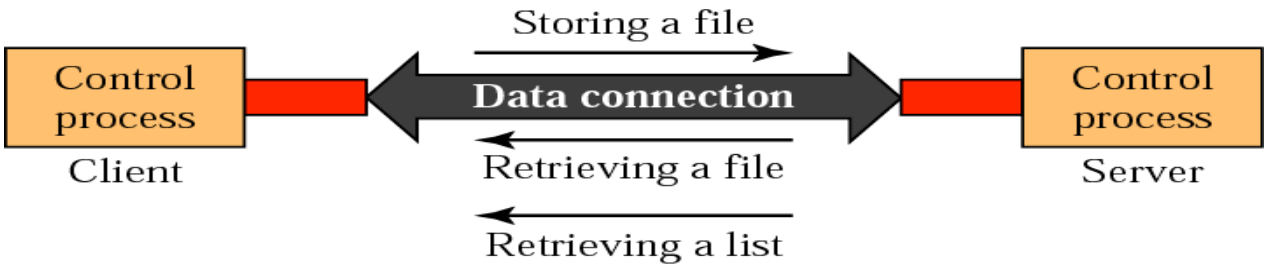
File are transferred thru data conn. Client must define the type of file, structure of data and transmission mode. Before sending file thru data conn., transmission preparation is made thru ctrl conn.

3 attributes solve the heterogeneity problem :

1. **File Type** – which could be ASCII (default for transferring text files), EBCDIC file (if 1 / both ends of conn use this type of file) and Image file (default for transferring binary files).
2. **Data Structure** – Interpretations regarding structure of data like File Structure (default), Record Structure, Page Structure.
3. **Transmission Mode** – stream mode (default mode), block mode, compressed mode.

File Transfer:

File transfer occurs over data conn under the ctrl of cmds sent over ctrl conn. File transfer in FTP means one of the following:



It is provided by OS to access services of FTP. I/F prompts user for appropriate i/p. After user types a line, FTP i/f reads the line and changes it to corresponding FTP cmd.

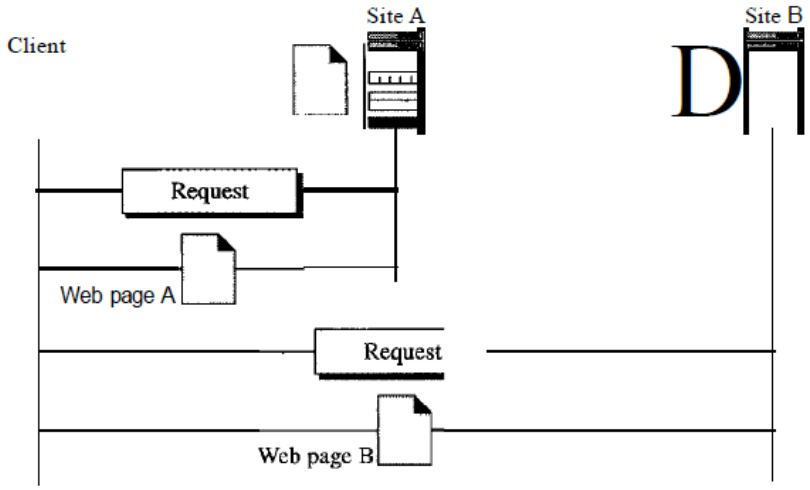
Anonymous FTP:

FTP services could be accessed thru user name & password. Some sites allow public access of files for which no authentication is required. User just gives 'anonymous' as user name and guest as 'password'. Anonymous users are allowed to use only a subset of cmds.

9. Explain WWW. (Nov/Dec 2012)

The **World Wide Web** (WWW) is a repository of information linked together from points all over the world. TheWWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet.

Architecture ofWWW



Each site holds one or more documents, referred to as *Web pages*. Each Web page can contain a link to other pages in the same site or at other sites. The pages can be retrieved and viewed by using browsers. Let us go through the scenario shown in Figure. The client needs to see some information that it knows belongs to site A. It sends a request through its browser, a program that is designed to fetch Web documents. The request, among other information, includes the address of the site and the Web page, called the URL, which we will discuss shortly. The server at site A finds the document and sends it to the client. When the user views the document, she finds some references to other documents, including a Web page at site B. The reference has the URL for the new site. The user is also interested in seeing this document. The client sends another request to the new site, and the new page is retrieved.

Client (Browser)

A variety of vendors offer commercial browsers that interpret and display a Web document, and all use nearly the same architecture. Each browser usually consists of three parts: a controller, client protocol, and interpreters. The controller receives input from the keyboard or the mouse and uses the client programs to access the document. After the document has been accessed, the controller uses one of the interpreters to display the document on the screen. The client protocol can be one of the protocols described previously such as FfP or HTIP (described later in the chapter). The interpreter can be HTML, Java, or JavaScript, depending on the type of document.

Server

The Web page is stored at the server. Each time a client request arrives, the corresponding document is sent to the client. To improve efficiency, servers normally store requested files in a cache in memory;

memory is faster to access than disk. A server can also become more efficient through multithreading or multiprocessing. In this case, a server can answer more than one request at a time.

9. Explain about SNMP and SMTP.

- A **network is a complex system**, both in terms of the number of nodes that are involved and in terms of the suite of protocols that can be running on any one node.
- All the state that is maintained and manipulated on any one of these nodes—for example, address translation tables, routing tables, TCP connection state, and so on— then it becomes tedious to manage all of this information.
- This is the **problem of network management.**
- Since the nodes we want to keep track of are distributed, our only real option is to **use the network to manage the network.**
- This means we need a protocol that allows us to read, and possibly write, various pieces of state information on different network nodes.
- The most widely used protocol for this purpose is the **Simple Network Management Protocol (SNMP).**
- **SNMP** is essentially a **specialized request/reply protocol** that supports two kinds of **request messages**: **GET and SET**.

GET is used to **retrieve a piece of state from some node.**
SET is used to **store a new piece of state in some node**.
SNMP also supports a third operation—**GET-NEXT.**

How does SNMP work?

- A system administrator interacts with a client program that displays information about the network.
- This client program usually has a graphical interface.
- You can think of this interface as playing the same role as a Web browser.
- Whenever the administrator selects a certain piece of information that he or she wants to see, the client program uses SNMP to request that information from the node in question.
- An SNMP server running on that node receives the request, locates the appropriate piece of information, and returns it to the client program, which then displays it to the user.
- **How does the client indicate which piece of information it wants to retrieve?**
- **How does the server know which variable in memory to read to satisfy the request?**
    - The answer is that SNMP depends on a companion specification called the management information base (MIB).
    - The MIB defines the specific pieces of information—the MIB variables—that you can retrieve from a network node.
- The current version of MIB, called MIB-II, organizes variables into 10 different groups.
- Some examples of the groups are:
    1. **System:** general parameters of the system (node) as a whole, including where the node is located, how long it has been up, and the system's name.
    2. **Interfaces:** information about all the network interfaces (adaptors) attached to this node, such as the physical address of each interface, how many packets have been sent and received on each interface.
    3. **Address translation:** information about the Address Resolution Protocol (ARP), and in particular, the contents of its address translation table.
    4. **IP:** variables related to IP, including its routing table, how many datagrams it has successfully forwarded, and statistics about datagram reassembly. Includes counts of how many times IP drops a datagram .
    5. **TCP:** information about TCP connections, such as the number of passive and active opens, the number of resets, the number of timeouts, default timeout settings, and so on.
    6. **UDP:** information about UDP traffic, including the total number of UDP datagrams that have been sent and received.

- There are also groups for ICMP, EGP, and SNMP itself. The 10th group is used by different media.