USN □□□□□□□□□□

13MCA31

Third Semester MCA Degree Examination, Dec.2016/Jan.2017
Computer Networks

Time: 3 hrs. Max. Marks:100

Note: ***Answer any FIVE full questions.***

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

1 a. What is a Computer Network?
Define the terms: i) Switch ii) Router iii) Hub. **(05 Marks)**
b. Discuss the classification of computer networks and write the difference between broad casting and multicasting. **(05 Marks)**
c. Discuss the responsibilities of each layer in OSI reference model. **(10 Marks)**

2 a. A channel capacity is intended to be 20Mbps, bandwidth allocated is 3MHz. To achieve this capacity compute the SNR required. **(04 Marks)**
b. Describe the characteristics of twisted pair cable and optical fiber cable in detail. **(06 Marks)**
c. Illustrate Nyquist bandwidth and Shannon capacity formula. **(10 Marks)**

3 a. Suppose we want to transmit the message 1101011011 and protect it from errors using CRC8 polynomial $x^4 + x + 1$.
i) Use polynomial long division to determine the message that should be transmitted.
Suppose the left most bit is inverted due to the noise on transmission link on the above message. What is the result of receivers CRC calculation? How does the receiver know that are error has occurred? **(10 Marks)**
b. Show the NRZ, NRZ1 and Manchester encoding for the bitpattern 10000101111. **(06 Marks)**
c. Discuss TDMA and CDMA. **(04 Marks)**

4 a. Explain the working of selective repeat sliding window protocol in flow control. **(10 Marks)**
b. Discuss the types of ALOHA collision resolution protocol in detail. **(10 Marks)**

5 a. Give the 802.11 standard frame formats. Explain the fields in detail. **(05 Marks)**
b. Describe the Bluetooth protocol architecture. **(05 Marks)**
c. Describe various Ethernet implementations. **(10 Marks)**

6 a. Describe TCP connection management process with the help of a flow diagram. **(10 Marks)**
b. Explain the working of AODV algorithm for Ad-hoc Networks. **(10 Marks)**

7 a. Discuss IPV4 packet header format. Compare the features of IPV4 and IPV6. **(10 Marks)**
b. Explain leaky bucket and token bucket congestion control algorithm with suitable diagrams. **(10 Marks)**

8 Give a brief note on :
a. DNS **(05 Marks)**
b. SIP and VOIP **(05 Marks)**
c. BGP **(05 Marks)**
d. Streaming audio and video. **(05 Marks)**

* * * * *

1.What is a computer network?Define the terms i)Switch ii)router iii)Hub.

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

Switch:

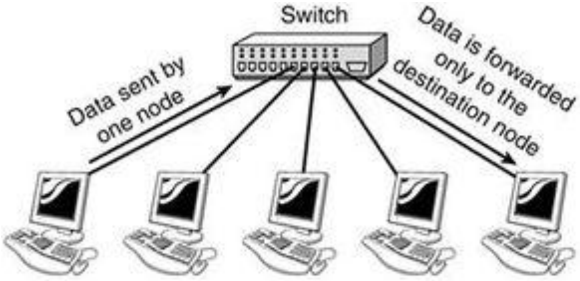
A switch is an intelligent device that works in the data link layer and has decission making capacity.

As it works in the Data link layer, it has knowledge of the MAC addresses of the ports in the network.

Switch uses Mac addresses to repeat incoming data frames only to the computer or computers to which a frame is addressed.

It speeds up the network and reduces congestion.

A switch is a secure device, because it sends information only to the desired destinations, and also certain security features such as firewalls can be implemented in the Switches.



Router:

Routers are networking devices used to extend or segment networks by forwarding packets from one logical network to another. Routers are most often used in large internetworks that use the TCP/IP protocol suite and for connecting TCP/IP hosts and local area networks (LANs) to the Internet using dedicated leased lines.

Hub:

Hub is one of the basic icons of networking devices which works at physical layer of th OSI model and hence connect networking devices physically together.

It is basically a non-intelligent device, and has no decision making capability.

It takes the input data from one of the ports and broadcast the information to all the other ports connected to the network.

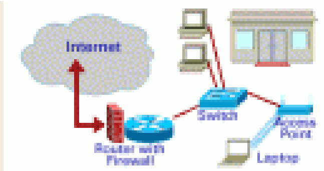
if a network is connected using hubs, the chances of a collision increases linearly with the number of computers.

Hubs pose a security risk since all packets are flooded to all ports all the time.

b) Discuss the classification of computer networks and write the difference between broadcasting and multicasting.

Local Area Network (LAN)

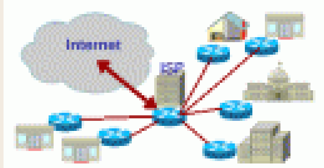
A local area network is a computer network covering a small geographic area, like a home, office, or group of buildings e.g. a school. Current LANs are most likely to be based on Ethernet technology. For example, a library will have a wired or wireless LAN for users to interconnect local devices (e.g., printers and servers) connect to the internet. All of the PCs in the library are connected by category 5 (Cat5) cable, running the IEEE 802.3 protocol through a system of interconnection devices and eventually connect to the internet. The cables to the servers are on Cat 5e enhanced cable, which will support IEEE 802.3 at 1 Gbps.



LAN example for Small Businesses

Metropolitan Area Network (MAN)

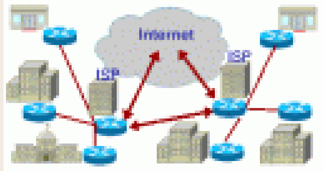
A Metropolitan Area Network is a network that connects two or more Local Area Networks or Campus Area Networks together but does not extend beyond the boundaries of the immediate town, city, or metropolitan area. Multiple routers, switches & hubs are connected to create a MAN.



Metropolitan Area Network (MAN)

Wide Area Network (WAN)

Wide Area Network (WAN) is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries). Or, less formally, a network that uses routers and public communications links.The largest and most well-known example of a WAN is the Internet.



Wide Area Network (WAN)

c) Discuss the responsibilities of each layer in OSI reference model.

The OSI model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye towards defining internationally standardized protocols.

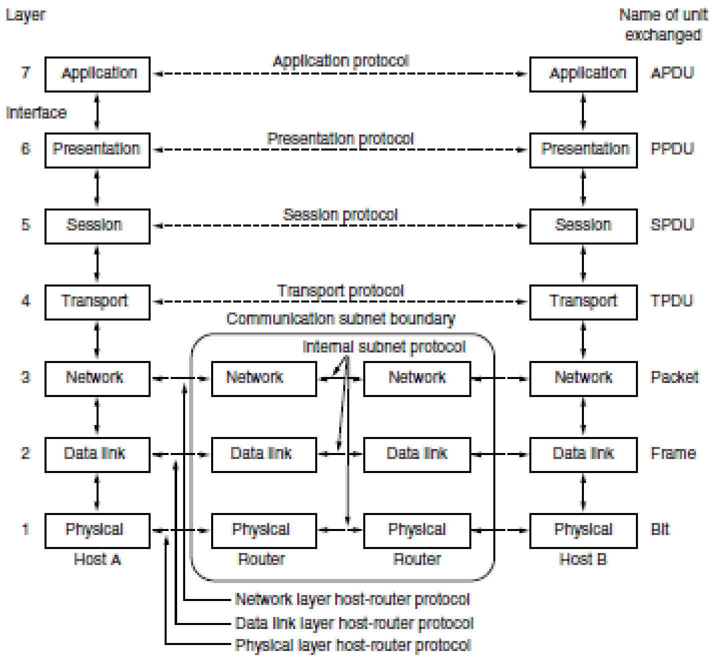


Figure 1-20. The OSI reference model.

4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy

Application Layer:

1. Using this layer the user interacts with application to provide data.
2. It acts like an interface to application program.
3. Http and ftp protocols will be used in this layer.

Presentation Layer:

1. It describes the syntax and semantics of the information to be transmitted.
2. Data structure to be used will be defined in an abstract way along with encoding with different representation to be communicated.
3. It compresses the data to be communicated .
4. It converts system specific data to network specific.

Session Layer:

1. It creates, establishes and manages sessions between them.
2. It provides services like dialog control, token management, synchronization.

Transport Layer:

1. It provides end-to-end connection of transporting messages.
2. It provides error control and flow control.
3. It specifies how much information should be sent and when to send.

Network Layer:

1. It specifies how packets are routed from source to destination.
2. Routing can be based on static tables that are wired into the network.
3. It handles congestion.
4. It specifies the quality of service like jitter, delay etc

Data Link Layer:

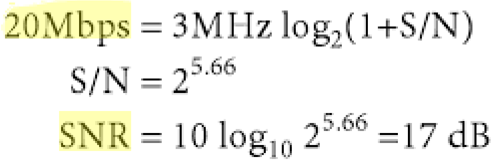
It provides transmission of error free data in the form of frames.
Switches will be operated in this layer.
It provides synchronization, error and flow control.
It is responsible for providing acknowledgement frame.

Physical Layer:

It is responsible for transmitting raw bits over a channel.
It specifies whether transmission may proceed simultaneously in both directions.

It specifies how to represent 0 or 1.
It specifies mechanical, electrical interfaces as well as physical transmission medium.

2.a A channel capacity is intended to be 20Mbps, bandwidth allocated is 3MHz.To achieve this capacity compute the SNR required.



$$20\text{Mbps} = 3\text{MHz} \log_2(1+S/N)$$

$$S/N = 2^{5.66}$$

$$\text{SNR} = 10 \log_{10} 2^{5.66} = 17 \text{ dB}$$

2.b. Describe the characteristics of twisted pair cable and optical fiber cable in detail.

Twisted pair cable:

One of the oldest and still most common transmission media is twisted pair. A twisted pair consists of two insulated copper wires, typically about 1 mm thick. The wires are twisted together in a helical form, just like a DNA molecule. Twisting is done because two parallel wires constitute a fine antenna. When the wires are twisted, the waves from different twists cancel out, so the wire radiates less effectively. A signal is usually carried as the difference in voltage between the two wires in the pair. This provides better immunity to external noise because the noise tends to affect both wires the same, leaving the differential unchanged.

Twisted pairs can be used for transmitting either analog or digital information. The bandwidth depends on the thickness of the wire and the distance traveled, but several megabits/sec can be achieved for a few kilometers in many cases. Due to their adequate performance and low cost, twisted pairs are widely used and arelikely to remain so for years to come.

Category 5:

A category 5twisted pair consists of two insulated wires gently twisted together. Four suchpairs are typically grouped in a plastic sheath to protect the wires and keep them together. This arrangement is shown in Fig.

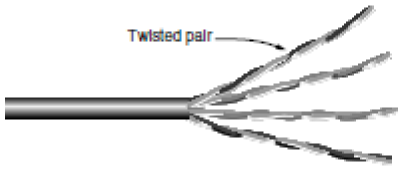


Figure 2-3. Category 5 UTP cable with four twisted pairs.

Category 3:

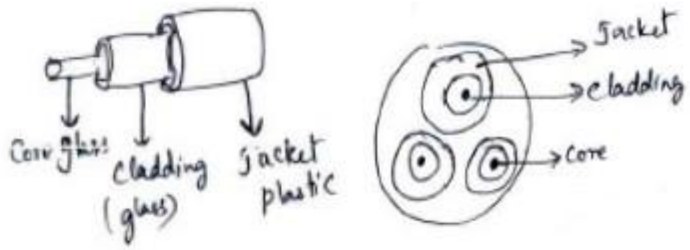
Category 3 cables with a similar cable that uses the same connector, but has more twists per meter. More twists result in less crosstalk and a better-quality signal over longer distances, making the cables more suitable for high-speed computer communication, especially100-Mbps and 1-Gbps Ethernet LANs.

Category 6 or Category 7:

These categories has more stringent specifications to handle signals with greater bandwidths. Some cables in Category 6 and above are rated for signals of 500 MHz and can support the 10-Gbps links that will soon be deployed

optical fiber cable:

Optical Fiber cables use optical fibers that carry digital data signals in the form of modulated pulses of light. An optical fiber consists of an extremely thin cylinder of glass, called the core, surrounded by a concentric layer of glass, known as the cladding. There are two fibers per cable—one to transmit and one to receive. The core also can be an optical-quality clear plastic, and the cladding can be made up of gel that reflects signals back into the fiber to reduce signal loss.



Optical Fiber is used for long-distance transmission in network backbones, high-speed LANs and high-speed Internet access. An optical transmission system has 3 components: A light source, The transmission medium and a Detector. Usually, a pulse of light indicates a 1 bit, while a 0 is indicated by the absence of light.

2.c Illustrate Nyquist bandwidth and Shannon capacity formula.

Nyquist Bandwidth: let us consider the case of a channel that is noise free. In this environment, the limitation on data rate is simply the bandwidth of the signal. A formulation of this limitation, due to Nyquist, states that if the rate of signal transmission is 2B, then a signal with frequencies no greater than B is sufficient to carry the signal rate. The converse is also true: Given a bandwidth of B, the highest signal rate that can be carried is 2B. This limitation is due to the effect of inter symbol interference, such as is produced by delay distortion. The result is useful in the development of digital-to-analog encoding schemes

If the signals to be transmitted are binary (two voltage levels), then the data rate that can be supported by B Hz is 2B bps. signals with more than two levels can be used; that is, each signal element can represent more than one bit. For example, if four possible voltage levels are used as signals, then each signal element can represent two bits. With multilevel signaling, the Nyquist formulation becomes

$$C = 2B \log_2 M$$

where M is the number of discrete signal or voltage levels

Shannon capacity: The higher the data rate, the more damage that unwanted noise can do. For a given level of noise, we would expect that a greater signal strength would improve the ability to receive data correctly in the presence of noise. The key parameter involved in this reasoning is the signal-to-noise ratio (SNR, or S/N),10 which is the ratio of the power in a signal to the power contained in the noise that is present at a particular point in the transmission.Typically, this ratio is measured at a receiver, because it is at this point that an attempt is made to process the signal and recover the data. For convenience, this ratio is often reported in decibels:

$$\mathrm{SNR_{dB}} = 10 \log_{10} \frac{\text{signal power}}{\text{noise power}}$$

This expresses the amount, in decibels, that the intended signal exceeds the noise level.

A high SNR will mean a high-quality signal and a low number of required intermediate repeaters. The signal-to-noise ratio is important in the transmission of digital data because it sets the upper bound on the achievable data rate. Shannon's result is that the maximum channel capacity, in bits per second, obeys the equation

$$C = B \log_2(1 + \mathrm{SNR})$$

3.a Suppose we want to transmit the message 1101011011 and protect it from errors using CRC* polynomial x4+x+1.

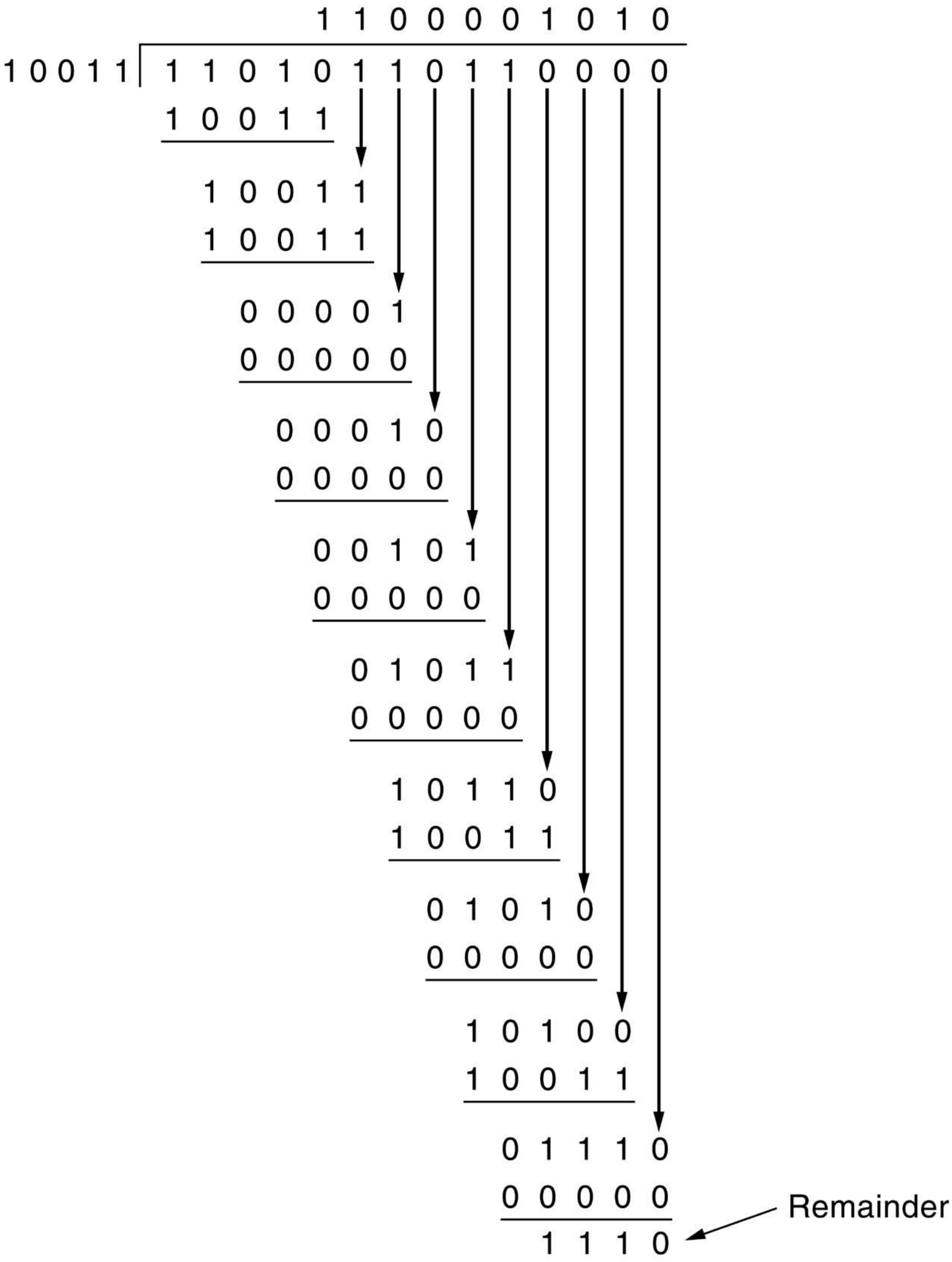
i) Use polynomial long division to determine the message that should be transmitted.

Suppose the left most bit is inverted due to the noise on transmission link on the above message. What is the result of receivers CRC calculation? How does the receiver know that an error has occurred?

Frame   : 1 1 0 1 0 1 1 0 1 1

Generator: 1 0 0 1 1

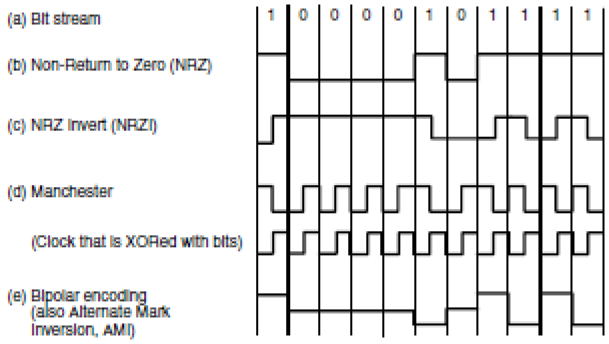
Message after 4 zero bits are appended: 1 1 0 1 0 1 1 0 1 1 0 (0



```
                     1 1 0 0 0 0 1 0 1 0
           ________________________________
  1 0 0 1 1 | 1 1 0 1 0 1 1 0 1 1 0 0 0 0
              1 0 0 1 1
              ---------
                1 0 0 1 1
                1 0 0 1 1
                ---------
                  0 0 0 0 1
                  0 0 0 0 0
                  ---------
                    0 0 0 1 0
                    0 0 0 0 0
                    ---------
                      0 0 1 0 1
                      0 0 0 0 0
                      ---------
                        0 1 0 1 1
                        0 0 0 0 0
                        ---------
                          1 0 1 1 0
                          1 0 0 1 1
                          ---------
                            0 1 0 1 0
                            0 0 0 0 0
                            ---------
                              1 0 1 0 0
                              1 0 0 1 1
                              ---------
                                0 1 1 1 0
                                0 0 0 0 0
                                ---------
                                  1 1 1 0
```

Transmitted frame: 1 1 0 1 0 1 1 0 1 1 1 1 1 0

b. Show the NRZ, NRZ1 and Manchester encoding for the bit pattern 10000101111.


(a) Bit stream
1 0 0 0 0 1 0 1 1 1 1
(b) Non-Return to Zero (NRZ)
(c) NRZ Invert (NRZI)
(d) Manchester
(Clock that is XORed with bits)
(e) Bipolar encoding (also Alternate Mark Inversion, AMI)

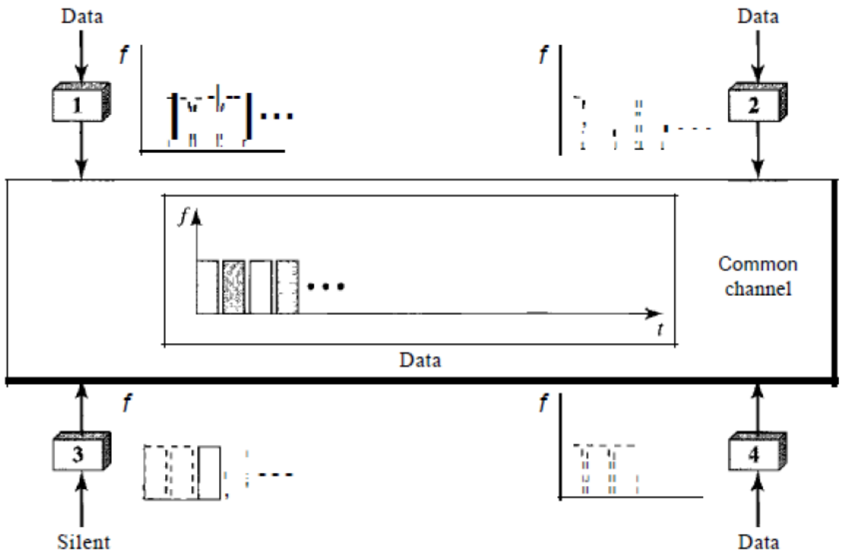
c. Discuss TDMA and CDMA.

In time-division multiple access (TDMA), the stations share the bandwidth of the channel in time. Each station is allocated a time slot during which it can send data. Each station transmits its data in is assigned time slot. The main problem with TDMA lies in achieving synchronization between the different stations. Each station needs to know the beginning of its slot and the location of its slot. This may be difficult because of propagation delays introduced in the system if the stations are spread over a large area. To compensate for the delays, we can insert *guard times.* Synchronization is normally accomplished by having some synchronization bits (normally refened to as preamble bits) at the beginning of each slot.

In TDMA, the bandwidth is just one channel that is timeshared between different stations.

We also need to emphasize that although TDMA and TDM conceptually seem the same, there are differences between them, TDMA is a physical layer technique that combines the data from slower channels and transmits them by using a faster channel. The process uses a physical multiplexer that interleaves data units from each channel.

TDMA, on the other hand, is an access method in the data link layer. The data link layer in each station tells its physical layer to use the allocated time slot. There is no physical multiplexer at the physical layer.



CDM (Code Division Multiplexing) is a form of spread spectrum communication in which a narrowband signal is spread out over a wider frequency band. This can make it more tolerant of interference, as well as allowing multiple signals from different users to share the same frequency band. Because code division multiplexing is mostly used for the latter purpose it is commonly called CDMA (Code Division Multiple Access).

CDMA allows each station to transmit over the entire frequency spectrum all the time. Multiple simultaneous transmissions are separated using coding theory.
In CDMA, each bit time is subdivided into m short intervals called chips.Typically, there are 64 or 128 chips per bit, but in the example given here we will use 8 chips/bit for simplicity. Each station is assigned a unique m-bit code called
a chip sequence. For pedagogical purposes, it is convenient to use a bipolar notation to write these codes as sequences of −1 and +1. We will show chip sequences in parentheses.
To transmit a 1 bit, a station sends its chip sequence. To transmit a 0 bit, it sends the negation of its chip sequence. No other patterns are permitted. Thus, for m □ □ 8, if station A is asigned the chip sequence (−1 −1 −1 □ 1 □ 1 −1 □ 1 □ 1), it
can send a 1 bit by transmiting the chip sequence and a 0 by transmitting (□ 1 □ 1 □ 1 −1 −1 □ 1 −1 −1). It is really signals with these voltage levels that are sent, but it is sufficient for us to think in terms of the sequences.

Each station has its own unique chip sequence. Let us use the symbol S to indicate the m-chip vector for station S, and
S for its negation. All chip sequences are pair wise orthogonal, by which we mean that the normalized inner product of any two distinct chip sequences, S andT (written as S T), is 0. It is known how to generate such orthogonal chip sequences using a method known as Walsh codes. In mathematical terms, orthogonality of the chip sequences can be expressed as follows

$$\mathbf{S} \bullet \mathbf{T} = \frac{1}{m}\sum_{i=1}^{m} S_i T_i = 0$$

This orthogonality property will prove crucial later. Note that if S T □ □ 0, then S T is also 0. The normalized inner product of any chip sequence with itself is 1:

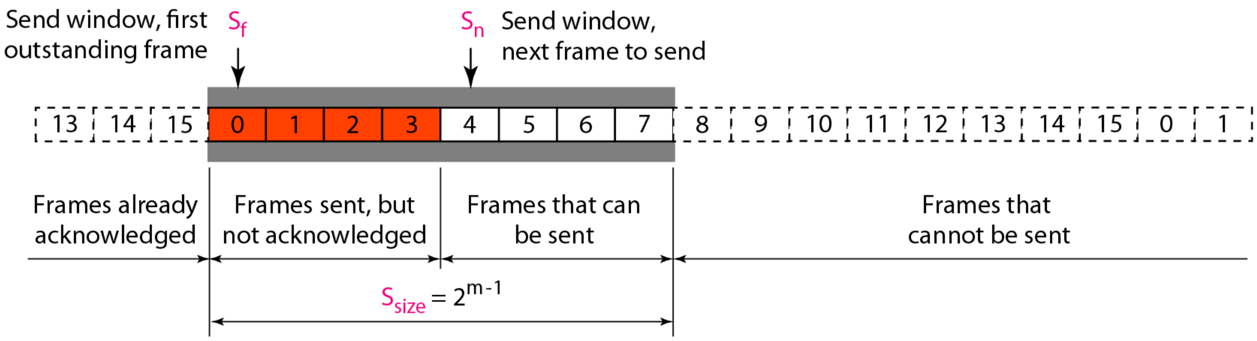
$$\mathbf{S} \bullet \mathbf{S} = \frac{1}{m}\sum_{i=1}^{m} S_i S_i = \frac{1}{m}\sum_{i=1}^{m} S_i^2 = \frac{1}{m}\sum_{i=1}^{m} (\pm 1)^2 = 1$$

This follows because each of the m terms in the inner product is 1, so the sum is
m. Also note that **S S** = □1.

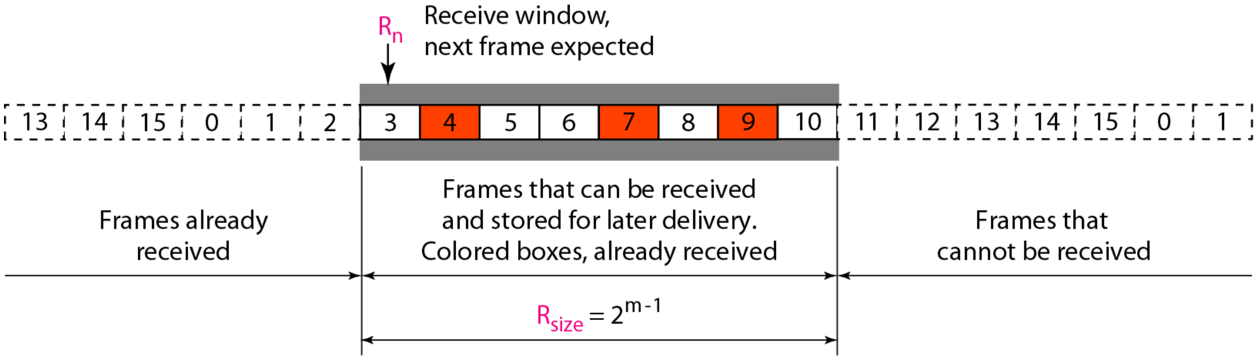
4. a. Explain the working of selective repeat sliding window protocol in flow control.

- Go-Back-N always discards out-of-order frames
  - Losing one frame may result in retransmission of multiple frames
  - Very inefficient in noisy link
- Selective Repeat ARQ allows frames to be received out of order
  - Therefore, receive window > 1
- Sender and receiver share window space equally
- For m-bit sequence numbers
- Send window: up to 2m-1
- Receive window: up to 2m-1

Sender window:

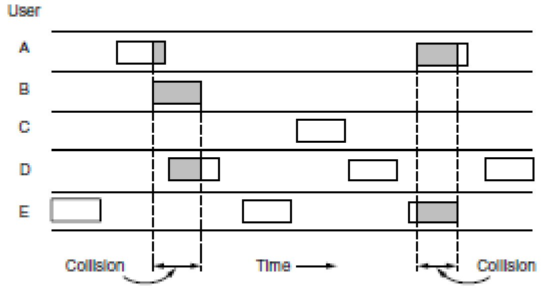

Send window, first outstanding frame
S_f
S_n
Send window, next frame to send
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already acknowledged
Frames sent, but not acknowledged
Frames that can be sent
Frames that cannot be sent
$S_{size} = 2^{m-1}$

Receiver Window:


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

b. Discuss the types of ALOHA collision resolution protocol in detail.

The basic idea of an ALOHA system is simple: let users transmit whenever they have data to be sent. There will be collisions, of course, and the colliding frames will be damaged. Senders need some way to find out if this is the case. In the ALOHA system, after each station has sent its frame to the central computer, this computer rebroadcasts the frame to all of the stations. A sending station can thus listen for the broadcast from the hub to see if its frame has gotten through. In other systems, such as wired LANs, the sender might be able to listen for collisions while transmitting



Slotted ALOHA divide timeinto discrete intervals called slots, each interval corresponding to one frame. This approach requires the users to agree on slot boundaries. One way to achieve synchronization would be to have one special station emit a pip at the start of each interval,
like a clock

The first carrier sense protocol that we will study here is called 1-persistent CSMA (Carrier Sense Multiple Access).When a station has data to send, it first listens to the channelto see if anyone else is transmitting at that moment. If the channel is idle, the stations sends its data. Otherwise, if the channel is busy, the station just waits until it becomes idle. Then the station transmits a frame. If a collision occurs, the station waits a random amount of time and starts all over again. The protocol is called 1-persistent because the station transmits with a probability of 1 when it
finds the channel idle.

A second carrier sense protocol is nonpersistent CSMA. A station senses the channel when it wants to send a frame, and if no one else is sending, the station begins doing so itself. However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission. Instead, it waits a random period of time and then repeats the algorithm. Consequently, this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA.

The last protocol is p-persistent CSMA. It applies to slotted channels and works as follows. When a station becomes ready to send, it senses the channel. If it is idle, it transmits with a probability p. With a probability q = 1 − p, it defers until the next slot. If that slot is also idle, it either transmits or defers again, with probabilities p and q. This process is repeated until either the frame has been transmitted or another station has begun transmittingand starts again). If the station initially senses that the channel is busy, it waits.
until the next slot and applies the above algorithm. IEEE 802.11 uses a refinement
of p-persistent CSMA

5. a. Give the 802.11 standard frame formats. Explain the fields in detail.

The 802.11 standard defines three different classes of frames in the air: data,control, and management. Each of these has a header with a variety of fields used within the MAC sublayer
the Frame control field which is made up of 11 subfields.
The first of these is the Protocol version, set to 00. It is there to allow future versions of 802.11 to operate at the same time in the same cell. the Type(data, control, or management) and Subtype fields (e.g., RTS or CTS). For a regulardata frame (without quality of service), they are set to 10 and 0000 in binary.The To DS and From DS bits are set to indicate whether the frame is going to or coming from the network connected to the APs, which is called the distribution system. The More fragments bit means that more fragments will follow. TheRetry bit marks a retransmission of a frame sent earlier. The Power management bit indicates that the sender is going into power-save mode. The More data bit indicates that the sender has additional frames for the receiver. The Protected Frame bit indicates that the frame body has been encrypted for security. We will discuss security briefly in the next section. Finally, the Order bit tells the receiver that the higher layer expects the sequence of frames to arrive strictly in order.

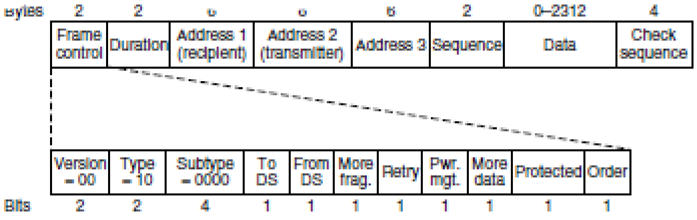


Figure 4-29. Format of the 802.11 data frame.

the Duration field, tells how long the frame and its acknowledgement will occupy the channel, measured in microseconds. It is present in all types of frames, including control frames, and is what stations use to manage the NAV mechanism. The first address is the receiver, and the second address is the transmitter. The third address gives this distant endpoint. The Sequence field numbers frames so that duplicates can be detected. Management frames have the same format as data frames, plus a format for the data portion that varies with the subtype (e.g., parameters in beacon frames).
Control frames are short. Like all frames, they have the Frame control, Duration, and Frame check sequence fields. However, they may have only one address and no data portion. Most of the key information is conveyed with the Subtype field(e.g., ACK, RTS and CTS).

5. b. Describe the blue tooth protocol architecture.

The Bluetooth standard has many protocols grouped loosely into the layers shown in Fig. 4-35. The first observation to make is that the structure does notfollow the OSI model, the TCP/IP model, the 802 model, or any other model.The bottom layer is the physical radio layer, which corresponds fairly well tothe physical layer in the OSI and 802 models. It deals with radio transmission and modulation. Many of the concerns here have to do with the goal of making thesystem inexpensive so that it can become a mass-market item.

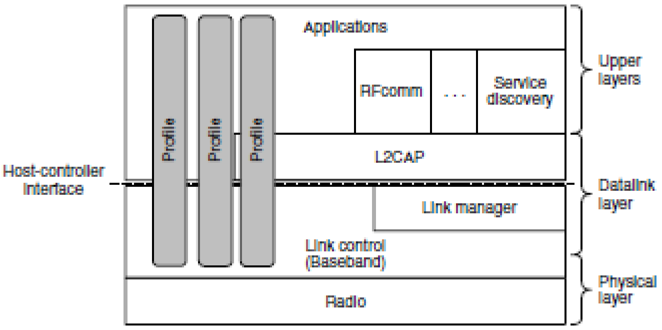


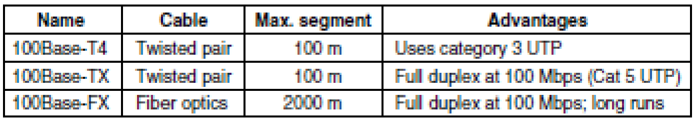
Figure 4-35. The Bluetooth protocol architecture.

The link control (or baseband) layer is somewhat analogous to the MAC sublayer but also includes elements of the physical layer. It deals with how the master controls time slots and how these slots are grouped into frames.Next come two protocols that use the link control protocol. The link manager handles the establishment of logical channels between devices, including power management, pairing and encryption, and quality of service. It lies below the host controller interface line. This interface is a convenience for implementation: typically, the protocols below the line will be implemented on a Bluetooth chip, and the protocols above the line will be implemented on the Bluetooth device that hosts the chip.The link protocol above the line is L2CAP (Logical Link Control Adaptation Protocol). It frames variable-length messages and provides reliability if needed. Many protocols use L2CAP, such as the two utility protocols that areshown. The service discovery protocol is used to locate services within the network.The RFcomm (Radio Frequency communication) protocol emulates the standard serial port found on PCs for connecting the keyboard, mouse, and modem, among other devices.

The top layer is where the applications are located. The profiles are represented by vertical boxes because they each define a slice of the protocol stack for a particular purpose. Specific profiles, such as the headset profile, usually contain only those protocols needed by that application and no others.

c. Describe various Ethernet implementations.

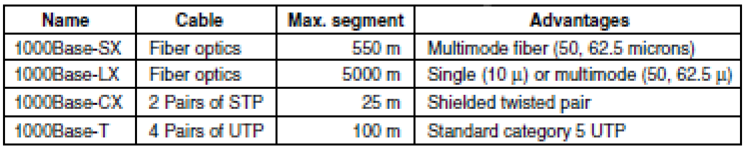
The IEEE 802.3z specification for extending Gigabit Ethernet functions into the optical fiber environment was ratified in 1998. Endorsed by the IEEE 802.3z Gigabit Ethernet Task Force, the Gigabit Ethernet Alliance, and the IEEE Standards Committee, the IEEE 802.3z standard defines Ethernet operations at rates of 1000 Mbps or 1 Gbps for half-duplex transmissions and Ethernet operations at 2000 Mbps or 2 Gbps for full-duplex transmissions. The Gigabit Ethernet IEEE 802.3z standard also clarifies capabilities of transceivers that operate in conjunction with single-mode and multimode optical fiber plants and supports ongoing utilization of in-place optical fiber links that interconnect multiple buildings in campus LANs. The role of optical components such as optical lasers in transporting data-, voice-, and video-over-optical fiber is also indicated.



Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps (Cat 5 UTP)
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

Figure 4-19. The original fast Ethernet cabling.

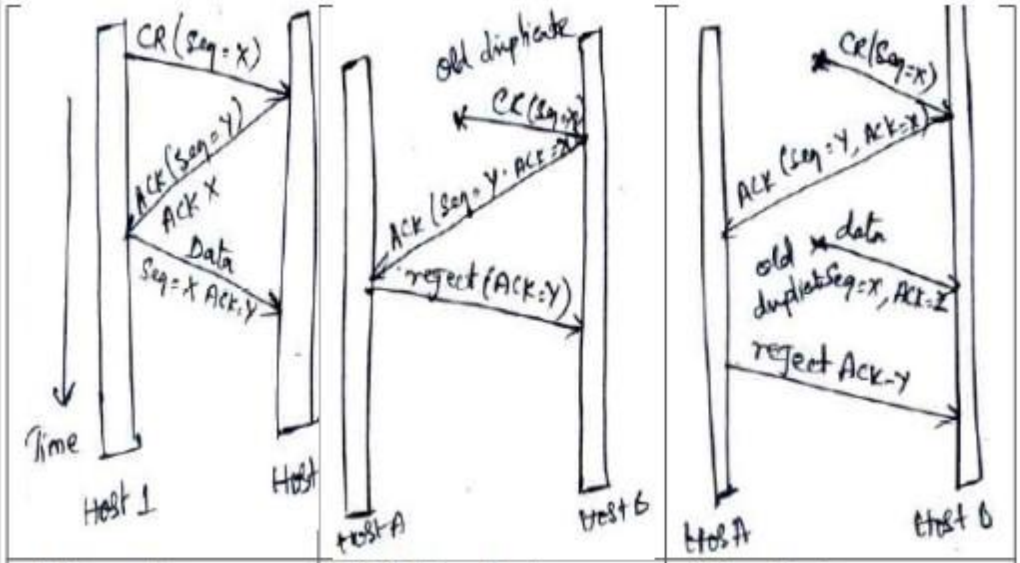
Gigabit Ethernet



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

Figure 4-21. Gigabit Ethernet cabling.

6.a. Describe TCP connection management process with the help of a flowdiagram.



a) Normal Operation

b) Old duplicate Connection Request appears

c) Duplicate Connection Request

and Duplicate Ack

This establishment protocol involves one peer checking with the other that the connection request is indeed current. The normal setup procedure when host 1 initiates is shown in **Figure a.).** Host 1 chooses a sequence number, x, and sends a CONNECTION REQUEST segment containing it to host 2. Host 2 replies with an ACK segment acknowledging x and announcing its own initial sequence number, y. Finally, host 1 acknowledges host 2's choice of an initial sequence number in the first data segment that it sends.

Figure b.) depicts how the three-way handshake works in the presence of delayed duplicate control segments. Here, the first segment is a delayed duplicate CONNECTION REQUEST from an old connection. This segment arrives at host 2 without host 1's knowledge.This results in Host 2 abandoning the connection, without any harm being caused.

Figure c.) represents the worst case, where both a delayed CONNECTION REQUEST and an ACK are floating around in the subnet. At this point, it is crucial to realize that host 2 hasproposed using y as the initial sequence number for host 2 to host 1 traffic, knowing full well that no segments containing sequence number y or acknowledgements to y are still in existence. When the second delayed segment arrives at host 2, the fact that z has been acknowledged rather than y tells host 2 that this, too, is an old duplicate. The important thing to realize here is that there is no combination of old segments that can cause the protocol to fail and have a connection set up by accident when no one wants it.

6.b. Explain the working of AODV algorithm for Ad-hoc networks.

Reactive algorithms like AODV create routes on-demand. They must however, reduce as much as possible the acquisition time

We could largely eliminate the need of periodically system-wide broadcasts

AODV uses symmetric links between neighboring nodes. It does not attempt to follow paths between nodes when one of the nodes can not hear the other one

Nodes that have not participate yet in any packet exchange (inactive nodes), they do not maintain routing information. They do not participate in any periodic routing table exchanges

Each node can become aware of other nodes in its neighborhood by using local broadcasts known as hello messages

neighbor routing tables organized to :

1.optimize response time to local movements

2.provide quick response time for new routes requests

AODV main features:

1.Broadcast route discovery mechanism

2.Bandwidth efficiently (small header information)

3.Responsive to changes in network topology

4.Loop free routing

Path Discovery:

Initiated when a source node needs to communicate with another node for which it has no routing info

Every node maintains two counters:

1. node_sequence_number
2. broadcast_id

The source node broadcast to the neighbors a route request packet (called RREQ)

RREQ structure

<src_addr, src_sequence_#, broadcast_id, dest_addr, dest_sequence_#, hop_cnt>

src_addr and broadcast_id uniquely identifies a RREQ

broadcast_id is incremented whenever source node issues a RREQ

Each neighbor either satisfy the RREQ, by sending back a routing reply (RREP), or rebroadcast the RREQ to its own neighbors after increasing the hop_count by one.

If a node receives a RREQ that has the same <src_addr, broadcast_id> with a previous RREQ it drops it immediately

If a node cannot satisfy the RREQ, stores:

Destination IP

Source IP

broadcast_id

Expiration time (used for reverse path process)

src_sequence_#

Reverse Path Setup

In each RREQ there are:

src_sequence_#

the last dest_sequence_#

src_sequence_# used to maintain freshness information about the reverse route to the source

dest_sequnece_# indicates how fresh a route must be, before it can be accepted by the source

As RREQ travels from source to many destinations, it automatically sets up the reverse path, from all nodes back to the source.

Each node records the address of the neighbor from which it received the first copy of the RREQ

These entries are maintained for at least enough time, for the RREQ to traverse the network and produce a reply.

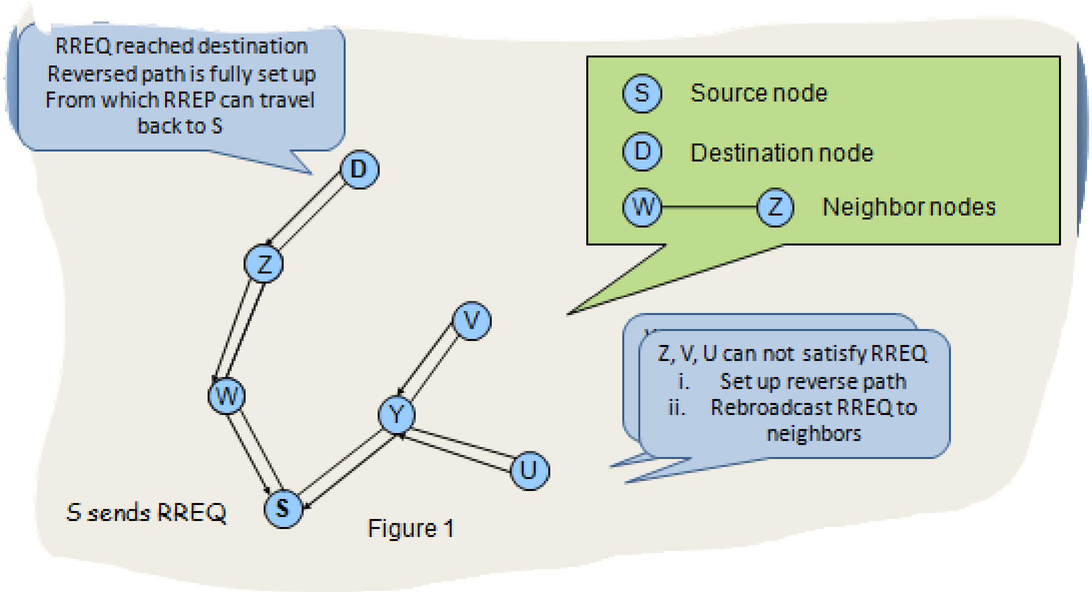


Figure 1

2. Forward Path Setup

A node receiving a RREP propagates the first RREP for a given source towards the source (using the reverse path that has already established)

Nodes that are not in the path determined by the RREP will time out after 3000 ms and will delete the reverse pointers

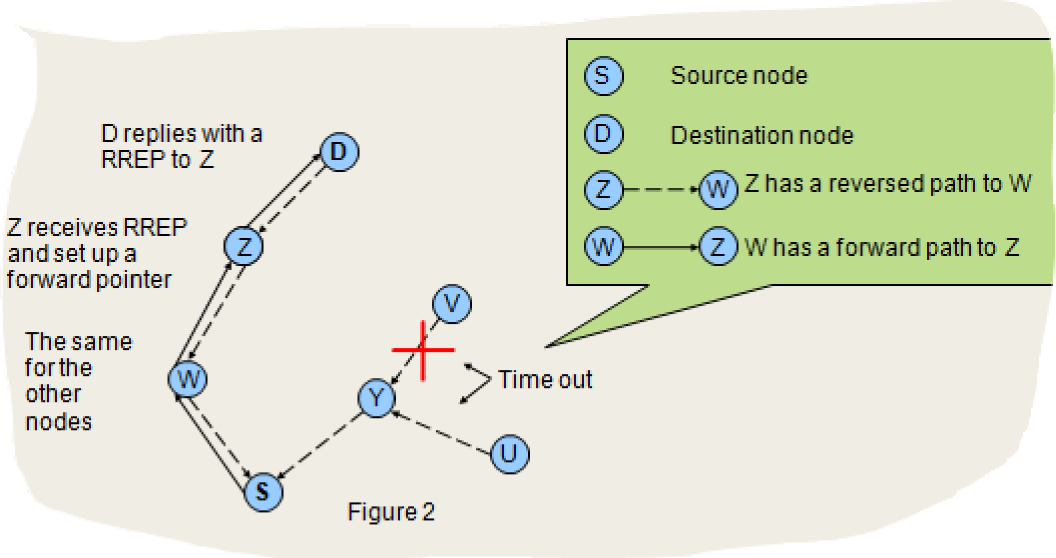
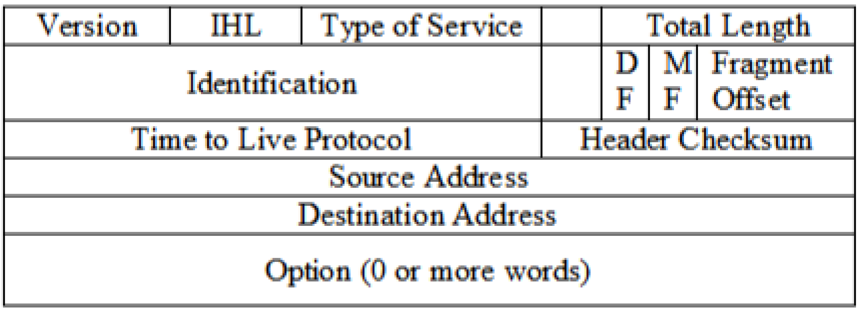


Figure 2

7.a. Discuss IPV4 packet header format. Compare the features of IPV4 and IPV6.

The header has a 20-byte fixed part and a variable-length optional part. The header format is shown in the following figure. The bits are transmitted from left to right and top to bottom, with the high-order bit of the Version field going first.



Version	IHL	Type of Service		Total Length		
Identification				D F	M F	Fragment Offset
Time to Live Protocol			Header Checksum			
Source Address						
Destination Address						
Option (0 or more words)						

The fields in the IPv4 Header are as follows:

1. The Version field keeps track of which version of the protocol the datagram belongs to.

2. IHL: Since the header length is not constant, this field specifies how long the header is, in 32-bit words. It can have values from 5 to 15, where 5 means no options are present, while 15 signifies that the header is limited to 60 bytes.

3. Type of Service: It is an indicator of which class of services is being provided, as that would have an impact on reliability and speed. These could be Differentiatedservices for example. 4. Total length includes everything in the datagram—both header and data. The maximum length is 65,535 bytes.

5. The Identification field is needed to allow the destination host to determine which packet a newly arrived fragment belongs to. All the fragments of a packet contain the same Identification value.

6. DF stands for Don’t Fragment. It is an order to the routers not to fragment the packet.It is used as part of the process to discover the path MTU, which is the largest packet that can travel along a path without being fragmented. By marking the datagram with the DF bit, the sender knows it will either arrive in one piece, or an error message will be returned to the sender.

7. MF stands for More Fragments. All fragments except the last one have this bit set. It is needed to know when all fragments of a datagram have arrived.

8. The Fragment offset tells where in the current packet this fragment belongs. All fragments except the last one in a datagram must be a multiple of 8 bytes, the elementary fragment unit. Since 13 bits are provided, there is a maximum of 8192 fragments per datagram, supporting a maximum packet length up to the limit of the Total length field. Working together, the Identification, MF, and Fragment offset fields are used to implement fragmentation.

9. The TtL (Time to live) field is a counter used to limit packet lifetimes. It was originally supposed to count time in seconds, allowing a maximum lifetime of 255 sec. It must be decremented on each hop and is supposed to be decremented multiple times when a packet is queued for a long time in a router. In practice, it just counts hops.

10. Since the header carries vital information such as addresses, it rates its own checksum for protection, the Header checksum. For purposes of this algorithm, the Header checksum is assumed to be zero upon arrival. Such a checksum is useful for detecting errors while the packet travels through the network.

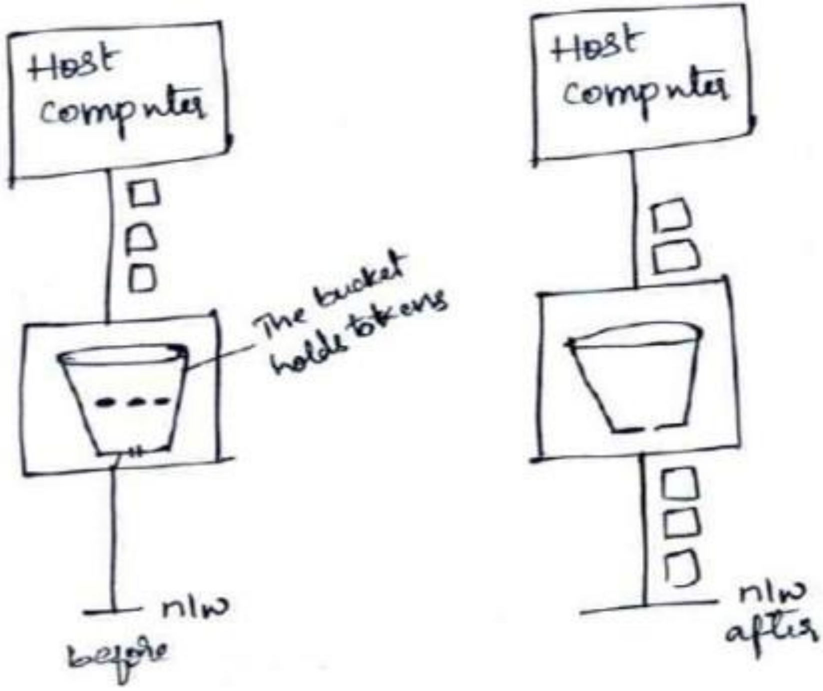
11. The Source address and Destination address indicate the IP address of the source and destination network interfaces.

12. The Options field was designed to allow subsequent versions of the protocol to include information not present in the original design, to permit experimenters to try out new ideas, and to avoid allocating header bits to information that is rarely needed. The options are of variable length. Some common options include Security, Source Routing and Timestamp.

IPv4	IPv6
IPv4 addresses are 32 bit length.	IPv6 addresses are 128 bit length.
IPv4 addresses are binary numbers represented in decimals.	IPv6 addresses are binary numbers represented in hexadecimals.
IPSec support is only optional.	Inbuilt IPSec support.
Fragmentation is done by sender and forwarding routers.	Fragmentation is done only by sender.
No packet flow identification.	Packet flow identification is available within the IPv6 header using the Flow Label field.
Checksum field is available in IPv4 header	No checksum field in IPv6 header.
Options fields are available in IPv4 header.	No option fields, but IPv6 Extension headers are available.
Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses.	Address Resolution Protocol (ARP) is replaced with a function of Neighbor Discovery Protocol (NDP).
Internet Group Management Protocol (IGMP) is used to manage multicast group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.

Broadcast messages are available.	Broadcast messages are not available. Instead a link-local scope "All nodes" multicast IPv6 address (FF02::1) is used for broadcast similar functionality.
Manual configuration (Static) of IPv4 addresses or DHCP (Dynamic configuration) is required to configure IPv4 addresses.	Auto-configuration of addresses is available.

b. Explain leaky bucket and token bucket congestion control algorithm with suitable diagrams.



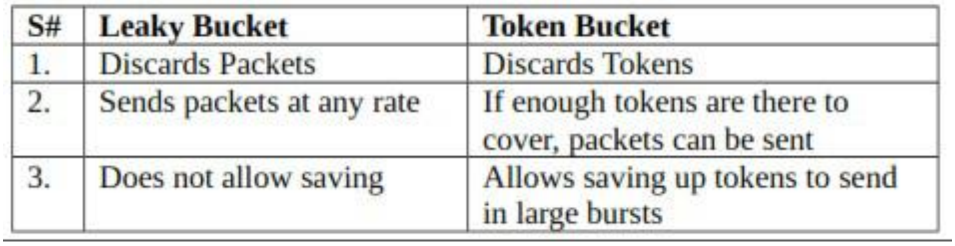
Leaky Bucket

Try to imagine a bucket with a small hole in the bottom. No matter the rate at which water enters the bucket, the outflow is at a constant rate, R, when there is any water in the bucket and zero when the bucket is empty. Also, once the bucket is full to capacity B, any additional water entering it spills over the sides and is lost. Conceptually, each host is connected to the network by an interface containing a leaky bucket.To send a packet into the network, it must be possible to put more water into the bucket. If a packet arrives when the bucket is full, the packet must either be queued until enough water leaks out to hold it or be discarded.

Token Bucket

A different but equivalent formulation is to imagine the network interface as a bucket that is being filled. The tap is running at rate R and the bucket has a capacity of B, as before. Now, to send a packet we must be able to take water, or tokens, as the contents are commonly called,out of the bucket (rather than putting water into the bucket). No more than a fixed number of tokens, B, can accumulate in the bucket, and if the bucket is empty, we must wait until more
tokens arrive before we can send another packet. This algorithm is called the token bucket algorithm.

We can differentiate the two mechanisms, as follows:



S#	Leaky Bucket	Token Bucket
1.	Discards Packets	Discards Tokens
2.	Sends packets at any rate	If enough tokens are there to cover, packets can be sent
3.	Does not allow saving	Allows saving up tokens to send in large bursts

8. Explain the following.

a) DNS

Uses transport services to build distributed applications. For the Internet, the top of the naming hierarchy is managed by an organization called **ICANN** (**Internet Corporation for Assigned Names and Numbers**).

The Internet is divided into over 250 **top-level domains**, where each domain covers many hosts. Each domain is partitioned into sub domains, and these are further partitioned, and so on. The leaves of the tree represent domains that have no subdomains (but do contain machines, of course). A leaf domain may contain a single host, or it may represent a company and contain thousands of hosts.

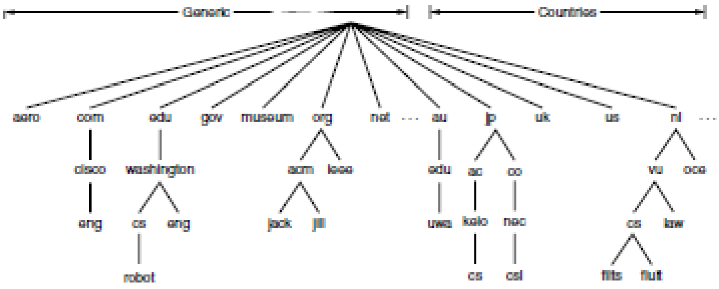


Figure 7-1. A portion of the Internet domain name space.

The top-level domains are run by **registrars** appointed by ICANN. Getting a name merely requires going to a corresponding registrar (for *com* in this case) to check if the desired name is available and not somebody else's trademark. If there are no problems, the requester pays the registrar a small annual fee and gets the name.

Every domain, whether it is a single host or a top-level domain, can have a set of **resource records** associated with it. These records are the DNS database. For a single host, the most common resource record is just its IP address, but many other kinds of resource records also exist. When a resolver gives a domain name to DNS, what it gets back are the resource records associated with that name. Thus, the primary function of DNS is to map domain names onto resource records.
A resource record is a five-tuple. Although they are encoded in binary for efficiency, in most expositions resource records are presented as ASCII text, one line per resource record. The format we will use is as follows:
Domain name Time to live Class Type Value

b. SIP and VOIP

SIP:

- Internet-centric alternative, initially for large multicast conferences
  - SIP for call signaling, SDP (Session Description Protocol) for media
- Initially very simple, light-weight, loosely-coupled sessions; oriented towards direct signaling between endpoints
- Network servers for additional capabilities:
  - Registrar for terminal registration, aliases
  - Redirect returns contact address directly to end user
  - Proxy forwards signaling (requests, responses)
- Evolution towards greater use of proxy/registrar for locating users, vertical services, call tracking, network control
- Strong, rapidly growing support (e.g., Microsoft XP, 3GPP)

VOIP:

- Consolidation of voice, data on a single network
  - Simplify infrastructure, operations; provide bundled services
- Support for intelligent terminals as well as phones
- Increased flexibility
  - Multiple bit rates, multiple media types, richer signaling
  - Distinguish calls from connections (add/modify streams during call)
- Separation of service control from switching/routing

  - Accelerate new service development, increase end-user control, evolve from VoIP towards advanced services
- Expansion of competition

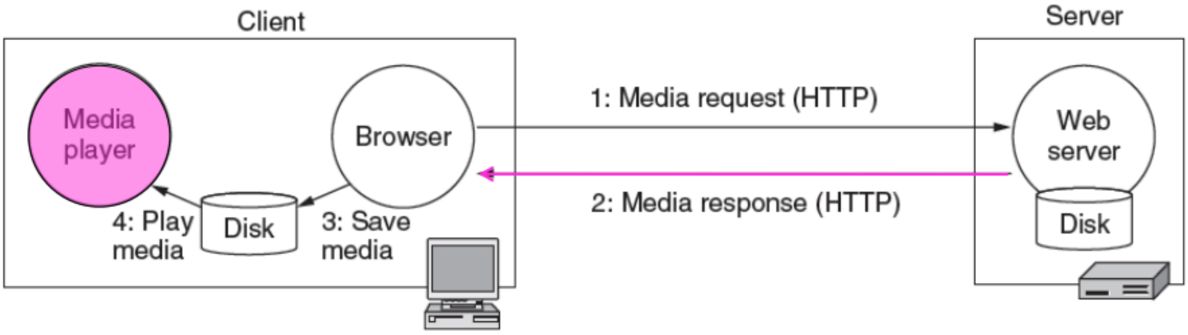
BGP:

- BGP provides each AS a means to:
  - Obtain subnet reachability information from neighboring ASs
  - Propagate reachability information to all AS-internal routers
  - Determine “good” routes to subnets based on reachability information and policy
- Pairs of routers (BGP peers) exchange routing info over semi-permanent TCP connections: BGP sessions
  - BGP sessions need not correspond to physical links
- when AS2 advertises a prefix to AS1:
  - AS2 promises it will forward datagrams towards that prefix
  - AS2 can aggregate prefixes in its advertisement

Streaming Audio and Video:

A technique for transferring data such that it can be processed as a steady and continuous stream, client does not have to download the entire file to view it.

A simple method to stream stored media, e.g., for video on demand, is to fetch the video as a file download . But has large startup delay, except for short files


Client
Media player
Browser
Disk
4: Play media
3: Save media
1: Media request (HTTP)
2: Media response (HTTP)
Server
Web server
Disk